ASIN
AGENCE DES SYSTÈMES D'INFORMATION ET DU NUMÉRIQUE
RÉPUBLIQUE DU BÉNIN

REFERENTIEL DE SECURITE POUR LA PROTECTION DES SERVICES

Table des matières

1. Préambule

1.1. Contexte

Avec le développement de l'Internet, les organisations (entreprises publiques comme privées) cherchent de plus en plus à y avoir une présence via des services en ligne ou des applications web offrant des services aux citoyens ou aux entités tierces.
A la Faveur du programme d'action du Gouvernement béninois, un accent particulier a été mis sur le développement du Numérique. De ce fait, l'écosystème du numérique connait une émulation remarquable qui favorise l'adoption des services en ligne par la population.

Cette dépendance toujours plus croissante à l'égard des services en ligne, associée à la découverte continue de faiblesses qui menacent la confidentialité, l'intégrité et la disponibilité des données numériques et des transactions, représente un défi permanent pour les organisations et l'Etat du Bénin.

Par conséquent, il est donc important de garantir que les services en ligne déployés par tous les acteurs ont un niveau de sécurité acceptable, en s'assurant que les préoccupations liées à la sécurité ont été prises en compte dans le processus de développement ou d'acquisition et de mise en production.

1.2. Enjeux

Les enjeux de ce référentiel résident dans l'engagement continue de l'Etat à protéger les services en ligne des entités (publiques et privées) par les dispositions et règles constituant les bonnes pratiques. Le référentiel vise à adresser les points spécifiques ci-dessous :

- ☑ renforcer les dispositions et règles de la Politique de Sécurité des Systèmes d'Information de l'Etat (PSSIE) sur le périmètre de la sécurité des services en ligne et infrastructures servant à leur fonctionnement
- ☑ fournir un cadre de développement sécurisé des services en ligne et des infrastructures qui servent à leur fonctionnement
- ☑ augmenter la confiance numérique des citoyens qui ont recourent à

l'usage des services en ligne dans leurs relations avec les entités visées par le présent référentiel

1.3. Risques

La mise en œuvre réussie des services en ligne doit prendre en considération les risques sommaires suivants :

- ☑ risques liés aux technologies de développement
- ☑ risques liés au paiement et à la livraison
- ☑ risques liés à la confiance vis-à-vis des services en ligne
- ☑ risques liés à l'hébergement
- ☑ risques liés à la relation avec les sous-traitants
- ☑ risques liés à l'administration des services en ligne
- ☑ risques liés à l'interfaçage avec d'autres systèmes
- ☑ risques liés aux données à caractère personnel
- ☑ risques liés à la continuité de service
- ☑ risques liés au Cloud

1.4. Objectifs

Ce référentiel vise à fournir aux entités concernées un ensemble de bonnes pratiques nationales pour sécuriser leur service en ligne en mettant en évidence les principales considérations de cybersécurité pour ceux qui utilisent, ou exploitent un service en ligne en République du Bénin. Il vise à sécuriser les données et les transactions éventuelles en assurant :

- ☑ la disponibilité, qui est la propriété pour un service en ligne d'être accessible et utilisable à la demande par les utilisateurs autorisés
- ☑ l'intégrité, qui est la propriété pour les données engagées dans un service en ligne de n'être modifiées que par les personnes ou processus autorisés
- ☑ la confidentialité, qui est la propriété pour les données engagées dans un service en ligne de ne pas être accessible à des utilisateurs ou autres systèmes d'information non autorisés
- ☑ l'authenticité, qui est la propriété selon laquelle un service en ligne est ce qu'il revendique ou prétend être
- ☑ l'imputabilité, qui est la responsabilité d'une entité mettant en œuvre un service en ligne de pouvoir identifier les actions menées par un utilisateur

☑ la non-répudiation, qui est la capacité à prouver l'occurrence d'un événement ou d'une action donnée et les entités qui en sont à l'origine
☑ la traçabilité est l'aptitude à retrouver l'historique, l'utilisation ou la localisation d'une entité au moyen des données enregistrées en conformité aux lois et règlementations en vigueur.

1.5. Démarche d'élaboration

Pour établir les règles de ce référentiel, l'ASIN s'est inspirée des standards nationaux et internationaux tels que le Code du Numérique, la PSSIE, ISO 27002, PCI DSS, RGPD, OWASP, ISO 27034 portants sur la sécurité des services en ligne et s'est basée sur les résultats de benchmarks auprès d'autres pays ayant fait preuve d'innovation dans le domaine de la protection des services en ligne.

2. Dispositions générales

2.1. Définitions

ASIN	Agence des Systèmes d'Information et du Numérique
APDP	Autorité de Protection des Données à caractère Personnel
INFORMATION	Tous signes, tous signaux, tous écrits, toutes images, tous sons ou tous enregistrements de toutes natures pouvant être véhiculés par des procédés de communications électroniques
SERVICE EN LIGNE	Un service en ligne fait référence à toutes les informations et services fournis sur Internet ou accessible à travers les technologies de l'information et de la communication.

PSSIE	Politique de Sécurité des Systèmes d'Information de l'Etat
RSSI	Responsable de la Sécurité du Système d'Information
SECURITE DU SYSTEME D'INFORMATION	Ensemble des mesures techniques et non techniques (organisationnelles et humaines) de protection permettant à un système d'information de résister à des événements susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises
SYSTEME D'INFORMATION (SI)	Ensemble organisé de ressources (matériels, logiciels, personnel, données et procédures) qui permet de regrouper, de classifier, de traiter et de diffuser de l'information sur un environnement donné
RGPD	Règlement Général sur la protection des données
DPO	Data Protection Officer

2.2. Champ d'application

Le référentiel de sécurité pour la protection des services en ligne s'applique uniquement :

☑ à toutes les entités gouvernementales engagées dans le développement et la mise en œuvre des services en ligne

☑ à toutes les entreprises privées opérant pour le compte d'une entité gouvernementale engagée dans le développement et la mise en œuvre des services en ligne.

Ce référentiel peut servir de référence de bonnes pratiques aux entreprises privées opérant dans le secteur du commerce électronique et établies en République du Bénin ou offrant des services en ligne aux Béninois.

2.3. Documents de référence

Référence n°1 : Loi n° 2017-20 portant code du numérique en République du Bénin communément appelée **le Code du Numérique du Benin**

Référence n°2 : PSSIE
Politique de Sécurité du Système d'Information de l'Etat

Référence n°3 : ISO/CEI 27001 :2022
Technologies de l'information -- Techniques de sécurité -- Systèmes de management de la sécurité de l'information – Exigences

Référence n°4 : ISO/CEI 27034
Technologies de l'information -- Techniques de sécurité – Sécurité des applications

Reference n°5: OWASP
Open Web Application Security Project

Référence n°6 : PCI DSS
Norme de sécurité de l'industrie des cartes de paiement

Référence n°7 : RGPD
Règlement général sur la protection des données relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données

Référence n°8 : ISO/CEI 27017
Technologies de l'information -- Techniques de sécurité – Code de bonnes pratiques pour la sécurité des services Cloud

2.4. Evolution du Référentiel

L'ASIN élabore les évolutions du référentiel, en liaison avec les entités concernées, en prenant en compte :

- ☑ les évolutions des contextes organisationnel, juridique, réglementaire et technologique relatifs aux services en ligne
- ☑ les résultats des missions d'évaluation de conformité au référentiel
- ☑ les évolutions normatives.

2.5. Date d'entrée en vigueur

Le référentiel entre en vigueur à partir de la date de son adoption par le Directeur général de l'Agence des systèmes d'information et du numérique.

3. Exigences de sécurité du référentiel

3.1. Conformité à la PSSIE

Nomenclature	Exigences	Contrôles
CONF-PSSIE-01	Conformité avec les exigences de la PSSIE	Les entités visées par le présent référentiel doivent être conformes à la PSSIE qui est un cadre minimal pour la sécurité des systèmes d'information en République du Bénin. La mise en conformité avec la PSSIE couvre l'ensemble des risques pesant sur le SI des entités

3.2. Exigences complémentaires à la sécurité des e-services

3.2.1. Gouvernance de la sécurité des e-services

Nomenclature	Exigences	Contrôles
GOUV-ESERV-01	Rôles et responsabilités	Un comité dédié à la sécurité des services en ligne (qui peut être un sous-comité du comité sécurité instauré par la PSSIE) doit être créé pour assurer la mission d'identification des besoins de sécurité, de conception, de développement et de mise en production du service. Ce groupe devra être composé à minima des développeurs, des architectes logiciels, des administrateurs concernés, les métiers et du RSSI pour la validation des besoins de sécurité des services en ligne.
GOUV-ESERV-02	Sensibilisation à la sécurité logicielle	L'entité mettant en œuvre un e-service doit dispenser au moins une fois l'an des sensibilisations et formations sur les bonnes pratiques en matière de sécurité logicielle à tous ses développeurs.
GOUV-ESERV-03	Formation à la sécurité logicielle	Les développeurs, membres du comité de sécurité des e-services, doivent recevoir annuellement des formations avancées relatives à la sécurité de l'information dans le développement d'applications.

3.2.2. Exigences liées aux technologies de développement

a) Concevoir et développer de manière sécurisée les services en ligne

Nomencla-ture	Exigences	Contrôles
DEV-ESERV-01	Besoins de sécurité dans les projets de développement des applications e-services	Un schéma de classification des données, basé sur les critères de disponibilité, d'intégrité et de confidentialité, qui sera utilisé par les e-services à développer, doit être instauré et suivi. L'ensemble des données des e-services implémentant l'e-service doit être classifié selon ce schéma.
DEV-ESERV-02	Appréciation des risques des services en ligne	Un processus d'appréciation des risques incluant la modélisation des attaques contre les e-services développés doit être défini et utilisé systématiquement dans les projets de développement des applications mettant en œuvre l'e-service. Ce processus doit permettre de disposer d'une vue détaillée des attaques courantes, des vulnérabilités connues ou potentielles et de maintenir l'évolution des connaissances autour de la sécurité applicative.
DEV-ESERV-03	Principes de conception sécurisée	Le principe de « Security by design » doit être mis en œuvre pour l'implémentation des fonctionnalités de sécurité attendues (validation des données, sécurité des sessions, protection contre la divulgation des informations techniques, protection contre l'interception des données en transit, authentification, journalisation, gestion des privilèges, intégration dans le système de sécurité existant, ...) qui doivent être identifiées lors de la phase de conception des e-services.
DEV-ESERV-04	Exigences de sécurité applicatives	L'entité doit recourir à des normes de sécurité à partir de la phase de conception des e-services. L'entité pourra s'appuyer sur les guides internationaux (OWASP, ISO 27034, ...) en matière de sécurité logicielle ou à minima ceux publiés par l'ASIN du Bénin.

DEV-ESERV-05	Cycle de vie du développement sécurisé	Tout e-service doit être développé en suivant un processus formel de développement sécurisé (confer Guide : Sécurité by design) incluant des jalons de sécurité dans toutes les phase de développement (qualification de la sensibilité de l'application, analyse de vulnérabilités, exigences, tests de sécurité, ...)
DEV-ESERV-06	Codage sécurisé	Les développeurs des applications mettant en œuvre les e-services doivent suivre un ensemble de lignes directrices de codage sécurisé et utiliser un ensemble de bibliothèques de sécurité reconnues ou promues par l'ASIN du Bénin.
DEV-ESERV-07	Revue de code	Une revue indépendante du code source avant la mise en production doit obligatoirement être faite par une personne qualifiée de l'équipe interne ou un FSSNQ pour toutes les applications à haut risque mettant en œuvre les e-services. Cette revue, qui allie des procédés automatisés et manuels, doit permettre de s'assurer : • que l'e-service ne fait que ce pourquoi elle a été conçue • qu'il n'existe pas de vulnérabilités permettant ultérieurement une modification illicite ou un détournement de ses fonctionnalités de sécurité • que le code est dépourvu de fonctions malicieuses ou frauduleuses connus au sens de l'état de l'art (bombe portes dérodée, logique, cheval de Troie, ...)

DEV-ESERV-08	Recette sécurité applicative	Les fonctionnalités de sécurité attendues définies à la phase de conception doivent être testées par une personne qualifiée de l'équipe interne ou un FSSNQ pour s'assurer que les applications développées résistent aux attaques identifiées dans la phase d'analyse des risques. Ces tests doivent être réalisés préalablement au déploiement des applications en environnement de production.
DEV-ESERV-09	Données de test	Les données utilisées comme jeu d'essais dans les environnements non-production ne peuvent être des données réelles contenant des données sensibles. Elles doivent être tout au moins anonymisées. Si pour des contraintes techniques, des données réelles doivent être utilisées, une dérogation doit être obtenue de la part des propriétaires des données de l'e-service. Ces données doivent être détruites systématiquement après les tests.

b) Exigences additionnelles pour le développement des e-services mobiles

Nomencla-ture	Exigences	Contrôles
APPMOB-ESERV-01	Protection du code	Des techniques de protection appropriées (obfuscation, ...) contre le risque reverse engineering doivent être appliquées dans le développement des e-services mobiles mettant en œuvre des e-services.
APPMOB-ESERV-02	Signature du code source	L'entité développant un e-service mobile doit signer le code source afin de protéger son intégrité en faisant recours aux signatures fournies par la PKI nationale.
APPMOB-ESERV-03	Distribution des applications mobiles	Un processus formel de distribution des applications mobiles doit être conçu et prendre en compte le choix de fournisseurs réputés de magasins d'applications (Google, Apple, ...), le canal de communication utilisé pour transmettre l'e-service aux magasins d'applications
APPMOB-ESERV-04	Sécurité avec les appareils mobiles	Les e-services doivent être conçues de manière à enregistrer en toute sécurité les appareils mobiles les utilisant sur la base d'une authentification forte et en utilisant des caractéristiques uniques de ces appareils (adresse IP, empreintes digitales de l'appareil)
APPMOB-ESERV-05	Considérations sur les données personnelles	Les e-services doivent être conçues de manière qu'aucune donnée sensible ne soit stockée de manière persistante sur les appareils mobiles conformément aux exigences de la Loi sur la protection des données à caractères personnels en République du Bénin (par exemple, fichiers journaux, cookies de sécurité, fichiers temporaires, mots de passe pré-enregistrés, historique des transactions, etc.). Dès qu'une session est fermée ou que l'application se ferme, ces types de données doivent être supprimées

3.2.3. Exigences de sécurité liées au paiement et à la livraison des produits et services

Nomenclature	Exigences	Contrôles
TRANSAC-ESERV-01	Sécurité du paiement	Les modes de paiement proposés par l'e-service (par carte bancaire, via une plateforme tierce à l'instar d'un opérateur de paiement mobile, ou les agrégateurs de paiements, ...) doivent être sécurisés au moyen de fonctionnalités garantissant que le canal initiant le paiement (ex : application Web) est différent de celui utilisé pour valider le paiement (ex : application mobile ou code d'authentification permettant de poursuivre le processus de paiement)
TRANSAC-ESERV-02	Accusés d'enregistrement et de réception	Toute demande, déclaration ou production de documents adressée par un utilisateur à l'entité par le biais de l'e-service ainsi que tout paiement opéré dans le cadre d'un e-service doit faire l'objet d'un accusé de réception électronique et, lorsque celui-ci n'est pas instantané, d'un accusé d'enregistrement électronique, lequel est horodaté à minima.

3.2.4. Exigences liées à la confiance vis-à-vis des e-services

Nomenclature	Exigences	Contrôles
CONF-ESERV-01	Authentification serveur	Lorsque l'e-service implique des transactions en ligne, les fonctions de sécurité d'authentification serveur doivent être implémentées sur les serveurs hébergeant les applications fournissant l'e-service. Ceci implique l'usage de certificats de la PKI nationale (ex : certificats SSL, ...) permettant d'établir des sessions sécurisées entre les serveurs et les utilisateurs ou avec d'autres serveurs.
CONF-ESERV-02	Signature électronique	Dans le cadre d'un e-service requérant une signature électronique, l'entité doit mettre en œuvre un mécanisme de signature respectant le cadre légal en République du Bénin. Le recours à la PKI nationale est recommandé pour l'obtention des certificats numériques.
CONF-ESERV-03	Chiffrement des informations liées aux transactions en ligne	Les données sensibles impliquées dans les transactions en ligne doivent être chiffrées au moyen de mécanismes de chiffrement utilisant des algorithmes robustes et/ou des certificats de la PKI nationale. Ce chiffrement doit s'appliquer aux données en transit comme celles au repos.
CONF-ESERV-04	Horodatage	Lorsque les besoins de preuve sont élevés eu égard à la nature des transactions en ligne, l'entité doit mettre en œuvre un mécanisme d'horodatage conforme au cadre légal en République du Bénin. Le recours à la PKI nationale est recommandé pour l'obtention des informations d'horodatage.

CONF-ESERV-05	Protection contre la cyber-criminalité	Toute entité mettant en œuvre un e-service doit déployer des mesures de surveillance de la sécurité numérique à l'égard des activités cybercriminelles (usurpation d'identité, phishing, campagne de propagation de codes malveillants, piégeage de site web, redirections des utilisateurs vers d'autres sites n'appartenant pas à l'entité ...).

3.2.5. Exigences liées à l'hébergement (environnement) des e-services

Nomencla-ture	Exigences	Contrôles
PROD-ESERV-01	Périmètre de sécurité réseau	Le réseau hébergeant les applications du service en ligne doit être segmenté en périmètres de sécurité : périmètre des ressources en Datacenter, périmètre des utilisateurs, périmètre des réseaux externes. Le filtrage entre les périmètres de sécurité doit être fait au moyen d'un pare-feu implémentant des mécanismes de prévention et de détection d'intrusion.
PROD - ESERV-02	Modèle de segmentation du réseau	Le modèle de zoning du réseau adopté par l'entité doit imposer une séparation par niveau, pour soutenir le principe de défense en profondeur. Les e-services Web destinées au public doivent être hébergées dans au moins trois zones dédiées et filtrées : une zone DMZ avec l'utilisation obligatoire d'un WAF, une zone des Applications, une zone Data.
PROD - ESERV-03	Configurations durcies	Les configurations de tous les équipements déployés pour le fonctionnement des e-service en ligne (serveurs, routeurs, pare-feu, ...) doivent être durcis en suivant les standards internationaux (Ex : ICS) en la matière ou à minima ceux publiés par l'ASIN Bénin.

PROD - ESERV-04	Protection contre les attaques de déni de service	Les systèmes hébergeant les e-service doivent être protégés à l'aide de solutions permettant de contre-carrer une attaque de déni de service lorsque le besoin de disponibilité de cet e-service est élevé.
PROD - ESERV-05	Tests de sécurité	Des tests d'intrusion externes et internes doivent être menés, à minima avant la mise en service de tout e-service, en cas de changement majeur, et annuellement sur les infrastructures de l'e-service par des personnes indépendantes jouissant de compétences avérées dans le domaine de la sécurité numérique ou des FSSNQ. Les résultats de ces tests conduisent à un plan d'action de correction des éventuelles vulnérabilités découvertes. Le plan d'action doit indiquer clairement les délais de mise en œuvre des recommandations.
PROD - ESERV-06	Gestion des vulnérabilités techniques	Des scans de vulnérabilités doivent être réalisés, à minima à fréquence mensuelle, sur les actifs de l'e-service exposés sur Internet à l'aide d'outils fiables de gestion des vulnérabilités techniques homologués par l'ASIN. Pour les actifs non exposés à Internet, ces scans seront réalisés à fréquence trimestrielle. Les résultats de ces scans de vulnérabilités conduisent à un plan d'action de correction des éventuelles vulnérabilités découvertes. Le plan d'action doit indiquer clairement les délais de mise en œuvre des recommandations.

3.2.6. Exigences liées à la sécurisation de l'administration des environnements des e-services

Nomencla-ture	Exigences	Contrôles
ADMIN - ESERV-01	Réseau d'administration dédié	Les machines depuis lesquelles sont administrées les systèmes et équipements du périmètre des services en ligne doivent être situées dans une zone séparée logiquement du reste des autres segments du réseau.
ADMIN - ESERV-02	Administration des applications Web	Les applications e-services doivent être administrées via des protocoles sécurisés (ex : utiliser les protocoles sécurisés tels que SSH, HTTPS, ...).
ADMIN - ESERV-03	Postes administrateurs	L'accès aux interfaces d'administration des e-services ne doit être accessibles qu'aux seuls postes d'administration autorisés.
ADMIN - ESERV-04	Hébergement externalisé	Dans le cas d'un hébergement externalisé de e-service, celle-ci ne doit être administré exclusivement qu'à partir d'une adresse IP fixe.

3.2.7. Exigences liées à la gestion de l'identité et les accès utilisateurs aux e-services

Nomencla-ture	Exigences	Contrôles
IDEN-ESERV-01	Gestion de l'identité de l'utilisateur	Un mécanisme de gestion de l'identité des utilisateurs de l'e-service doit être implémenté à travers la collecte d'un ou plusieurs attributs de l'utilisateur (ex : NPI/NPIR, nom, prénom, adresse IP, adresse électronique, photo, numéro de référence, ...). NB : Les entités du secteur public peuvent s'appuyer sur les informations disponibles sur xRoad. Ce mécanisme contribue à la mise en place du dispositif anti-fraude de l'entité.
IDEN-ESERV-02	Vérification de l'identité de l'utilisateur	Un mécanisme de vérification de l'identité déclarée des utilisateurs de l'e-service doit être implémenté à travers des éléments de sécurité dont est doté l'utilisateur (ex : mot de passe, certificats, jeton d'authentification, ...).
IDEN-ESERV-03	Principe du moindre privilège	Le principe du moindre privilège doit être appliqué. Cela implique l'attribution des droits d'accès qui est strictement nécessaire pour les activités associées à chaque utilisateur.
IDEN-ESERV-04	Approbation et autorisation d'accès aux données	L'entité mettant en œuvre l'e-service doit établir les règles de gestion des droits d'accès aux données et aux applications impliquées et doit garantir l'application de ces règles et leurs mises à jour si nécessaire.
IDEN-ESERV-05	Authentification par mot de passe	Lorsque l'accès à l'e-service requiert une authentification par mot de passe, un mécanisme de robustesse des mots de passe doit être implémenté de façon à refuser les mots de passe faibles. L'utilisation de l'authentification multi facteur est obligatoire pour les applications des e-services

3.2.8. Exigences liées à la continuité des e-services

Nomenclature	Exigences	Contrôles
CONT - ESERV-01	Gestion des incidents de sécurité	Le plan de gestion des incidents de sécurité doit être documenté et testé annuellement. Le plan de gestion des incidents doit contenir les règles de coordination, de circonscription de l'incident, de collecte de preuves, l'escalade, et la communication.
CONT - ESERV-02	Gestion de la continuité de services	Les exigences de continuité des e-service doivent être clairement définies à la suite de l'analyse d'impacts d'une interruption de service (BIA). Notamment le RTO et le RPO (le temps de récupération et le point de récupération) optimales doivent être clairement définis pour le service. Le plan de continuité d'activité doit être documenté et testé au moins annuellement

3.2.9. Exigences liées à la sécurité de la chaîne d'approvisionnement autour des e-services (fournisseurs, tiers, hébergeurs, ...)

Nomenclature	Exigences	Contrôles
APPRO-ESERV-01	Recours aux produits qualifiés	L'entité doit faire recours aux technologies de sécurité qualifiées comme technologiques de confiance reconnues à l'international ou par l'ASIN du Bénin lorsque celles-ci sont utilisées dans la mise en œuvre des e-services. La qualification de ces technologies (pare-feu, pare-feu applicatif, solution de gestion des privilèges, solution antivirale, prévention et détection d'intrusion, chiffrement, ...) fait l'objet d'une liste publiée par l'ASIN.

APPRO-ESERV-02	Recours aux prestataires qualifiés	L'entité doit faire recours aux Fournisseurs de Services de Sécurité Numériques Qualifiés par l'ASIN du Bénin lorsque les prestations offertes sur le périmètre des e-services requiert un haut degré de confiance (audits de sécurité, tests d'intrusion, investigations informatiques, surveillance sécurité, délivrance de certificats électroniques, ...). La qualification de ces prestataires fait l'objet d'une liste publiée par l'ASIN.
APPRO-ESERV-03	Contractualisation des exigences de sécurité	Toute fourniture de biens et/ou services en rapport avec les e-services doit être encadrée par des clauses contractuelles entre l'entité et les tiers. Le contrat signé entre l'entité et ces tiers doit refléter les exigences de sécurité à la hauteur des risques induits par la relation entre l'entité et ces tiers. Les clauses de sécurité minimales à aborder incluent : la responsabilité du tiers, les procédures d'échanges des données, l'auditabilité, la réversibilité, la confidentialité, la protection des données à caractère personnel ...

3.2.10. Exigences liées à la protection des données à caractère personnel

Nomenclature	Exigences	Contrôles
DCP-ESERV-01	Applicabilité des lois sur la protection des données à caractère personnel	L'entité qui met en œuvre un e-service doit réaliser une étude d'impact de l'applicabilité des lois nationales ou conventions sur la protection des données à caractère personnel (en fonction des potentiels utilisateurs ou clients) afin d'adopter les mesures de conformité idoines (registre de traitement, désignation de DPO, déclaration à une autorité compétente de protection des données en Union Européenne, ...)

DCP-ESERV-02	Politique relative aux données personnelles	L'entité doit publier à l'attention des utilisateurs de l'e-service qu'elle met en œuvre et rendre accessible une politique relative aux données à caractère personnel lorsque l'e-service collecte ce type de données. Cette politique abordera à titre d'exemple : l'identité et les coordonnées du responsable de traitement, les catégories de données collectées, les finalités de la collecte, la confidentialité, la durée de conservation des données, la gestion de l'exercice des droits, gestion des cookies, …
DCP-ESERV-03	Collecte du consentement	L'entité doit mettre en œuvre un mécanisme de collecte du consentement des usagers de l'e-service, par un acte positif, lorsque des données à caractère personnel sont collectées sur ces usagers. Il doit être rendu possible pour les usagers de retirer aussi facilement leur consentement qu'ils ne le donnent à travers l'e-service.
DCP-ESERV-04	Evaluation d'impact sur la vie privée	Lorsque des données à caractère personnel dites sensibles (profilage d'individus, données de santé, pièces d'identité, données bancaires, géolocalisation, …) sont manipulées par les e-services, l'entité doit procéder à une étude d'impact sur la vie privée débouchant sur la définition de mesures techniques et organisationnelles à mettre en œuvre en complément des autres règles de ce référentiel (chiffrement des tables de bases de données, anonymisation en environnement de test, accès très limité qu'aux personnes autorisées, …).
DCP-ESERV-05	Protection des données par défaut	L'e-service doit se limiter à ne collecter que les données strictement nécessaires sur les usagers qui utilisent cet e-service. Ceci répond au principe de minimisation et implique que les données non nécessaires ne sont pas collectées abusivement.

DCP-ESERV-06	Protection des données dès la conception	Les données à caractère personnel collectées dans le cadre de la relation entre l'usager et l'e-service doivent être protégées au même titre que les données sensibles manipulées au sein des applications mettant en œuvre l'e-service. Ceci implique que les fonctionnalités de sécurité s'appliqueront de la même manière sur les données à caractère personnel comme sur les données sensibles.
DCP-ESERV-07	Sensibilisation des usagers de l'e-service	L'entité doit communiquer dans un format accessible par les usagers de l'e-service, les bonnes pratiques de sécurité ainsi que les mesures dont ils disposent pour leur sécurité (mots de passe, lutte contre l'hameçonnage et l'usurpation d'identité, remontée d'évènements sécurité, ...)
DCP-ESERV-08	Contrôle des sous-traitants	En cas de sous-traitance de la gestion de tout ou une partie de l'e-service, les clauses relatives à la protection des données à caractère personnel doivent être intégrées dans le contrat de sous-traitance. Ces clauses doivent garantir que le sous-traitant traitera les données en respectant le cadre légal sur la protection des données en République du Bénin.

3.2.11. Exigences liées à la journalisation et à la surveillance des évènements de sécurité

Nomencla-ture	Exigences	Contrôles
EVENT-ESERV-01	Evènements de sécurité à enregistrer	Les évènements de sécurité à journaliser, à minima, doivent comprendre les évènements d'accès sur les e-services et sur les environnements hébergeant ces e-services, les évènements liés aux connexions réseaux, l'usage des privilèges, les actions d'administration, l'accès à des données sensibles, altération des données sensible, etc. La liste exhaustive des évènements doit être établie et refléter les risques associés à l'e-service.
EVENT-ESERV-02	Surveillances des évènements	Les évènements de sécurité enregistrés doivent être surveillés activement ou périodiquement au moyen de procédures de surveillance (SIEM/ SOC, monitoring, alertes, ...). Il est recommandé de recourir à un Security Opération Center (SOC) avec un FSSNQ.
EVENT-ESERV-03	Sécurité des données dans les journaux	L'enregistrement des données confidentielles (mot de passe, numéro de carte bancaire, ...) dans les logs est interdit. Si ces données étaient amenées à figurer dans les journaux pour des raisons d'audit, elles doivent être enregistrées d'une manière chiffrée.
EVENT-ESERV-04	Protection des journaux d'évènements de sécurité	Les journaux d'évènements de sécurité doivent être entreposés et entretenus de manière appropriée afin d'éviter leur perte ou leur compromission (en les redirigeant par exemple vers un autre système ou support comme WORM)

3.2.12. Exigences complémentaires liées à la sécurité du Cloud

Nomencla-ture	Exigences	Contrôles
CLOUD-ESERV-01	Maitrise du processus de récupération des données et des systèmes	L'entité doit prévoir une clause permettant de détailler les cas et conditions de réversibilités (cas de rupture de contrat). Le contrat d'hébergement doit contenir une clause détaillant les conditions de récupération de données et services dans le cas de rupture de contrat : délai, coût de l'intervention et pénalités
CLOUD-ESERV-02	Continuité des services du fournisseur Cloud	L'entité doit assurer une redondance des lignes de communication afin de garantir la disponibilité de l'accès à l'information et aux e-services.

Glossaire

3.3. Glossaire

Analyse des risques : Utilisation systématique d'informations pour identifier les sources et pour estimer le risque.

Audit : Activité périodique (ou ponctuelle) permettant d'évaluer la sécurité d'un système ou de détecter les traces d'une activité malveillante.

Cloisonnement du réseau : Technique ayant pour objectif de diviser un réseau informatique en plusieurs sous-réseaux. Le cloisonnement est principalement utilisé afin d'augmenter les performances globales du réseau et améliorer sa sécurité ; c'est un découpage en domaines ou périmètres de sécurité, qui facilite le contrôle d'accès pour mieux se protéger contre les intrusions, et empêcher la fuite d'information.

Confidentialité : Objectif de sécurité permettant de s'assurer que les informations transmises ou stockées ne sont accessibles qu'aux personnes autorisées à en prendre connaissance.

Certificat : Le certificat se matérialise par un fichier de données liant une clé cryptographique aux informations d'une personne physique ou morale.

Disponibilité : Objectif de sécurité qui consiste à assurer un accès permanent à l'information et aux services offerts par le système d'information. C'est une garantie de la continuité de service et de performances des applications, du matériel et de l'environnement organisationnel.

Filtrage : Technique de contrôle de flux sur un réseau qui empêche le passage des informations jugées suspectes.

Intégrité : Objectif de sécurité qui consiste à empêcher, ou tout du moins à détecter, toute altération non autorisée de données. Par altération on entend toute modification, suppression partielle ou insertion d'information. Cet objectif peut être assuré par la signature électronique.

Intrusion : Accès non autorisé à un système informatique afin de lire ses données internes ou d'utiliser ses ressources.

Menace : Cause potentielle d'un incident indésirable, pouvant entraîner des dommages au sein d'un système ou d'une entité.

Mesure : Moyen de gérer un risque, et pouvant être de nature administrative, technique, gestionnaire ou juridique.

Normes : Document de référence contenant des spécifications techniques précises destiné à être utilisé comme règles ou lignes directrices.

Tiers : Personne ou organisme reconnu(e) comme indépendant(e) des parties concernées.

Vulnérabilité : Faille de sécurité dans un programme ou sur un système informatique.

Cybersécurité : Ensemble des moyens utilisés pour assurer la sécurité des systèmes et des données informatiques d'un État, d'une entreprise.

Security by design : Une approche qui consiste à prendre en considération tous les aspects de sécurité lors du processus permettant la fourniture d'un bien ou d'un service.

3.4. ANNEXES

3.4.1. ANNEXE 1 : FAMILLE DE RISQUES COUVERTS PAR LE REFERENTIEL

Famille de risques liés aux technologies de développement :

☑ Risques de sécurité liés à l'utilisation d'application Web ne respectant pas les règles de développement sécurisée
☑ Risques de sécurité liés à l'utilisation d'applications Mobiles ne respectant pas les règles de développement sécurisé
☑ Risques de sécurité liés à l'utilisation d'API ne respectant pas les règles de développement sécurisé
☑ Risques de sécurité liées à la publication ou utilisation des réseaux sociaux sans respects des règles de sécurité dans l'utilisation de ces services

Famille de risques liés au paiement et à la livraison :

☑ Risques de sécurité engendrant un problème de confiance dans le service à la suite du non-respect des standards de payement par une carte de crédit ou par paiement mobile
☑ Risques de sécurité engendrant un problème de confiance dans le service à la suite du non-respect de la protection des données par les sous-traitants (livreurs, ...)
☑ Risques de sécurité liés à la liaison du service payé en ligne et non livré au demandeur.

Famille de risques liés à la confiance vis-à-vis des services en ligne :

☑ Risques de sécurité engendrant un problème de confiance dans le service à la suite d'un problème d'authenticité du portail / service (non-utilisation de certificat)
☑ Risques de sécurité engendrant un problème de confiance dans le service à la suite d'un problème d'authenticité de la page ou du compte au niveau du réseau social (page non authentifié, ...)
☑ Risques de sécurité engendrant un problème de confiance dans le service à la suite d'une arnaque ou piégeage de personnes
☑ Risques de sécurité engendrant un problème de confiance dans le service lié à la réputation du site web ou application ou réseau social

Famille de risques liés à l'hébergement :

☑ Risques de sécurité à la suite du non-respect des règles de protection du réseau hébergeant les applications / services en ligne

☑ Risques de sécurité à la suite d'une mauvaise configuration de la plate-forme / serveur hébergeant l'application en ligne

☑ Risques de sécurité à la suite d'une mauvaise définition du cadre contractuel définissant la relation avec l'hébergeur (clause de sécurité)

Famille de risques liés à la relation avec les sous-traitants :

☑ Risques de sécurité à la suite de l'absence ou manquement dans les clauses de sécurité au niveau contractuel

☑ Risques de sécurité à la suite de l'absence ou manquement dans la définition des règles de sécurité à appliquer par le personnel du sous-traitant (absence de charte, NDA, ...)

☑ Risques de sécurité à la suite de mauvaise gestion des accès du sous-traitant (accès à privilèges, méthode d'accès, ...)

Famille de risques liés à l'administration des services en ligne :

☑ Risques de sécurité à la suite du non-respect des règles de protection du poste de travail de l'administrateur (règle d'hygiènes)

☑ Risques de sécurité à la suite d'une mauvaise gestion des accès à privilège aux plateformes d'hébergement

☑ Risques de sécurité lié à un manque de traçabilité à la suite d'une mauvaise configuration des applications et équipements

☑ Risques de sécurité lié à la gestion des changements sur les plateformes d'hébergement

Famille de risques liés à l'interfaçage avec d'autres systèmes :

☑ Risques de sécurité à la suite d'une mauvaise protection du service permettant l'échange / l'interfaçage avec d'autres systèmes

☑ Risques de sécurité à la suite de l'absence ou manquement dans les clauses de sécurité (définition des exigences de sécurité) au niveau contractuel avec l'entreprise partenaire (se connectant sur le service)

Famille de risques liés aux données à caractère personnel :

☑ Risques de non-respect de la réglementation de protection de données lié à une déclaration (APDP) non réalisé

☑ Risques de non-respect de la réglementation de protection de données lié à un manque de maitrise de la relation avec les sous-traitants (livreurs, ...)

Famille de risques liés à la continuité de service :

☑ Risques de perte de données (données ou codes source) à la suite d'incident de sécurité (backup, ...)
☑ Risques d'absence ou d'incapacité à récupérer le service à la suite d'un incident de sécurité (redondance, reprise d'activité, ...)
☑ Risques de manque de maitrise (capacité de résilience) du processus de récupération à la suite d'un incident de sécurité (maitrise du temps de reprise, PRI, PCA, ...)

Famille de risques du Cloud :

☑ Risques liés à la compétence dans l'environnement du cloud
☑ Risques d'action non autorisé à la suite d'une mauvaise gestion de la sécurité du SI du fournisseur Cloud (absence de clause de sécurité, clause d'audit, ...)
☑ Risques d'absence de clause de réversibilité engendrant un manque de maitrise du processus de récupération des données et des systèmes
☑ Risques d'indisponibilité du Système suite un dysfonctionnement de la communication avec le fournisseur Cloud (problème de connexion internet au niveau du fournisseur ou du client)

3.4.2. ANNEXE 2 : GUIDE DE SÉCURITÉ POUR LE DÉVELOPPEMENT D'UNE APPLICATION DE SERVICES EN LIGNE

1. Objectifs

L'objectif du présent guide est de donner une orientation au développeur pour la sécurisation de leur des e-services avant la mise en production.
Le présent document prend comme référence les exigences de sécurités et les bonnes pratiques présentées par le référentiel de l'OWASP. L'approche adoptée prend comme point de départ les différents risques liés au développement des e-services, donnant ainsi, lieu à un ensemble de principes de sécurité qui seront traduit en exigences qui doivent être respectées.

2. Principaux risques

Le tableau ci-dessous liste les différents risques liés au développement des e-services :

Risque	Description
Risque de collecte d'informations conduisant à une reconnaissance de l'architecture et les technologies utilisées.	Elaborer une conception à partir des sources d'information publiquement disponibles dans le but d'identifier l'architecture et les technologies qui sont utilisées.
Risque d'accès non autorisé suite à une mauvaise gestion des identités	Risque d'accès non autorisé suite à une faiblesse dans les mécanismes et les procédures de gestion des identités et/ou authentification.
Risque d'accès non autorisé suite à une mauvaise gestion l'authentification	Risque d'accès non autorisé suite à une mauvaise gestion des sessions et/ou des autorisations.
Risque d'accès non autorisé suite à une mauvaise gestion des autorisations	Risque d'intrusion sur la plateforme suite à l'exploitation d'une faille ou d'une vulnérabilité ou une mauvaise gestion du filtrage au niveau des inputs (Injections, upload, ...)

Risque d'accès non autorisé suite à une mauvaise gestion des sessions	Risque de vol des données sensibles suite à l'exploitation des faiblesses au niveau des protocoles de chiffrement utilisées.
Risque d'intrusion sur la plateforme de l'entreprise suite à une mauvaise gestion du filtrage au niveau des inputs (Injections, ...)	Risque d'accès non autorisé sur la plateforme suite à une utilisation non légitimes fonctionnalité d'un e-service due à une mauvaise protection.
Risque de divulgations d'informations sensibles suite à une mauvaise gestion des messages d'erreurs	Risque d'extraction et d'exploitation des données sensibles contenu dans les messages d'erreurs.
Risque mauvaise gestion des moyens de chiffrement	Risque de déchiffrement des communication suite a l'exploitation des faiblesses au niveau des moyens de chiffrement
Risque d'utilisation non légitime de certaines fonctionnalités suite à une mauvaise gestion du logique métier.	Risque d'accès non autorisé ou élévation de privilèges suite à une mauvaise gestion et configuration des fonctionnalités ou la logique métier de l'e-services.
Risque d'intrusion ciblant le client suite à une mauvaise gestion du filtrage du côté du client	Risque lié à l'exploitation des faiblesses au niveau du filtrage des commandes et requêtes au niveau des clients

3. Principes à respecter

Le tableau ci-dessous énonce les différents principes à respecter

Principe	Description
Protéger les informations contre les risques de reconnaissance	Protéger le portail et son environnement contre toute divulgation d'information sensible pouvant être exploitée lors d'une attaque.

Protéger les identités contre le risque d'usurpation, de vol, ...	Protéger les droits d'accès contre tout abus touchant la gestion des identités et les autorisations.
Protéger les paramètres d'authentification contre tous risques de vol ou de contournement	Assurer une gestion sécurisée des sessions et la protection des paramètres d'authentifications et variables de session contre tout vol et/ou toute modification non autorisée.
Protéger les autorisations contre les risques de bypass (contournement) ou de modifications non autorisé	Assurer des contrôles sur les autorisations d'accès aux fonctionnalités et objets.
Protéger les sessions des risques d'usurpation ou de détournement	Appliquer des règles de sécurité pour empêcher l'usurpation des identités à travers l'exploitation des faiblesses au niveau de la gestion des variables de sessions.
Protéger les formulaires de saisie contre les risques d'exploitation des faiblesses des contrôles implémentés	Mettre en place des mesures pour bloquer l'exploitation des faiblesses des contrôles implémentés au niveau des formulaires de saisie (Injection, files upload, ...).
Protéger les informations sensibles contre toute divulgation à travers l'affichage des messages d'erreurs	Améliorer la sécurité des services par un renforcement de leurs configurations en personnalisant les messages d'erreurs.
Protéger les données chiffrées contre les risques liés aux faiblesses des mesures de chiffrement	Mesures qui doivent être appliquées pour protéger les données chiffrées.
Protéger les e-services contre les risques d'exploitation des erreurs logiques de fonctionnement de l'e-service	Protection de l'enchainement de l'e-services contre les attaques de détournement du logique métier et attaques forgées.
Protéger les données des risques d'exploitation des faiblesses au niveau des clients	Mettre en œuvre les mesures nécessaires pour la protection des données et s'assurer que l'e-services contrôle les attaques ciblant la partie client.

4. Exigences à respecter

Afin de mettre en œuvre les principes énoncés au niveau du paragraphe précédent, des exigences sont établies et doivent être mis en application.

4.1. Reconnaissance des informations

☑ Les données qui sont publiquement accessibles, constituent une source très importante pour la collecte des informations clés qui peuvent être utilisées lors de la mise en place attaque.
☑ Les informations recherchées sont en relation avec les architectures matériels et logiciels, les versions des services installés, les e-services publiés, etc.

Exigence	Recommandation
Reconnaissance sur les moteurs de recherche	☑ Veiller à ne pas publier des informations sensibles qui peuvent être facilement trouvées par une simple recherche en utilisant les moteurs de recherche. ☑ Ne pas publier des informations relatives aux domaines de compétences du personnel clé permanant ou occasionnel.
Identification des serveurs d'e-services	☑ Modifier les bannières et les entête des serveurs configurés par défaut qui peuvent donner une indication sur le type et la version du serveur utilisé.
Analyse des informations dans les métafichiers du serveur d'e-services	·Protection des données au niveau des fichiers de méta data : ☑ robots.txt, ☑ balises META, ☑ Plan de site, o...
Reconnaissance des e-services publiés	☑ Ne pas utiliser les ports standards pour les services utilisés, ☑ Utiliser des noms de DNS et de transfert de Zone DNS non conventionnel.

Protection des données dans le code source	☑ Effacer les commentaires et les codes sources quoi ne sont pas utilisés au niveau de l'e-service. ☑ Offusquer les codes sources (java script par exemple) du côté des clients.
Minimisation de surface d'attaque	☑ Réduire au maximum la surface d'attaque en limitant au maximum les points d'entrée à l'e-service optimisant ainsi les fonctionnalités de contrôles et de surveillance.
Identification des Framework	☑ Rendre les Framework et les composantes utilisées non identifiable au niveau des entêtes http, des cookies, du code sources et messages d'erreurs. ☑ Modifier les noms, les chemins des fichiers et répertoires, les références et les extensions de fichiers par défaut utilisés par les Framework.
Identification de l'architecture applicative	☑ Renforcer la configuration des différentes composantes de l'architecture applicative afin de rendre toute identification difficile.

4.2. Protection des Identités

La sécurité de la gestion des identités passe par la mise en œuvre des exigences suivantes :

Exigence	Recommandation
Validation des rôles	·Une documentation contenant les informations suivantes relatives aux différents rôles doit être maintenue à jour : ☑ listing des différents rôles, ☑ les autorisations et les droits attribués à chaque rôle. ·Le passage de l'utilisateur d'un rôle à un autre ne doit se faire qu'à travers des mécanismes de validation et d'approbation de l'identité.
Processus d'enregistrement des utilisateurs	·Toute inscription ne doit être effectuée qu'en passant par des étapes de validation avant la création du compte.
Création, suppression et modification de compte	·Limiter l'accès aux fonctionnalités de création, suppression de compte, de modification de droit et de privilèges aux comptes au super administrateur. Appliquer une procédure de gestion des comptes en cas d'absence, de rupture de contrat ou d'inactivité des comptes à pendant trente (30) jours ·Les événements liés à la gestion des comptes doivent être Journalisés.
Enumération des comptes	·Lier le processus de connexion à un compte à plusieurs paramètres, l'utilisateur doit saisir tous les identifiants avant de pourvoir lancer la demande de connexion. ·La réponse affichée par l'e-service ou retourné par le serveur suite à un échec de connexion ne doit pas apporter des renseignements sur la validité du compte.

4.3. Protection des paramètres d'authentification

Les exigences suivantes ont pour but de protéger les identifiants des utilisateurs contre les attaques

Exigence	Recommandation
Protection des identifiants par un canal crypté	☑ Rediriger tout trafic de HTTP vers HTTPS ☑ Utiliser un protocole de chiffrement fort pour le transport des identifiants de compte lors de la création et de connexion au compte. ☑ Configurer HTTP Strict Transport Security (HSTS) du côté du serveur pour forcer les navigateurs à utiliser HTTPS par défaut.
Identifiants par défaut	☑ Modifier, supprimer ou désactiver tous les comptes par défaut. ☑ Eliminer tous les comptes ayant des identifiants génériques.
Verrouillage et déverrouillage des comptes	☑ Limiter le nombre de tentative de connexion infructueuse trois (3) tentatives avant le verrouillage du compte. ☑ Utilisation de mécanismes de protection contre les robots. ☑ Mettre en place une mécanique de verrouillage des comptes apres 5 mn d'inactivité.
Contournement des mécanismes d'authentification	☑ Imposer la vérification d'identifiants valides à chaque fois qu'une fonction sensible est lancée. ☑ Utiliser un générateur aléatoire de session ID pour bloquer les tentatives de deviner des Id de session valide. ☑ Ne pas faire passer des paramètres de connexion au niveau des requêtes.

Enregistrement des identifiants	☑ Les identifiants doivent être stockés en utilisant des moyens de chiffrements. ☑ Limiter dans le temps la validité de la session et des valeurs de session au niveau des cookies pour une durée ne dépassant pas 900 secondes d'inactivité.
Critères de sélection de mots de passe	☑ Imposer 12 caractères comme longueur minimale du mot de passe. ☑ Exiger que le mot de passe soit complexe : formé de lettres majuscules et minuscules, chiffres et caractères spéciaux. ☑ Imposer un changement systématique des mots de passe qui ont atteint 60 jours de validité et interdire la réutilisation des 10 derniers mots de passes. ☑ Utiliser des mécanismes d'authentification multi facteurs pour les systèmes les plus critiques.
Exigences liées à la modification ou réinitialisations du mot de passe	☑ La réinitialisation du mot de passe se fait via un lien qui est envoyé par l'e-service sur l'adresse mail avec laquelle l'utilisateur s'est enregistré. ☑ Un mot de passe temporaire à courte validité (30 minutes au maximum) est envoyé à l'adresse mail avec laquelle l'utilisateur s'est enregistré. ☑ Imposer à l'utilisateur de changer son mot de passe directement après la première tentative de connexion avec un mot de passe temporaire valide avant de se connecter à l'e-service. ☑ Interdire la réutilisation de l'une des dix derniers mots de passe valides.

4.4. Protection des Autorisations

Les exigences ci-dessous doivent être respectées pour la protection des autorisations :

Exigence	Recommandation
Directory traversal	☑ Valider les saisies des utilisateurs avant tout traitement en se basant sur des Access-lists. ☑ Adaptation des chemins du côté serveur pour éviter les chemins d'accès standard aux fichiers et répertoires système.
Contournement des autorisations	☑ Limiter les privilèges attribués à chaque rôle ☑ Implémenter des ACLs pour l'accès aux ressources.
Escalassions de privilèges	☑ Imposer une validation des privilèges au niveau du serveur. ☑ Bloquer les autorisations par défaut pour les accès aux ressources.
Les références d'objet directes non sécurisées	☑ Implémenter une fonction de validation d'accès aux ressources par un utilisateur au niveau du serveur ☑ au niveau des URL, utiliser des références indirectes non prévisibles au lieu des références internes directes permettant ainsi de minimiser la manipulation des requêtes avec des valeurs valides

4.5. Gestion des sessions

Les exigences suivantes doivent être respectées pour la sécurité des sessions de connexion des utilisateurs :

Exigence	Recommandation
Gestion des variables des sessions et des cookies	☑ Appliquer un chiffrement pour toutes les variables de session au niveau du jeton de session. ☑ Limiter la durée de validité des jetons de session, durée maximale 8 heures et fermer toute session qui a atteint la durée de validité du côté client et serveur. ☑ Renouveler les jetons de session et les cookies à chaque nouvelle connexion ou appel à des fonctionnalités nécessitant une élévation de privilège. ☑ Configurer les paramètres de sécurité au niveau des cookies, les paramètres suivants sont à renseigner : ***Secure Attribute :*** Forcer l'utilisation du protocole HTTPS pour l'envoie des cookies. ***HttpOnly Attribute :*** Bloquer l'exécution des scripts qui accèdent aux cookies. ***Domain Attribute :*** Vérifier la validité du domaine. ***Path Attribute :*** identifie le chemin de validité des cookies. ***Expires Attribute :*** Limiter la durée de validité des cookies - Valeurs possibles : Persistant, duré de vie limitée, date d'expiration

Fixation des sessions	☑ Forcer le renouvellement de la session a chaque nouvelle identification. ☑ Générer une nouvelle session pour chaque nouvelle connexion utilisant un navigateur différent. ☑ Interdire la réutilisation des jetons de session et des cookies qui ont atteint la fin de vie.

4.6. Validation des Inputs

Les exigences suivantes doivent être mises en œuvre pour sécuriser les saisies au niveau de l'e-service.

Exigence	Recommandation
Validation des saisies	☑ Utiliser des Framework de validation des inputs tels que Django validator, Apache Commons Validators. ☑ Renforcer les contrôles côtés client par des contrôles du côté serveur. ☑ Implémenter des contrôles pour bloquer tous les caractères sauf ceux qui sont autorisés. ☑ Limiter le nombre de caractères dans inputs.

4.7. Gestion des erreurs

Les erreurs sont considérées comme sources d'information très importantes pour les attaquants. En effet, elles peuvent divulguer des données sensibles sur les configurations, les accès et les mécanismes implémentés. Les exigences suivantes doivent être appliquées afin de prévenir toute fuite de données.

Exigence	Recommandation
Sécurité des informations au niveau des messages d'erreurs	☑ Assurer une gestion centralisée des erreurs au niveau de l'e-services. ☑ Personnaliser les messages d'erreurs affichées coté client en supprimant toute information sensible. ☑ Rediriger les messages d'erreur sensibles vers des fichiers journaux sécurisés du côté serveurs.

4.8. Gestion des moyens cryptographiques

Cette partie traite des exigences à respecter pour assurer la sécurité des données en transit.

Exigence	Recommandation
Sécurité des communications	☑ Forcer l'utilisation des protocoles de chiffrement robustes pour la transmission des données. ☑ Exiger une valeur minimale de la force des clés utilisées – 2048 bits au minimum ☑ Utiliser des algorithmes de chiffrement fort –SHA-256. ☑ Rediriger tout le trafic http vers HTTPS et Configurer le paramètre HSTS pour forcer l'utilisation du HTTPS.
Sécurité des informations envoyées sur des canaux chiffrés	☑ Utiliser des protocoles de chiffrement robuste pour le transfert des données ☑ Chiffrer les données sensibles au niveau des entêtes http

Vulnérabilité des moyens cryptographique	☑ Utiliser la dernière version à jour des protocoles et moyens cryptographiques.

4.9. Gestion du logique métier

La logique du métier est l'enchaînement des étapes d'un processus particulier. Le but des exigences ci-dessous est de s'assurer qu'aucune tentative de contourner cette logique n'est possible afin de générer des erreurs ou exploiter des failles de sécurité.

Exigence	Recommandation
Validation du logique métier et workflow	☑ Formaliser une documentation du business logique et des contrôles de sécurité à implémenter. ☑ Implémenter les contrôles d'authentification et d'autorisation. ☑ Implémenter des contrôles de respect de l'ordre du workflow du processus et du logique métier. ☑ Désactiver ou supprimer les fonctionnalités cachées.
Validation des données	☑ Implémenter des contrôles sur les donner transmise du côté client et serveur. ☑ Contrôler les données avant tout traitement à tous les niveaux du logique métier.
Intégrité des données	☑ Utiliser des canaux sécurisés et de confiances de communication et de saisie des données. ☑ Implémenter les contrôles stricts d'authentification et d'autorisation. ☑ Implémenter des fonctionnalités de journalisation pour les accès et les actions de modifications sur les données.

Gestion des temps de réponse	☑ Aligner les réponses des e-services aux traitements les plus longs. ☑ Imposer un temps maximal de réponse avant l'annulation ou la réinitialisation des transactions. ☑ Implémenter un jeton de validité des opérations au niveau des bases de données pour forcer les utilisateurs de renouveler l'authentification une fois le jeton n'est plus valide.
Gestion des fichiers téléchargés	☑ Identifier les types de fichiers qui sont acceptés dans une liste et systématiquement bloquer les fichiers non validés. ☑ Procéder à une vérification des types de fichiers téléchargés et n'accepter que ceux qui sont autorisés. ☑ Imposer au nom des fichiers - Une longueur maximale - Un format spécifique des noms des fichiers. - Une taille maximale ☑ Systématiquement renommer les fichiers téléchargés en se basant sur un standard prédéfini par l'e-service. ☑ Avant tout traitement sur les fichiers il faut : - Enregistrer les fichiers dans un dossier sécurisé. - Calculer et valider la signature des fichiers. - Scanner les fichiers par une solution antivirale intégrant les fonctionnalités de sand boxing.

4.10. Validation des données coté clients

Afin de prévenir les attaques ciblant les clients les exigences suivantes doivent être respectés :

Exigence	Recommandation
Exigence liées DOM-Based Cross Site Scripting	☑ Implémenter des contrôles sur objets et les fonctions afin de vérifier leur légitimité. ☑ Appliquer les bonnes pratiques d'écriture de code source. ☑ Utiliser des bibliothèques et des Framework non vulnérables.
Exécution des scripts	☑ Minimiser l'exécution des scripts du côté du client. ☑ Dupliquer les contrôles cotés client au niveau du serveur. ☑ Implémenter des fonctions d'obfuscation des scripts qui s'exécutent au niveau des navigateurs.
Injection HTML, CSS	☑ Utiliser des mécanismes d'échappement avant l'intégration des données.
Client-side URL Redirect and Ressources manipulation	☑ Implémenter des mécanismes de validation des URL.
Accès aux ressources partagées	☑ Appliquer un contrôle d'accès sur les ressources en se basant sur les listes blanches.

Vol des clicks	☑ Renforcer la configuration des serveurs pour interdire la manipulation des clicks - Content-Security-Policy : frame-ancestors - X-Frame-Options - SameSite cookie attribute
Websocket	☑ Implémenter des restrictions sur les connexions websocket en n'autorisant que les connexions de source de confiance et en utilisant les protocoles sécurisés.
Sauvegarde des clients	☑ Sauvegarder les données sensibles du côté du serveur et non du côté client. ☑ Chiffrer les données enregistrées.

5. Guide de test

L'ensemble des éléments présentés ci-dessous permettent d'orienter l'utilisateur du document à définir les tests nécessaires afin de valider le service en ligne.

Chaque sous chapitre sera structuré comme suit :

☑ Guide de test :
Enonce l'ensemble des tests nécessaire afin de valider la conformité du service en ligne

☑ Exemple de test :
Des exemples de test qui pourront être réalisés

☑ Outils :
Un aperçu d'outils de tests qui pourront être utilisés

5.1. Reconnaissance des informations

☑ **Guide de test :**

Exigence	Objectifs de test
Reconnaissance sur les moteurs de recherche	Identifier les informations sensibles de conception et de configuration de l'application, du système ou de l'organisation sont exposées directement (sur le site Web de l'organisation) ou indirectement (sur un site Web tiers).
Identification des serveurs web	Trouver la version et le type d'un serveur Web en cours d'exécution
Analyse des informations dans les métafichiers du serveur Web	Identifier les fuites d'informations au niveau des répertoires ou du ou des chemins de dossier de l'application d'e-services. Créez la liste des répertoires qui doivent être évités par les Spiders, les Robots ou les Crawlers.
Identification des Framework	Identifier le type de framework web utilisé afin d'avoir une meilleure compréhension de la méthodologie de test de sécurité.
Identification de l'architecture applicative	Cartographier l'application cible et comprendre les principaux workflows.

Exemple de test :

Exigence	Exemple de test
Reconnaissance sur les moteurs de recherche	Test des Opérateurs de recherche Un opérateur de recherche est un mot-clé ou une syntaxe spéciale qui étend les capacités des requêtes de recherche régulières et peut aider obtenir des résultats plus précis. Ils prennent généralement la forme de operator:query . Quelques exemples couramment pris en charge : opérateurs de recherche : ☑ site : limitera la recherche au domaine fourni. ☑ inurl : renverra uniquement les résultats qui incluent le mot-clé dans l'URL. ☑ intitle : ne renverra que les résultats contenant le mot-clé dans le titre de la page. ☑ intext: ou inbody: recherchera uniquement le mot-clé dans le corps des pages. ☑ filetype : correspondra uniquement à un type de fichier spécifique, par exemple png ou php. Par exemple, pour trouver le contenu Web de owasp.org tel qu'indexé par un moteur de recherche typique, la syntaxe requise est : site : owasp.org `GET / SANTA CLAUS/1.1` `HTTP/1.1 400 Bad Request` `Date: Fri, 06 Sep 2019 19:21:01 GMT` `Server: Apache/2.4.41 (Unix)` `Content-Length: 226` `Connection: close` `Content-Type: text/html; charset=iso-8859-1` `<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">` `<html><head>` `<title>400 Bad Request</title>` `</head><body>` `<h1>Bad Request</h1>` `<p>Your browser sent a request that this server could not understand. ` `</p>` `</body></html>`

Exigence	Exemple de test
Identification des serveurs web	Envoi de requêtes malformées Les serveurs Web peuvent être identifiés en examinant leurs réponses d'erreur, et dans les cas où ils n'ont pas été personnalisés, leurs pages d'erreur par défaut. Une façon de contraindre un serveur à les présenter est d'envoyer des messages intentionnellement incorrects ou demandes malformées. Par exemple, voici la réponse à une requête pour la méthode inexistante SANTA CLAUS d'un serveur Apache. `GET / SANTA CLAUS/1.1` `HTTP/1.1 400 Bad Request` `Date: Fri, 06 Sep 2019 19:21:01 GMT` `Server: Apache/2.4.41 (Unix)` `Content-Length: 226` `Connection: close` `Content-Type: text/html; charset=iso-8859-1` `<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">` `<html><head>` `<title>400 Bad Request</title>` `</head><body>` `<h1>Bad Request</h1>` `<p>Your browser sent a request that this server could not understand. ` `</p>` `</body></html>`

Exigence	Exemple de test
Analyse des informations dans les métafichiers du serveur Web	**Analysez le fichier robots.txt et identifiez les balises <META> du site Web** Les spiders/robots/crawlers du web peuvent intentionnellement ignorer les directives Disallow spécifiées dans un fichier robots.txt, telles que ceux des réseaux sociaux pour s'assurer que les liens partagés sont toujours valides. Par conséquent, robots.txt ne doit pas être considéré comme un mécanisme pour appliquer des restrictions sur la façon dont le contenu Web est consulté, stocké ou republié par des tiers. La directive Disallow spécifie quelles ressources sont interdites par les spiders/robots/crawlers. Dans l'exemple ci-dessous, les répertoires tels que les suivants sont interdits : ☑ User-agent: * ☑ Disallow: /search ☑ Disallow: /sdch ☑ Disallow: /groups ☑ Disallow: /images ☑ Disallow: /catalogs

Exigence	Exemple de test
Identification des Framework	**Analyser les HTTP Headers** La forme la plus élémentaire d'identification d'un framework Web consiste à examiner le champ X-Powered-By dans l'en-tête de réponse HTTP. Considérer la requête-réponse HTTP suivante : $ nc 127.0.0.1 80 HEAD / HTTP/1.0 HTTP/1.1 200 OK Server: nginx/1.0.14 Date: Sat, 07 Sep 2013 08:19:15 GMT Content-Type: text/html;charset=ISO-8859-1 Connection: close Vary: Accept-Encoding X-Powered-By: Mono D'après le champ X-Powered-By, nous comprenons que le framework d'application Web est susceptible d'être Mono. Cependant, bien que cette approche soit simple et rapide, cette méthodologie ne fonctionne pas dans 100% des cas. Il est possible de facilement désactiver l'en-tête X-Powered-By par une configuration appropriée. Il existe également plusieurs techniques qui permettent à un site Web de masquer les en-têtes HTTP (voir un exemple dans la section Correction).

Exigence	Exemple de test
Identification de l'architecture applicative	**Cartographier l'architecture de l'application** L'architecture de l'application doit être cartographiée via des tests pour déterminer quels différents composants sont utilisés pour créer l'application d'e-services. Dans les petites configurations, comme une simple application basée sur CGI, un seul serveur peut être utilisé qui exécute le serveur Web qui exécute l'application CGIs C, Perl ou Shell, et peut-être aussi l'authentification mécanisme.

- **Outils :**

Exigence	Outils
Analyse des informations dans les métafichiers du serveur Web	- Browser (View Source function) - curl - wget - rockspider
Identification des Framework	- WhatWeb - BlindElephant - Wappalyzer

Guide de test :

Exigence	Objectifs de test
Validation des rôles	Valider les rôles système définis dans l'application définir et séparer suffisamment chaque rôle système et métier pour gérer l'accès approprié aux fonctionnalités et aux informations du système.
Processus d'enregistrement des utilisateurs	Vérifiez que les exigences d'identité pour l'enregistrement des utilisateurs sont alignées sur les exigences de sécurité. Validez le processus d'inscription des utilisateurs.
Enumération des comptes	Passez en revue les processus liés à l'identification de l'utilisateur (par exemple, l'enregistrement, la connexion, etc.). Énumérer les utilisateurs dans la mesure du possible grâce à l'analyse des réponses.

Exemple de test :

Exigence	Exemple de test
Validation des rôles	**Tester l'existence de Matrice des rôles** Vérifier l'existence d'une matrice des rôles par rapport aux autorisations. La matrice doit énumérer tous les rôles qui peuvent être provisionnés et explorer les autorisations qui peuvent être appliquées aux objets, y compris les éventuelles contraintes. Si une matrice est fournie avec la demande, elle doit être validée par le testeur, si elle n'existe pas, le testeur doit la générer et déterminer si la matrice satisfait l'accès souhaité politique de l'application.

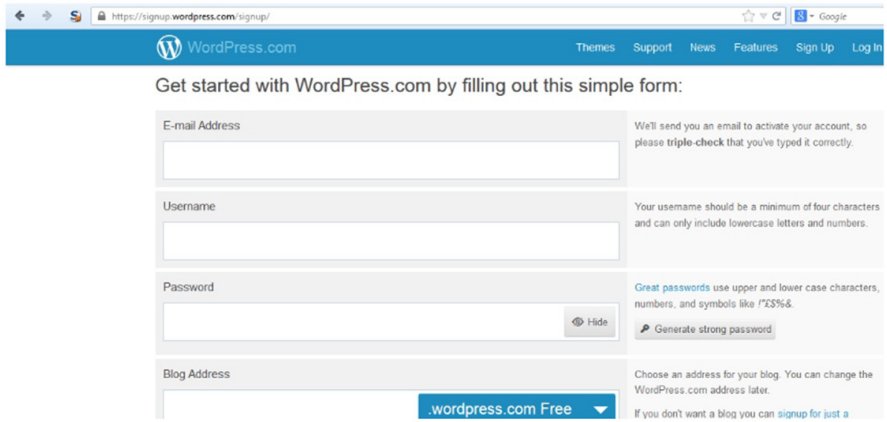
<table>
<tr>
<td>Validation des rôles</td>
<td>Exemple de matrice
<table>
<tr><th>ROLE</th><th>PERMISSION</th><th>OBJECT</th><th>CONSTRAINTS</th></tr>
<tr><td>Administrator</td><td>Read</td><td>Customer records</td><td></td></tr>
<tr><td>Manager</td><td>Read</td><td>Customer records</td><td>Only records related to business unit</td></tr>
<tr><td>Staff</td><td>Read</td><td>Customer records</td><td>Only records associated with customers assigned by Manager</td></tr>
<tr><td>Customer</td><td>Read</td><td>Customer record</td><td>Only own record</td></tr>
</table>
</td>
</tr>
<tr>
<td>Processus d’enregistrement des utilisateurs</td>
<td>Analyse du processus d’enregistrement des utilisateurs
Vérifier que les exigences d’identité pour l’enregistrement des utilisateurs sont alignées sur les exigences de sécurité à travers la réponse aux questions suivantes :

1. Est-ce que n’importe qui peut s’inscrire pour y accéder ?
2. Les inscriptions sont-elles vérifiées par un humain avant le provisionnement, ou sont-elles automatiquement accordées si les critères sont remplis ?
3. La même personne ou identité peut-elle s’enregistrer plusieurs fois ?
4. Les utilisateurs peuvent-ils s’inscrire pour différents rôles ou autorisations ?
5. Quelle preuve d’identité faut-il pour qu’une inscription aboutisse ?
6. Les identités enregistrées sont-elles vérifiées ?
Puis

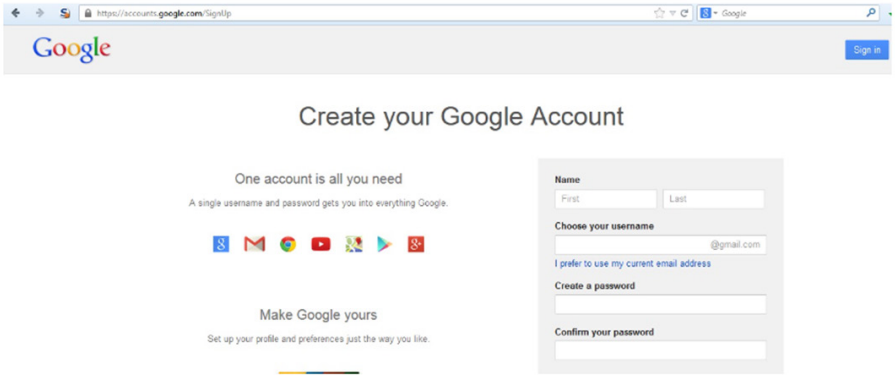
Validez le processus d’inscription :

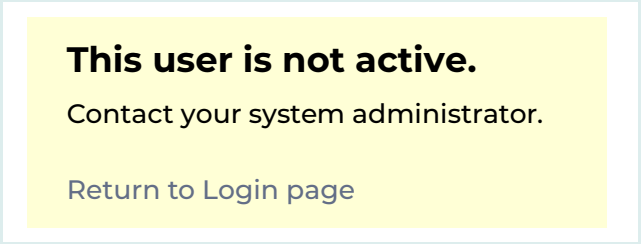
1. Les informations d’identité peuvent-elles être facilement falsifiées ou falsifiées ?
2. L’échange d’informations d’identité peut-il être manipulé lors de l’enregistrement ?

Dans l’exemple WordPress ci-dessous, la seule exigence d’identification est une adresse e-mail accessible au titulaire.</td>
</tr>
</table>



En revanche, dans l'exemple Google ci-dessous, les exigences d'identification incluent le nom, la date de naissance, le pays, le numéro de téléphone portable, l'adresse e-mail et la réponse CAPTCHA. Alors que seulement deux d'entre eux peuvent être vérifiés (adresse e-mail et numéro de téléphone portable), les exigences d'identification sont plus strictes que WordPress.



Enumération des comptes	Analyse des messages de réponse http Test des informations d'identification valides : - Enregistrez la réponse du serveur lorsque vous soumettez un ID utilisateur valide et un mot de passe valide. - À l'aide d'un proxy Web, notez les informations récupérées à partir de cette authentification réussie (réponse HTTP 200, longueur de la réponse). - Tester un nom d'utilisateur inexistant le testeur doit essayer d'insérer un ID utilisateur invalide et un mot de passe erroné et enregistrer la réponse du serveur (le testeur doit être sûr que le nom d'utilisateur n'est pas valide dans l'application). Enregistrez le message d'erreur et la réponse du serveur. Si le testeur saisit un ID utilisateur inexistant, il peut recevoir un message semblable à :  ou un message comme celui-ci : **Login failed for User foo: invalid Account** Généralement, l'application doit répondre avec le même message d'erreur et la même longueur aux différentes requêtes incorrectes. Si les réponses ne sont pas les mêmes, le testeur doit rechercher et trouver la clé qui crée une différence entre les deux réponses. Par exemple : Demande du client : Utilisateur valide/Mot de passe erroné Réponse du serveur : Le mot de passe n'est pas correct Demande client : Mauvais utilisateur/mauvais mot de passe Réponse du serveur : utilisateur non reconnu

Outils :

Exigence	Outils
Validation des rôles	Test manuel de l'existence de la matrice des rôles
Processus d'enregistrement des utilisateurs	HTTP proxy
Enumération des comptes	OWASP Zed Attack Proxy (ZAP) curl PERL

5.3. Protection des paramètres d'authentification

Guide de test :

Exigence	Objectifs de test
Protection des identifiants par un canal crypté	Évaluer si un cas d'utilisation du site Web ou de l'application amène le serveur ou le client à échanger des informations d'identification sans chiffrement.
Identifiants par défaut	Énumérer les applications pour les informations d'identification par défaut Examiner et évaluez les nouveaux comptes d'utilisateurs et s'ils sont créés avec des valeurs par défaut ou des modèles identifiables.
Verrouillage et déverrouillage des comptes	Évaluer la capacité du mécanisme de verrouillage de compte à atténuer la devinette de mot de passe par force brute. Évaluer la résistance du mécanisme de déverrouillage au déverrouillage de compte non autorisé.

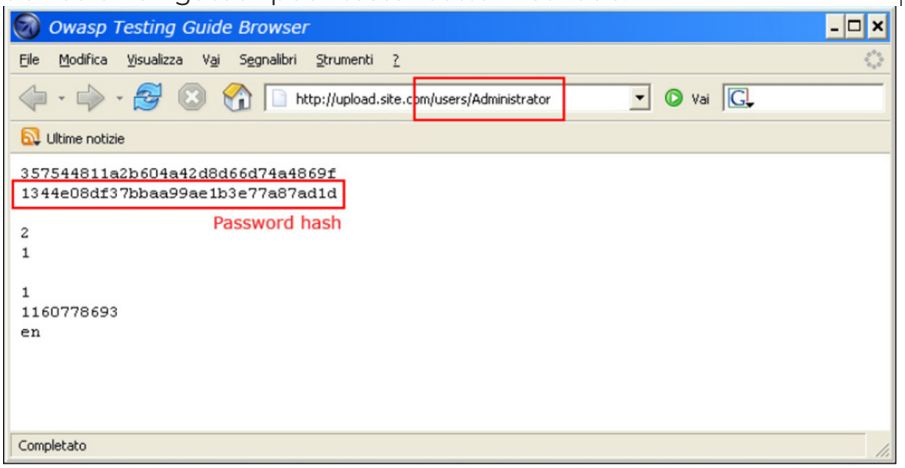
Exigence	Objectifs de test
Contournement des mécanismes d'authentification	Assurer que l'authentification est appliquée à tous les services qui en ont besoin
Exigences liées à la modification ou réinitialisations du mot de passe	Déterminer la résistance de l'application à la subversion du processus de changement de compte permettant à quelqu'un de changer le mot de passe d'un compte. Déterminer la résistance de la fonctionnalité de réinitialisation des mots de passe contre la devinette ou le contournement.

Exemple de test :

Exigence	Exemple de test

Protection des identifiants par un canal crypté	Envoi de données avec la méthode POST via http
	
	Supposons que la page de connexion présente un formulaire avec les champs User, Pass et le bouton Submit pour s'authentifier et donner accès à l'application. Si nous regardons les en-têtes de notre requête avec un proxy Web, nous pouvons obtenir quelque chose comme ceci :
	
	`delegated_service=218&User=test&Pass=test&Submit=SUBMIT`
	`Host: www.example.com`
	`User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; it; rv:1.8.1.14) Gecko/20080404`
	`Accept: text/xml,application/xml,application/xhtml+xml`
	`Accept-Language: it-it,it;q=0.8,en-us;q=0.5,en;q=0.3`
	`Accept-Encoding: gzip,deflate`
	`Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7`
	`Keep-Alive: 300`
	`Connection: keep-alive`
	`Referer: http://www.example.com/index.jsp`
	`Cookie: JSESSIONID=LVrRRQQXgwyWpW7QMnS49vtW1yBdqn98CGlkP4jTvVCGdyPkmn3S!`
	`Content-Type: application/x-www-form-urlencoded`
	`Content-length: 64`
	
	`delegated_service=218&User=test&Pass=test&Submit=SUBMIT`

	À partir de cet exemple, le testeur peut comprendre que la requête POST envoie les données à la page www.example.com/AuthenticationServlet en utilisant HTTP. Ainsi, les données sont transmises sans cryptage et un malveillant l'utilisateur pourrait intercepter le nom d'utilisateur et le mot de passe en reniflant simplement le réseau avec un outil comme Wireshark
Identifiants par défaut	**Test des informations d'identification par défaut des applications courantes** Dans les tests en boîte noire, le testeur ne sait rien de l'application et de son infrastructure sous-jacente. En réalité, ce n'est souvent pas vrai et certaines informations sur l'application sont connues. Nous supposons que vous avez identifié, grâce à l'utilisation des techniques décrites dans ce guide de test sous le chapitre Collecte d'informations, au moins une ou plusieurs applications courantes pouvant contenir des interfaces administratives accessibles. Étant donné que ces types d'identifiants par défaut sont souvent liés à des comptes administratifs, vous pouvez procéder de la manière suivante : Essayez les noms d'utilisateur suivants - « admin », « administrateur », « racine », « système », « invité », « opérateur » ou « super ». Ceux-ci sont populaires parmi les administrateurs système et sont souvent utilisés. De plus, vous pouvez essayer "qa", "test", "test1", "testing" et noms similaires.
Verrouillage et déver-rouillage des comptes	**Teste des mécanismes Verrouillage et déverrouillage des comptes** Un exemple de test peut être le suivant : 1. Essayer de vous connecter 3 fois avec un mot de passe incorrect. 2. Connecter avec succès avec le mot de passe correct, montrant ainsi que le mécanisme de verrouillage ne se déclenche pas après 3 tentatives d'authentification incorrectes.

	Un CAPTCHA peut aussi entraver les attaques par force brute, mais ils peuvent venir avec leur propre ensemble de faiblesses, et ne devraient pas remplacer un mécanisme de verrouillage. Pour évaluer la résistance du mécanisme de déverrouillage au déverrouillage de compte non autorisé, lancer le mécanisme de déverrouillage et chercher les faiblesses. Les mécanismes de déverrouillage typiques peuvent impliquer des questions secrètes ou un lien de déverrouillage envoyé par e-mail.
Contournement des mécanismes d'authentification	**Demande de page directe** Si une application d'e-service implémente le contrôle d'accès uniquement sur la page de connexion, le schéma d'authentification peut être contourné. Par exemple, si un utilisateur demande directement une autre page via la navigation forcée, cette page peut ne pas vérifier les informations d'identification de l'utilisateur avant d'accorder l'accès. Essayez d'accéder directement à une page protégée via la barre d'adresse de votre navigateur pour tester cette méthode. 

Exigences liées à la modification ou réinitialisations du mot de passe	**Test de la procédure du changement et la réinitialisation du mot de passe** Pour le changement et la réinitialisation du mot de passe, il est important de vérifier : ☑ si les utilisateurs, autres que les administrateurs, peuvent modifier ou réinitialiser les mots de passe de comptes autres que les leurs. -si les utilisateurs peuvent manipuler ou subvertir le processus de modification ou de réinitialisation du mot de passe pour modifier ou réinitialiser le mot de passe de un autre utilisateur ou administrateur. ☑ si le processus de modification ou de réinitialisation du mot de passe est vulnérable à CSRF. Vérification du mécanisme de changement/réinitialisation de mot de passes ☑ Vérifier que la question secrète est requise lors de la réinitialisation de mot de passes ☑ Vérifier que le mot de passe réinitialisé est envoyé via l'adresse email utilisée lors de l'inscription ☑ Vérifier l'ancien mot de passe est requis lors du changement du mot de passe

☑ **Outils :**

Exigence	Outils
Protection des identifiants par un canal crypté	☑ OWASP Zed Attack Proxy (ZAP) ☑ mitmproxy ☑ Burp Suite ☑ Wireshark ☑ TCPDUMP

Exigence	Outils
Identifiants par défaut	☑ Burp Intruder ☑ THC Hydra ☑ Nikto 2
Contournement des mécanismes d'authentification	☑ WebGoat ☑ OWASP Zed Attack Proxy (ZAP)

5.4. Protection des Autorisations

☑ **Guide de test :**

Exigence	Outils
Directory traversal	Identifiez les points d'injection qui se rapportent au path traversal Évaluer les techniques de contournement et identifier l'étendue de path traversal
Contournement des autorisations	Vérifier la manière dont le schéma d'autorisation a été implémenté pour chaque rôle ou privilège à accéder aux fonctions et ressources réservées. Évaluer si un accès horizontal ou vertical est possible
Escalassions de privilèges	Identifier les points d'injection liés à la manipulation des privilèges. Essayez de contourner les mesures de sécurité.
Les références d'objet directes non sécurisées	Cartographier tous les emplacements de l'application où l'entrée de l'utilisateur est utilisée pour référencer directement les objets.

Exemple de test :

Exigence	Exemple de test

Directory traversal	**Énumération des vecteurs d'entrée**
	Afin de déterminer quelle partie de l'application est vulnérable au contournement de la validation des entrées,
	le testeur doit énumérer toutes les parties de l'application qui acceptent le contenu de l'utilisateur.
	Cela inclut également les requêtes HTTP GET et POST et les options courantes telles que les téléchargements de fichiers et les formulaires HTML.
	
	Voici quelques exemples de vérifications :
	
	Existe-t-il des paramètres de requête qui pourraient être utilisés pour les opérations liées aux fichiers ?
	
	Existe-t-il des extensions de fichiers inhabituelles ?
	
	Existe-t-il des noms de variables intéressants ?
	
	`http://example.com/getUserProfile.jsp?item=ikki.html`
	`http://example.com/index.php?file=content`
	`http://example.com/main.cgi?home=index.ht`

Exigence	Exemple de test
Directory traversal	Est-il possible d'identifier les cookies utilisés par l'application web pour la génération dynamique de pages ou de templates ? ◦ `Cookie: ID=d9ccd3f4f9f18cc1:TM=2166255468:LM=1162655568:S=3cFpqbJgMSSPKVMV:TEMPLATE=flower` ◦ `Cookie: USER=1826cc8f:PSTYLE=GreenDotRed` **Techniques de test** Analyser les fonctions de validation des entrées présentes dans l'application Web. En utilisant le précédent Par exemple, la page dynamique appelée getUserProfile.jsp charge les informations statiques d'un fichier et affiche le contenu aux utilisateurs. Un attaquant pourrait insérer la chaîne malveillante "../../../../etc/passwd" pour inclure le fichier de hachage de mot de passe d'un Linux/UNIX système. Évidemment, ce type d'attaque n'est possible que si le point de contrôle de validation échoue ; selon le système de fichiers privilèges, l'application Web elle-même doit pouvoir lire le fichier. Exemple : `http://example.com/getUserProfile.jsp?item=../../../../etc/passwd` Un autre exemple courant consiste à inclure du contenu provenant d'une source externe :

<table>
<tr><th>Exigence</th><th>Exemple de test</th></tr>
<tr><td>Directory traversal</td><td>

```
http://example.com/index.php?
file=http://www.owasp.org/malicioustxt
```

</td></tr>
<tr><td>Contournement des autorisations</td><td>Test d'accès aux fonctions d'administration

Par exemple, supposons que la fonction AddUser.jsp fasse partie du menu d'administration de l'application et qu'elle soit possible d'y accéder en demandant l'URL suivante :

<code>https://www.example.com/admin/addUser.jsp</code>

Ensuite, la requête HTTP suivante est générée lors de l'appel de la fonction AddUser :

```
POST /admin/addUser.jsp HTTP/1.1
Host: www.example.com
[other HTTP headers]

userID=fakeuser&role=3&group=grp001
```


Donc il s'agit de vérifier si l'utilisateur a été créé ? Si oui, le nouvel utilisateur peut-il utiliser ses privilèges ?</td></tr>
<tr><td>Escalassions de privilèges</td><td>Manipulation of User Group

Par exemple : le HTTP POST suivant permet à l'utilisateur qui appartient à grp001 d'accéder à la commande #0001 :

```
POST /user/viewOrder.jsp HTTP/1.1
Host: www.example.com
...

groupID=grp001&orderID=0001
```

</td></tr>
</table>

Exigence	Exemple de test
Escalassions de privilèges	Vérifier si un utilisateur qui n'appartient pas à grp001 peut modifier la valeur des paramètres groupID et orderID pour obtenir accès à ces données privilégiées.
Les références d'objet directes non sécurisées	**Scénario de test :** **La valeur d'un paramètre est utilisée directement pour récupérer un enregistrement de base de données** **Exemple de requête :** `http://foo.bar/somepage?invoice=12345` Dans ce cas, la valeur du paramètre facture est utilisée comme index dans une table des factures de la base de données. L'application prend la valeur de ce paramètre et l'utilise dans une requête à la base de données. L'application renvoie alors la facture informations à l'utilisateur. Puisque la valeur de facture va directement dans la requête, en modifiant la valeur du paramètre il est possible de récupérer n'importe quel objet de facture, quel que soit l'utilisateur auquel appartient la facture. Pour tester ce cas, le testeur doit obtenir l'identifiant d'une facture appartenant à un autre utilisateur de test (garantissant qu'il n'est pas censé consulter cette information par logique métier de l'application), puis vérifier s'il est possible d'accéder aux objets sans autorisation.

Outils :

Exigence	Outils
Directory traversal	DotDotPwn - The Directory Traversal Fuzzer Path Traversal Fuzz Strings (from WFuzz Tool) OWASP ZAP Burp Suite Encoding/Decoding tools String searcher “grep” DirBuster
Contournement des autorisations	OWASP Zed Attack Proxy (ZAP)
Escalassions de privilèges	OWASP Zed Attack Proxy (ZAP)

5.5. Gestion des sessions

Guide de test :

Exigence	Objectifs de test
Gestion des variables des cookies	Tester les configurations de sécurité des cookies
Fixation des sessions	Analysez le mécanisme d'authentification et son déroulement. Forcer les cookies et évaluer l'impact.

Exemple de test :

Exigence	Exemple de test
Gestion des variables des cookies	**Vérifier l'utilisation des attributs sécurisés des Cookies** Attribut Secure L'attribut Secure indique au navigateur de n'envoyer le cookie que si la demande est envoyée via un canal sécurisé tel que comme HTTPS. Cela aidera à empêcher le cookie d'être transmis dans des requêtes non chiffrées. Si la demande peut être accessible via HTTP et HTTPS , un attaquant pourrait être en mesure de rediriger l'utilisateur pour envoyer son cookie dans le cadre de requêtes non protégées. Attribut HttpOnly L'attribut HttpOnly est utilisé pour aider à prévenir les attaques telles que les fuites de session, car il ne permet pas au cookie de accessible via un script côté client tel que JavaScript. Attribut Domain L'attribut Domain est utilisé pour comparer le domaine du cookie avec le domaine du serveur pour lequel le HTTP demande est en cours. Si le domaine correspond ou s'il s'agit d'un sous-domaine, l'attribut de chemin sera ensuite vérifié.

Fixation des sessions	**Test des vulnérabilités de fixation de session**
	La première étape consiste à faire une requête au site à tester (par exemple www.example.com). : `GET www.example.com`
	
	La réponse est la suivante :
	`HTTP/1.1 200 OK`
	`Date: Wed, 14 Aug 2008 08:45:11 GMT`
	`Server: IBM_HTTP_Server`
	`Set-Cookie: JSESSIONID=0000d8eyYq3L0z2fgq10m4v-rt4:-1; Path=/; secure`
	`Cache-Control: no-cache="set-cookie,set-cookie2"`
	`Expires: Thu, 01 Dec 1994 16:00:00 GMT`
	`Keep-Alive: timeout=5, max=100`
	`Connection: Keep-Alive`
	`Content-Type: text/html;charset=Cp1254`
	`Content-Language: en-US`

Exigence	Exemple de test

Fixation des sessions	L'application définit un nouvel identifiant de session JSESSIONID =0000d8eyYq3L0z2fgq10m4v-rt4:-1 pour le client.
	Ensuite, s'authentifier auprès de l'application avec le POST HTTPS suivant :
	 
	
	La réponse est la suivante :
	`HTTP/1.1 200 OK`
	`Date: Thu, 14 Aug 2008 14:52:58 GMT`
	`Server: Apache/2.2.2 (Fedora)`
	`X-Powered-By: PHP/5.1.6`
	`Content-language: en`
	`Cache-Control: private, must-revalidate, max-age=0`
	`X-Content-Encoding: gzip`
	`Content-length: 4090`
	`Connection: close`
	`Content-Type: text/html; charset=UTF-8`
	`...`
	`HTML data`
	`...`
	Comme aucun nouveau cookie n'a été émis après une authentification réussie, donc il est possible d'effectuer détournement de session.
	Envoyer un identifiant de session valide à un utilisateur (éventuellement en utilisant une astuce d'ingénierie sociale), attendre qu'il s'authentifier, puis vérifier que des privilèges ont été attribués à ce cookie.

Outils

Exigence	Outils
Gestion des variables des cookies	•Intercepting Proxy : OWASP Zed Attack Proxy Project, Web Proxy Burp Suite •Browser Plug-in : Tamper Data for FF Quantum “FireSheep” for FireFox “EditThisCookie” for Chrome “Cookiebro - Cookie Manager” for FireFox
Fixation des sessions	JHijack - a numeric session hijacking tool OWASP ZAP

5.6. Validation des Inputs

Guide de test :

Exigence	Objectifs de test
Validation des saisies	Identifier : Le backend et les méthodes de parsing utilisées. les différentes possibilités d’injection et tester les méthodes de Bypass des mécanismes de filtrage. les contrôles implémentés et l’encodage des données saisies

Exemple de test :

Exigence	Exemple de test
Validation des saisies	Une attaque par SQL injection consiste en l'insertion ou «l'injection» d'une requête SQL partielle ou complète via les données saisies et transmises du client (navigateur) à l'application d'e-services. En considérant la requête suivante : SELECT * FROM Users WHERE Username='$username' AND Password='$password' Si un utilisateur saisie les données suivantes au niveau de l'application, username = 1' or '1' = '1 password = 1' or '1' = '1 La requête sera comme suit : SELECT * FROM Users WHERE Username='1' OR '1' = '1' AND Password='1' OR '1' = '1' Cette requête sera toujours traitée puisqu'elle retournera toujour la valeur TRUE

Outils :

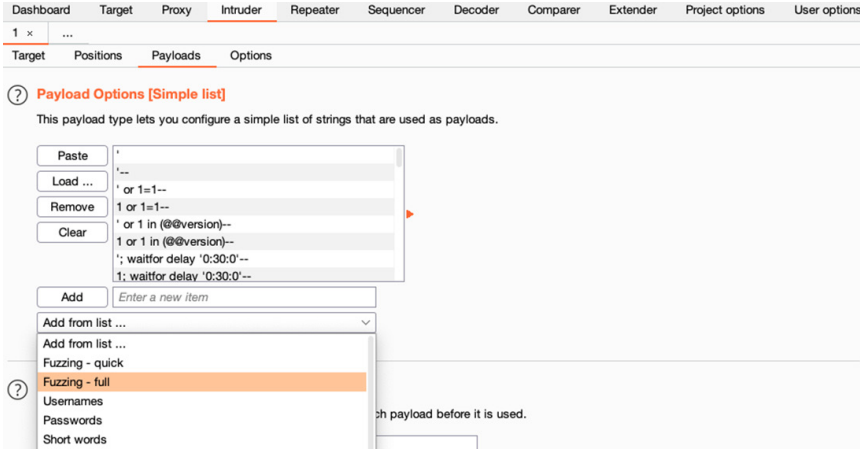
Exigence	Outils
Validation des saisies	Fuzzdb, SQLMAP, MySqloit PHP Charset Encoder, Hackvertor, XSS-Proxy, BeEF, Burp Proxy, Zed Attack Proxy (ZAP) Softerra LDAP Browser, XML Injection Fuzz Strings, kadimus, LFI Suite OWASP WebGoat, Metasploit, TCPProxy, WireShark

5.7. Gestion des erreurs

Guide de test :

Exigence	Objectifs de test
Sécurité des informations au niveau des messages d'erreurs	Analyser les différents messages qui sont retournés par l'application en se focalisant sur les messages d'erreurs qui révèlent des informations sensibles.

Exemple de test :

Exigence	Exemple de test
Sécurité des informations au niveau des messages d'erreurs	Amener les systèmes à générer des erreurs non gérées et afficher des messages qui révèles des données sensibles comme le type et la version du serveur, de service ou l'application utilisés Pour générer des messages d'erreur, il faut : ☑ Rechercher des fichiers et dossiers aléatoires qui ne seront pas trouvés (des pages avec le code 404) ☑ Essayez d'accéder à des pages qui existent et analyser le comportement du serveur (des pages avec le code 403, page vierge ou liste de répertoires). ☑ Modifier les données des requêtes http. ☑ Tester tous les points de saisie de données avec outils automatique (FUZZING) 

Outils :

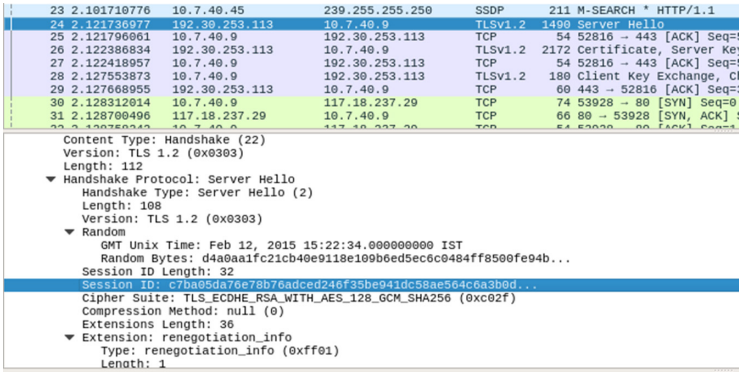
Exigence	Outils
Sécurité des informations au niveau des messages d'erreurs	Burp Proxy, ZAP

5.8. Gestion des moyens cryptographiques

Guide de test :

Exigence	Objectifs de test
Sécurité des communications	Tester la validité des certificats et des forces des algorithmes de chiffrement utilisés la possibilité de contourner les moyens de chiffrements utilisés
Sécurité des informations envoyées sur des canaux chiffrés	Identifier les différents canaux de transmissions chiffrées Evaluer le niveau de sécurité des moyens de chiffrements utilisés
Vulnérabilité des moyens cryptographique	Identifier les vulnérabilités connues dans les protocoles de chiffrement utilisés

Guide de test :

Exigence	Exemple de test
Sécurité des communications	Tester les vulnérabilités les plus courantes qui touchent les protocoles de chiffrements utilisées : Debian OpenSSL Predictable Random Number Generator (CVE-2008-0166) OpenSSL Insecure Renegotiation (CVE-2009-3555) OpenSSL Heartbleed (CVE-2014-0160) F5 TLS POODLE (CVE-2014-8730) Microsoft Schannel Denial of Service (MS14-066 / CVE CVE-2014-6321)
Sécurité des informations envoyées sur des canaux chiffrés	Vérifier que des protocoles sécurisés pour le cheminement des informations sont utilisés Vérifier que toutes les informations confidentielles sont chiffrées au niveau des requêtes http et cookies L'exemple suivant montre que la session ID est envoyée sans chiffrement au niveau du cookie 

Vulnérabilité des moyens cryptographique	Tester les vulnérabilités les plus courantes qui touchent les protocoles de chiffrements utilisées : ☑ Debian OpenSSL Predictable Random Number Generator (CVE-2008-0166) ☑ OpenSSL Insecure Renegotiation (CVE-2009-3555) ☑ OpenSSL Heartbleed (CVE-2014-0160) ☑ F5 TLS POODLE (CVE-2014-8730) Microsoft Schannel Denial of Service (MS14-066 / CVE CVE-2014-6321)

☑ **Outils :**

Exigence	Outils
Sécurité des communications	☑ Nmap (plusieurs scripts) ☑ OWASP O-Saft ☑ sslscan ☑ sslyze ☑ SSL Labs ☑ testssl.sh
Sécurité des informations envoyées sur des canaux chiffrés	☑ curl ☑ grep ☑ Identity Finder ☑ Wireshark ☑ TCPDUMP
Vulnérabilité des moyens cryptographique	☑ Nmap (plusieurs scripts) ☑ Nessus ☑ OpenVAS ☑ Fortify

5.9. Gestion du logique métier

Guide de test :

Exigence	Objectifs de test
Validation des données	L'objectif des tests est d'identifier : les différents champs de saisie possible les contrôles qui peuvent être bypassé et/ou qui ne sont pas validés du côté du serveur. le comportement lors de la saisie de données non valide.
Intégrité des données	Identifier des champs ou des fonctionnalités cachées ou protégés et manipuler les données qui y sont stockés Tester la possibilité d'exécuter des fonctionnalités qui ne sont pas permise comme d'insérer, mettre à jour, ou supprimer des enregistrements.
Gestion des temps de réponse	Identifier les processus qui demandent un temps d'exécution plus long que d'autre générant ainsi un mauvais comportement de l'application
Gestion des fichiers téléchargés	Vérifier que application implémente un contrôle sur les fichiers qui sont uploadés. Valider l'efficacité des contrôles mis en place

Exemple de test :

Exigence	Exemple de test
Validation des données	Intercepter les requêtes en utilisant un proxy et tenter de modifier les données valides par d'autres données non valides pour vérifier qu'ils sont contrôlés du côté serveur

Exigence	Exemple de test
Intégrité des données	À l'aide d'un proxy, Analyser les requêtes POST/GET à la recherche d'indications de champs protégés ou fonctionnalités cachées. Manipuler les données pour amener l'application à donner une réponse ou un comportement diffèrent.
Gestion des temps de réponse	Tester l'existence de processus qui s'exécutent entre deux autres processus qui demandent un temps d'exécution plus long et qui permettent de contourner les contrôles et les mesures de sécurité implémentés.
Gestion des fichiers téléchargés	Vérifier que : L'application n'accepte que les types de fichier qui sont approuvés Les contrôles sur les fichiers sont refaits au niveau du serveur L'application contrôle le paramètre «Content-Type» dans la requête http. L'application contrôle les extensions des fichiers. Les fichiers téléchargés ne sont pas directement accessibles par une adresse URL

- **Outils :**

Exigence	Outils
Validation des données	OWASP Zed Attack Proxy (ZAP)
Intégrité des données	OWASP Zed Attack Proxy (ZAP) Burp Suite
Gestion des temps de réponse	OWASP Zed Attack Proxy (ZAP) Burp Suite
Gestion des fichiers téléchargés	OWASP Zed Attack Proxy (ZAP) Burp Suite

5.10. Validation des données coté clients

Guide de test :

Exigence	Objectifs de test
Exigence liées DOM-Based Cross Site Scripting	Identifier les scripts qui manipulent des objets dans le but de les modifier et lancer des attaques
Exécution des scripts	Identifier les points possibles d'injection de script au niveau des pages
Injection HTML, CSS	Identifier les possibilités d'injection du code HTML dans les scripts
Client-side URL Redirect and Ressources manipulation	Localiser les points d'injection des URL ou des chemins dans le but de créer des redirections vers des sites malicieux
Accès aux ressources partagées	Identifier les ressources partagé qui sont utilisé par l'E-service et exploiter les erreurs de configuration
Vol des clicks	Vérifier la possibilité de contourner les mesures de sécurité implémentées et afficher des pages Web dans d'autres pages Web via des cadres
Websocket	Identifier les erreurs de configurations et de paramétrages qui peuvent être exploitées
Sauvegarde des clients	Déterminer si le site Web stocke des données sensibles du côté client Identifier les possibilités d'attaques par injection, l'utilisation de composante vulnérable ou un manque de contrôle

Exemple de test :

Exigence	Exemple de test
Exigence liées DOM-Based Cross Site Scripting	**Le code JavaScript qui suit modifie l'attribut href d'un élément** $(function() { $('#backLink').attr('href',(new URLSearchParams(window.location.search)).get('returnUrl')); }); Le test consiste à modifier l'URL afin que le lien location.search contienne un code malveillant qui renvoie des informations sensibles : ?returnUrl=javascript:alert(document.domain)

Exécution des scripts	**Identifier les scripts qui peuvent être manipulés, le script suivant est vulnérable :**
	<script>
	function loadObj(){
	var cc=eval('('+aMess+')');
	document.getElementById('mess').textContent=cc.message;
	}
	
	if(window.location.hash.indexOf('message')==-1) {
	var aMess='({«message»:»Hello User!»})';
	} else {
	var aMess=location.hash.substr(window.location.hash.indexOf('message=')+8)
	}
	</script>
	Le paramètre location.hash peut être manipulé pour injecter un script qui révèle des données sensible ou prendre contrôle du navigateur.

Exigence	Exemple de test

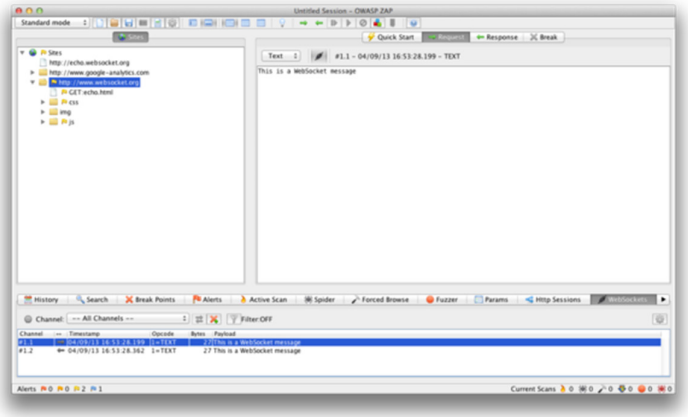
Injection HTML, CSS	**Analyser le code source des pages dans le bus de retrouver des scripts vulnérables. Le code qui suit peut etre manipulé de la façon à pouvoir injecter du code HTML**
	
	<script>
	
	function setMessage(){
	
	var t=location.hash.slice(1);
	
	$(«div[id=»+t+»]»).text(«The DOM is now loaded and can be manipulated.»);
	
	}
	
	$(document).ready(setMessage);
	
	$(window).bind(«hashchange»,setMessage)
	
	</script>
	
	<body>
	
	<script src=»../js/embed.js»></script>
	
	 Show Here Showing Message1
	
	 Show Here Showing Message2
	
	 Show Here Showing Message3
	
	</body>

Exigence	Exemple de test

Client-side URL Redirect and Ressources manipulation	**Identifier au niveau des scripts les redirections qui sont implémentées et manquent de contrôles**
	Le code suivant est un exemple de code vulnérable :
	var redir = location.hash.substring(1);
	if (redir) {
	window.location='http://'+decodeURIComponent(redir);
	}
	Le test consiste donner une modifier la valeur de redir en y mettant l'URL d'un site malicieux.

Accès aux ressources partagées	**Intercepter les requetés et les réponses du serveur dans le but de les analyser et localiser les erreurs de configuration dans l'utilisation les ressource partagés** L'exemple suivant montre une mauvaise configuration au niveau de la réponse du serveur qui donne des accès aux ressources sans limitation des origines de la requête : HTTP/1.1 200 OK [...] Access-Control-Allow-Origin: * Content-Length: 4 Content-Type: application/xml

Exigence	Exemple de test
Vol des clicks	**Analyser les codes sources des pages du e-service à fin de localiser celles qui peuvent être chargés dans un iframe le code suivant peut etre utilser dans lea mise en œuvre du test.** <html> <head> <title>Clickjack test page</title> </head> <body> <iframe src=»http://www.target.site» width=»500» height=»500»></iframe> </body> </html> Tester la possibilité de faire un bypass des protections implémentés est l'utilisation d'un proxy qui modifie l'entête de la page ce qui désactive les protections contre les vols de clicks.
Websocket	Identifier les erreurs de configurations et de paramétrages qui peuvent être exploitées
Sauvegarde des clients	Déterminer si le site Web stocke des données sensibles du côté client Identifier les possibilités d'attaques par injection, l'utilisation de composante vulnérable ou un manque de contrôle

Exigence	Exemple de test
Vol des clicks	**Analyser les codes sources des pages du e-service à fin de localiser celles qui peuvent être chargés dans un iframe le code suivant peut etre utilser dans lea mise en œuvre du test.** <html> <head> <title>Clickjack test page</title> </head> <body> <iframe src=»http://www.target.site» width=»500» height=»500»></iframe> </body> </html> Tester la possibilité de faire un bypass des protections implémentés est l'utilisation d'un proxy qui modifie l'entête de la page ce qui désactive les protections contre les vols de clicks.
Websocket	Tester les connexions web socket en utilisant un web proxy pour intercepter les requêtes et les réponses du serveur et lancer des attaques sur les différents paramètres. 

Exigence	Exemple de test
Sauvegarde des clients	Lister et analyser l'ensemble des cookies au niveau du client dans le but de retrouver des variables de session, des mots de passes, chemin d'accès,... Le code suivant peut etre utilisé pour lister les cookies au niveau du client : console.log(window.document.cookie);

Outils :

Exigence	Outils
Exigence liées DOM-Based Cross Site Scripting	Burp Proxy, DOMinator
Exécution des scripts	Burp Proxy, ZAP
Injection HTML, CSS	Burp Proxy, ZAP
Client-side URL Redirect and Ressources manipulation	Burp Proxy, ZAP
Accès aux ressources partagées	Burp Proxy, ZAP
Vol des clicks	Burp Proxy, ClickjackingTool
Websocket	OWASP Zed Attack Proxy (ZAP) WebSocket Client Google Chrome Simple WebSocket Client
Sauvegarde des clients	Chrome, Firebug, Burp Proxy, ZAP

3.4.3. ANNEXE 3 : GUIDE SUR LA METHODE SECURITY BY DESIGN DANS LE DEVELOPPEMENT DES APPLICATIONS DE SERVICES EN LIGNE

1. Objectifs :

Le présent guide constitue un référentiel de base pour présenter le processus permettant l'intégration du principe Security By Design dans toutes les étapes des projets de développement.

2. Définitions :

Security By Design (SBD) : Une approche qui consiste à prendre en considération tous les aspects de sécurité lors du processus permettant la fourniture d'un bien ou d'un service.

SDLC : est le processus global de développement de systèmes, de l'initiation à la mise en œuvre jusqu'à l'élimination. De nombreuses activités sont associées à chaque phase du SLDC. Bien que les activités réalisées dans chaque projet de développement de systèmes puissent varier, un SDLC typique commence par un besoin métier et se termine lorsque les coûts de maintenance l'emportent sur les avantages du système, d'où un « cycle de vie ».

Agile Development Lifecycle : Agile Development Lifecycle décrit un ensemble de principes pour le développement de systèmes selon lesquels les exigences et les solutions évoluent grâce à l'effort collaboratif d'équipes interfonctionnelles et autoorganisées. Il apparaît comme un besoin de développer des itérations rapides de systèmes de travail pour les utilisateurs qui ont des exigences et des priorités changeantes.

3. Vision des acteurs d'un projet :

Dans le cadre d'un projet de développement, plusieurs acteurs sont impliqués dans le cadre du processus de développement. Plusieurs problématiques se posent. L'intégration de la sécurité dans les projets permet d'apporter des réponses à ces différents acteurs.
Le tableau ci-dessous permet de définir les problématiques et les besoins exprimés par les différents acteurs dans le cadre des projets :

Acteurs	Problématiques	Besoins
Client	Le client est confronté aux enjeux suivants : ☑ Changement du contexte d'utilisation ☑ Environnement technologique de plus en plus complexe ☑ Maintenance VS Sécurité ☑ Analyse de l'impact d'une nouvelle application d'e-services sur l'activité ☑ Conformité au contexte juridique et business Le focus est principalement porté sur la partie fonctionnelle impliquant : ☑ Peu de contrôle sur les applications d'e-services ☑ Peu d'exigences de sécurité dans les appels d'offres ☑ Peu de clauses de sécurité dans les contrats	Le client a besoin d'outils / de démarche pour spécifier ses exigences de sécurité dès le début du projet et pour assurer le suivi pendant tout le cycle de vie.
Fournisseur	Le fournisseur est confronté à : ☑ Peu d'activités de sécurité dans les méthodes de développement ☑ Peu de contrôles de sécurité (bonnes pratiques) ☑ Peu de tests de sécurité ☑ Absence de critères formels et vérifiables ☑ Absence d'un processus répétable pour appliquer la sécurité dans un projet ☑ La sécurité d'une application d'e-servies dépend de la compétence de chaque équipe	Le fournisseur a besoin de connaitre les exigences afin de les prendre en considération et de fournir un produit conforme
Auditeur	L'auditeur est confronté : ☑ Difficulté à définir l'application d'-e-services et à délimiter la portée de l'évaluation ☑ Absence de processus d'évaluation adéquat ☑ Peu de similitude entre les projets d'évaluation	L'auditeur a besoin d'outils pour évaluer la sécurité d'une application d'e-services ☑ Processus ☑ Méthodologie ☑ Contrôles (critères)

4. Principes à respecter :

L'approche SBD devrait respecter les principes de bases suivants :

Principes à respecter	Description
Approche intégrée	L'approche SBD garantit que les considérations de sécurité sont prises en compte à chaque phase des processus du cycle de vie de la sécurité. Les activités au sein de ces processus de sécurité se concentrent sur l'ajout d'éléments de sécurité qui devraient être présents dans toutes les méthodologies SDLC.
Intégration dès le début du projet	Les processus SBD commencent tôt dans la phase SDLC et sont importants pour façonner les capacités de sécurité et la posture du système informatique tout au long des phases SDLC. Si ces processus ne sont pas exécutés de manière adéquate à chaque phase du SDLC, ils peuvent être plus coûteux à mettre en œuvre ultérieurement.
Approche processus et répétitif	Chaque processus peut être répété si le résultat n'est pas satisfaisant et s'il y a des changements importants dans le projet, la sécurité du projet doit être réévaluée dès la phase de lancement.
Framework à définir au niveau de l'entreprise	Une cadre de référence SBD (Framework) doit fournir une approche disciplinée et structurée qui intègre les processus de sécurité dans le SDLC. Ce cadre de référence doit montrer une relation hiérarchique entre les processus, les activités et les points de contrôle.
Approche basée sur le risque	De plus, le cadre exige que les risques soient continuellement gérés au moyen d'un cadre de gestion des risques. Pour que l'approche SBD soit efficace, les organisations doivent avoir une approche des risques cohérente et efficace appliquée à tous les processus de sécurité. Le cadre de gestion des risques peut faire partie d'un programme de gestion des risques à l'échelle de l'organisation qui implique la gestion des risques organisationnels ; c'est-à-dire le risque pour l'organisation associé au fonctionnement d'un système informatique.

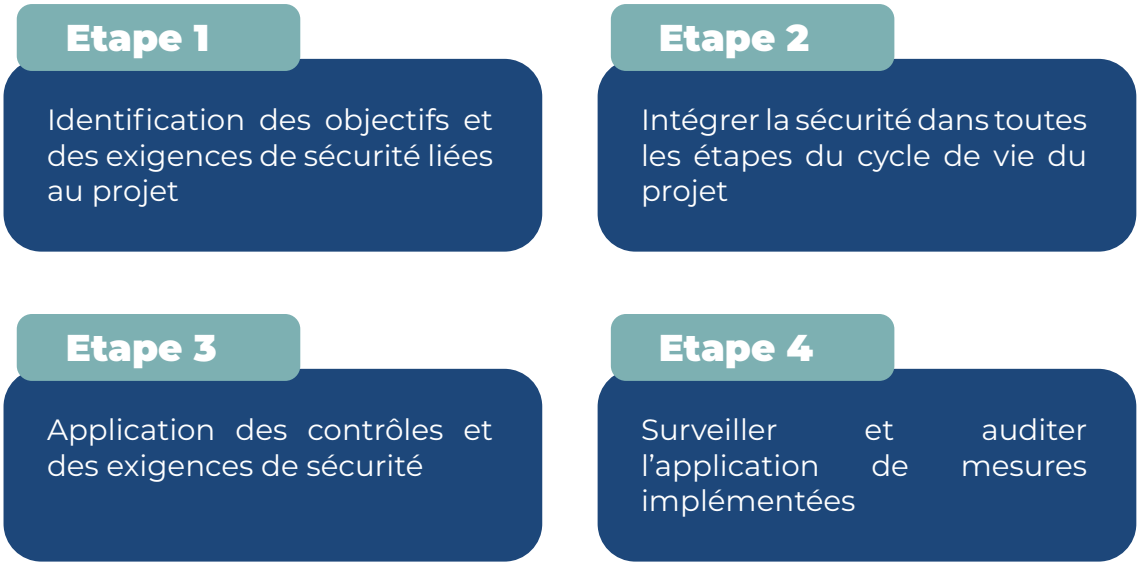
5. Fondements de l'approche :

L'approche SBD se compose de trois composantes, à savoir :

- **Cycle de vie** - Alignement des processus liés à la sécurité avec SDLC pour guider les projets afin d'atteindre les objectifs de sécurité dès la conception ;
- **Activités** - Activités liées à la sécurité qui prennent en charge les processus du cycle de vie de la sécurité ;
- **Contrôles** - Un moment où l'effort de développement du système sera évalué pour la sécurité et quand la direction déterminera si le projet doit continuer tel quel, changer de direction ou être interrompu.

Ainsi, l'approche Security By Design permet de s'assurer qu'au niveau des différentes étapes de développements du projet, la sécurité est prise en considération. L'identification des besoins en termes de sécurité est associée à l'identification des risques liés au développement et la mise en exploitation du projet.

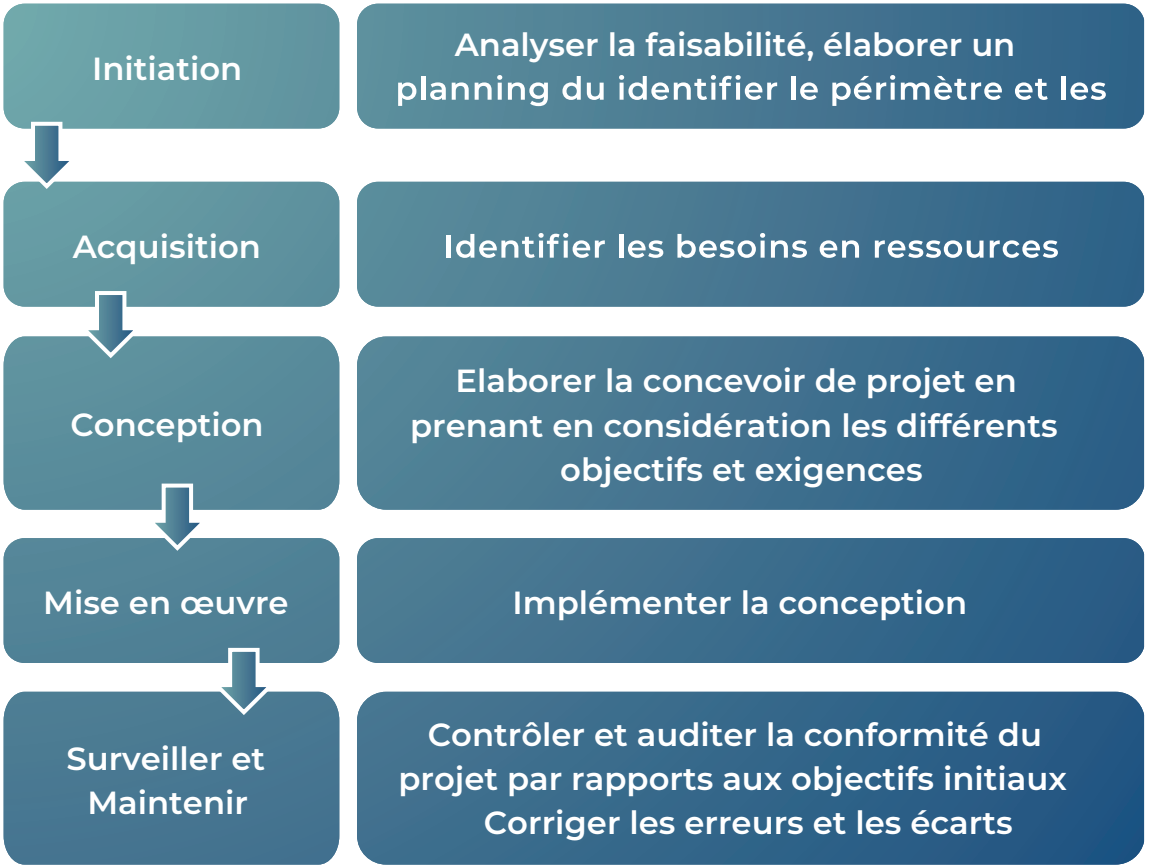
L'approche Security By Design se compose en quatre étapes essentielles tel que présenté dans la figure ci-dessous. La mise en œuvre de l'approche nécessite la définition et l'implémentation d'un processus respectant ces différentes étapes et objectifs.



6. Description du processus

6.1. Cycle de vie d'un projet

Dans le cadre de son cycle de vie, un projet passe par les étapes suivantes :



Dans un cycle standard, les processus et contrôle de sécurité ne sont pas clairement définies. Ainsi, afin d'assurer l'intégration de la sécurité dans le projet, nous serons amenés à définir :

- Les processus de sécurités à prévoir ;
- Les contrôles de sécurités à réaliser afin de vérifier l'application des règles.

6.2. Intégration de la Security By Design dans les projets

De ce fait, le processus permettant l'intégration de la sécurité dans les projets se présente comme suit :

Cycle de vie d'un projet	Processus Security By Design	Livrables
Initiation	• Identifier des objectifs liés à la sécurité • Analyse des risques	• Listes des objectifs et besoin en sécurité • Inventaire des risques liés au projet
Acquisition	• Formalisation des contrôles et exigences a au niveau des plateformes et services en se basant sur des standards	• Liste des contrôles pour la vérification
Conception	• Contrôle de la conformité de la partie conceptuelle avec les exigences et les contrôle de sécurité. • Mise à jour de l'analyse des risques	• Liste des contrôles pour la vérification • Inventaire des risques mise à jour
Mise en œuvre	• Analyse statique et dynamique des codes sources • Conduite de pentest	• Liste des vulnérabilités identifiées • Plan d'action pour la remédiation
Surveiller et Maintenir	• Auditer et surveiller les applications	• Rapports d'audit et de conformité • Plan d'action pour l'amélioration

Un ensemble de processus seront ainsi intégrés au cycle de vie d'un projet. Dix processus ont été identifiés se présentant comme suit :

Phases	Initiation	Acquisition	Design / Développement	Implémentation / évaluation	Opérationnel / Maintenance	Destruction
Processus à mettre en œuvre	Planification de la sécurité	Exigences de sécurité à formaliser	Revue de la conception sécurisé	Test de sécurité applicatif	Audit continue	Destruction sécurisé
	Appréciation de risque	Evaluation de / des proposition technique		Test / acceptation de sécurité du système	Surveillance continue	
				Pentest / audit intrusif		

L'ensemble de ces processus sont détaillés en un ensemble d'activités se présentant comme suit :

Phase d'initialisation

Phase	**Initiation**	
Processus	Planification de la sécurité	Appréciation de risque
Activités	Planification de la sécurité	Appréciation des risques et menaces Classification du système
Points de contrôles	L'autorité approbatrice pour cette phase est le Comité sécurité. Les validations de contrôle recommandées pour cette phase incluent : ☑ Rapport d'évaluation des menaces et des risques approuvés par le comité directeur. C'est le principal livrable de cette phase. Il sera largement utilisé pour développer les exigences de sécurité, les contrôles et la conception du système. ☑ Vérifier si toutes les exigences de sécurité de haut niveau ont été incluses ou exprimées sous la forme d'un ensemble de contrôles de sécurité dans le rapport d'évaluation des menaces et des risques. ☑ Vérifier si les rôles et les responsabilités de l'équipe de sécurité ont été établis. ☑ Évaluer si le projet est pris en charge avec les ressources de sécurité actuellement disponibles ou projetées d'être disponibles dans les délais souhaités.	

Phase d'acquisition

Phase	Acquisition	
Processus	Exigences de sécurité à formaliser	Evaluation de / des proposition technique
Activités	Définir les exigences de sécurité à intégrer au niveau du Cahier des charges	Evaluation des spécifications techniques et leurs adéquations avec le niveau de sécurité requis
Points de contrôles	L'objectif de ce point de contrôle est de faire correspondre les exigences de sécurité exprimées aux fonctionnalités de sécurité définies par les fournisseurs. Tous les contrôles de sécurité doivent être inclus dans la proposition du fournisseur. L'autorité approbatrice du point de contrôle est le comité de pilotage. Les validations de contrôle recommandées pour cette phase incluent : ☑ Tous les contrôles de sécurité convenus ont été inclus dans la proposition du fournisseur. ☑ Les activités et les résultats prévus du fournisseur sont conformes à la politique et aux procédures de sécurité de l'organisation. ☑ Acceptation formelle des risques par les principales parties prenantes sur la base de la proposition du fournisseur.	

Phase d'acquisition

Phase	Acquisition
Processus	Revue de la conception sécurisé
Activités	Revue de l'architecture sécurisé Revue des contrôles de sécurité
Points de contrôles	Avant le développement du système, la conception et les contrôles de sécurité proposés doivent être validés et acceptés par les principales parties prenantes. Les mises à jour et les modifications apportées à l'évaluation initiale des risques doivent être mises à jour pour refléter les modifications apportées aux exigences de sécurité et à la conception. Les validations de contrôle recommandées pour cette phase incluent : ☑ La conception du système est cohérente avec l'architecture de l'entreprise, y compris les composants de sécurité de cette architecture. ☑ La conception du système répond aux exigences de sécurité convenues. ☑ Le rapport de traitement de risque reflète les risques mis à jour après examen de l'architecture de sécurité et des contrôles de sécurité mis en place. ☑ Les principales parties prenantes ont officiellement accepté la conception du système proposé en tenant compte du rapport d'évaluation des menaces et des risques mis à jour.

Phase d'implémentation et d'évaluation :

Phase	**Implémentation / évaluation**		
Processus	Test de sécurité applicatif	Test / acceptation de sécurité du système	Pentest / audit intrusif
Activités	Réaliser une revue du code source Réaliser un test de sécurité applicatif	Réaliser un test de sécurité sur la plateforme	Réaliser un test intrusif externe et interne
Points de contrôles	Dans la phase de mise en œuvre, le système est construit et testé. Les principales parties prenantes s'appuient sur les résultats des tests de sécurité pour évaluer si les contrôles de sécurité mis en place sont efficaces. L'autorité approbatrice de ce point de contrôle est le Comité de Pilotage. Les validations de contrôle recommandées pour cette phase incluent : ☑ Les contrôles de sécurité définis par les exigences convenues sont correctement mis en œuvre dans le système. ☑ Les mesures d'atténuation découlant des rapports d'examen du code source, des rapports de test de sécurité et des rapports de test de pénétration sont traitées, les risques acceptés et formellement approuvés par le comité de pilotage. ☑ Les utilisateurs sont correctement formés aux composants de sécurité des systèmes.		

Phase d'opérationnalisation et de maintenance :

Phase	**Opérationnel / Maintenance**	
Processus	Audit continue	Surveillance continue
Activités	Réaliser une revue sécurité continue Réaliser une revue de la configuration continue	Assurer un suivi des changements Assurer une surveillance continue des vulnérabilités et des événements
Points de contrôles	Dans cette phase, tout en utilisant le système, nous réévaluons son statut en fonction des commentaires des utilisateurs, des changements technologiques, des changements de politique, des nouvelles menaces et vulnérabilités et d'autres problèmes liés à l'entreprise. L'autorité approbatrice pour ce point de contrôle est le propriétaire du système. Les validations de contrôle recommandées pour cette phase incluent : ☑ Validation des revues de sécurité pour s'assurer que les contrôles intégrés restent efficaces et rapport des résultats au comité de pilotage. ☑ Validation des rapports d'évaluation et d'examen de la sécurité pour s'assurer que les systèmes et les changements environnementaux sont pris en compte. ☑ Examen régulier des rapports d'appréciation de risque et du registre des risques pour s'assurer que les risques restent valables et sont continuellement traités.	

Phase de destruction :

Phase	Destruction
Processus	Destruction sécurisé
Activités	Préserver l'information Destruction des médias Destruction des hardwares et softwares
Points de contrôles	Dans la phase d'élimination / destruction, la principale préoccupation est que le système soit terminé de manière ordonnée et que les informations vitales sur le système soient préservées conformément aux réglementations et politiques de gestion des enregistrements applicables pour un accès futur. Tous les supports reçoivent la méthode de désinfection appropriée et enfin le matériel et les logiciels sont éliminés conformément à la politique. L'autorité approbatrice de ce point de contrôle est le propriétaire du système. Les validations de contrôle recommandées pour cette phase incluent : ☑ Les informations de validation du système ont été correctement conservées et correspondent à la bonne classification de sécurité. ☑ Valider que les enregistrements de nettoyage des supports ont été correctement enregistrés et classés. ☑ Validation des enregistrements d'élimination par rapport à l'inventaire matériel/ logiciel réel.

3.4.4. ANNEXE 4 : GUIDE TECHNIQUE DE DURCISSEMENT D'UN SERVEUR WEB IIS

Introduction

Ce guide fournit des conseils prescriptifs pour établir une posture de configuration sécurisée pour Microsoft IIS 10.

Le serveur IIS disponible en tant que serveur web sur les serveurs Windows, est également l'une des plates-formes de serveur Web les plus utilisées sur Internet. Le renforcement de la sécurité du serveur d'IIS implique l'application de certaines de configuration avancée qui sont au-delà des paramètres par défaut. Les paramètres par défaut sur IIS offrent un minimum de fonctionnalités et de sécurité.

Lors du durcissement d'une application d'e-services IIS, il est recommandé de passer en revue chaque contrôle et de déterminer son adéquation à votre déploiement existant. Quelle que soit la stratégie de durcissement, il est recommandé d'adopter une approche progressive, en appliquant et en testant chaque nouveau contrôle de sécurité dans un environnement de développement ou de test avant de le déployer dans un environnement de production. Aussi merveilleux qu'il soit d'avoir un déploiement sécurisé, ce n'est pas si merveilleux si l'application d'e-services que votre serveur IIS héberge ne fonctionne plus parce que vous avez tout rendu un peu trop sécurisé.

1. Recommandations

1.1. Configurations de base

Cette section contient des recommandations de base au niveau d'une application d'e-services IIS.

Règle 1 : Assurez-vous que le contenu Web se trouve sur une partition non-système

Description : Les ressources Web publiées via IIS sont mappées, via des répertoires virtuels, à des emplacements physiques sur le disque. Il est recommandé de mapper tous les répertoires virtuels sur un volume de disque non-système.

Raisonnement : Isoler le contenu Web des fichiers systèmes peut réduire la probabilité que :

- L'application d'e-services épuisent l'espace disque du système.
- La vulnérabilité des E/S de fichiers dans l'application d'e-services affecte la confidentialité et/ou l'intégrité des fichiers système.

Audit : Exécutez la commande suivante pour vous assurer qu'aucun répertoire virtuel n'est mappé sur le lecteur système :

Pour vérifier à l'aide d'AppCmd.exe, saisissez la commande suivante :

```
%systemroot%\system32\inetsrv\appcmd list vdir
```

OU

Pour vérifier à l'aide de PowerShell, saisissez la commande suivante :

```
Get-Website | Format-List Name, PhysicalPath
```

Correction :

1. Accédez au contenu Web dans **C:\inetpub\wwwroot\,**

2. Copiez ou coupez du contenu dans un dossier Web dédié et restreint sur un lecteur non-système tel que **D:\webroot**,

3. Modifiez les mappages pour toutes les applications ou les répertoires virtuels afin de refléter le nouvel emplacement,

Pour modifier le mappage de L'application d'e-services nommée app1 qui réside sous l'application d'e-services par défaut, ouvrez IIS Manager :

1. Développez le nœud du serveur,
2. Développer les sites,
3. Développer l'application d'e-services par défaut,
4. Cliquez sur app1,
5. Dans le volet Actions, sélectionnez Paramètres de base,
6. Dans la zone de texte Chemin physique, indiquez le nouvel emplacement de L'application d'e-services, **D:\wwwroot\app1** dans l'exemple ci-dessus.

Valeur par défaut : L'emplacement par défaut du contenu Web est : %systemdrive%\inetpub\wwwroot.

Règle 2 : Assurez-vous que les « en-têtes d'hôte » sont sur tous les sites.

Description : Les en-têtes d'hôte permettent d'héberger plusieurs applications d'e-services sur la même adresse IP et le même port. Il est recommandé de configurer les en-têtes d'hôte pour tous les sites. Les en-têtes d'hôte génériques sont désormais pris en charge.

Raisonnement : L'exigence d'un en-tête Host pour tous les sites peut réduire la probabilité de :

- Attaques de reliaison DNS compromettant ou abusant avec succès des données ou des fonctionnalités du site
- Analyses basées sur IP identifiant ou interagissant avec succès avec une application d'e-services cible hébergée sur IIS

Remarque : Si une entrée DNS générique existe et qu'un en-tête d'hôte générique est utilisé, vous pouvez fournir des données à plus de domaines que prévu.

Audit : Exécutez la commande suivante pour identifier les sites qui ne sont pas configurés pour exiger des en-têtes d'hôte. Pour vérifier à l'aide d'AppCmd.exe, saisissez la commande suivante :

```
%systemroot%\system32\inetsrv\appcmd list sites
```

OU

Pour vérifier à l'aide de PowerShell, saisissez la commande suivante :

```
Get-WebBinding -Port * | Format-List bindingInformation
```

Tous les sites seront répertoriés comme tels : SITE "Default Web Site" (id:1,bindings:http/*:80:test.com,state:Started) SITE "badsite" (id:3,bindings:http/*:80:,state:Started).

Pour tous les sites non-SSL, assurez-vous que le triplet de liaison IP:port:host contient un nom d'hôte. Dans l'exemple ci-dessus, le premier site est configuré comme recommandé étant donné que le Default Web Site a un en-tête d'hôte

test.com. badsite, cependant, n'a pas d'en-tête d'hôte configuré - il affiche *:80: ce qui signifie toutes les adresses IP sur le port 80, sans en-tête d'hôte.

Correction : Obtenez une liste de tous les sites à l'aide de la commande appcmd.exe suivante :
Entrez la commande suivante dans AppCmd.exe pour configurer l'en-tête de l'hôte :

```
%systemroot%\system32\inetsrv\appcmd.exe set config -
section:system.applicationHost/sites /"[name='<website name'].
bindings.[protocol='http',bindingInformation='*:80:<host header>'].
bindingInformation:"*:80:<host header>"" /commit:apphost
```

OU

Saisissez la commande suivante dans PowerShell pour configurer l'en-tête de l'hôte :

```
Set-WebConfigurationProperty -pspath 'MACHINE/WEBROOT/APPHOST'
-filter
'system.applicationHost/sites/site[@name='<website name>']/bindings/
binding[@protocol='http' and @bindingInformation='*:80:']' -name
'bindingInformation' -value '*:80:<host header value>'
```

OU

Effectuez les opérations suivantes dans IIS Manager pour configurer les en-têtes d'hôte pour le site Web par défaut :

1. Ouvrir le gestionnaire IIS.
2. Dans le volet Connexions, développez le nœud Sites et sélectionnez site web par défaut.
3. Dans le volet Actions, cliquez sur Liaisons.
4. Dans la boîte de dialogue Site Bindings, sélectionnez la liaison pour laquelle les en-têtes d'hôte vont être configurés, Port 80 dans cet exemple.
5. Cliquez sur Modifier.
Sous le nom d'hôte, entrez le nom de domaine complet des sites, par exemple **www.examplesite.com.**
6. Cliquez sur OK, puis sur Fermer.

Remarque : L'exigence d'un en-tête d'hôte peut altérer la fonctionnalité du site pour les clients HTTP/1.0.

Valeur par défaut : Par défaut, les en-têtes d'hôte ne sont pas obligatoires ou configurés automatiquement.

Règle 3 : Assurez-vous que la « navigation dans les répertoires » est désactivée

La description : La navigation dans les répertoires permet d'afficher le contenu d'un répertoire à la demande d'un client Web. Si la navigation dans les répertoires est activée pour un répertoire dans Internet Information Services, les utilisateurs reçoivent une page qui répertorie le contenu du répertoire lorsque les deux conditions suivantes sont remplies :
1. Aucun fichier spécifique n'est demandé dans l'URL
2. La fonctionnalité Documents par défaut est désactivée dans IIS, ou si elle est activée, IIS est incapable de localiser un fichier dans le répertoire qui correspond à un nom spécifié dans la liste de documents par défaut IIS

Il est recommandé de désactiver la navigation dans les répertoires.

Raisonnement : S'assurer que la navigation dans les répertoires est désactivée peut réduire la probabilité de divulguer du contenu sensible accessible par inadvertance via IIS.

Audit : Procédez comme suit pour vérifier que la navigation dans l'annuaire a été désactivée au niveau du serveur :
Pour vérifier à l'aide d'AppCmd.exe, saisissez la commande suivante :

```
%systemroot%\system32\inetsrv\appcmd list config /section:directoryBrowse
```

Si le serveur est configuré comme recommandé, ce qui suit s'affichera :

```
<system.webServer>
<directoryBrowse enabled="false" />
<system.webServer>
```

OU

Pour vérifier à l'aide de PowerShell, saisissez la commande suivante :

```
Get-WebConfigurationProperty -Filter system.webserver/directorybrowse
-PSPath iis:\ -Name Enabled | select Value
```

Correction : La navigation dans les répertoires peut être définie à l'aide de l'interface utilisateur, en exécutant les commandes appcmd.exe, en modifiant

directement les fichiers de configuration ou en écrivant des scripts WMI. Pour désactiver la navigation dans les répertoires au niveau du serveur à l'aide d'une commande appcmd.exe :

Entrez la commande suivante dans AppCmd.exe pour configurer :
%systemroot%\system32\inetsrv\appcmd set config /section:directoryBrowse /enabled:false

OU

Entrez la commande suivante dans PowerShell pour configurer :
Set-WebConfigurationProperty -Filter system.webserver/directorybrowse -PSPath iis:\ -Name Enabled -Value False

Valeur par défaut : Dans IIS, la navigation dans les répertoires est désactivée par défaut.

Règle 4 : Assurez-vous que "l'identité du pool d'applications" est configurée pour toutes les applications poules

La description : Les identités du pool d'applications sont les utilisateurs/autorités réels qui exécuteront le processus de travail - w3wp.exe. L'attribution de l'autorité d'utilisateur correcte permet de s'assurer que les applications peuvent fonctionner correctement, tout en n'accordant pas d'autorisations trop permissives sur le système. Ces identités peuvent en outre être utilisées dans les ACL pour protéger le contenu du système. Il est recommandé que chaque pool d'applications s'exécute sous une identité unique.
IIS possède des identités de moindre privilège intégrées supplémentaires destinées à être utilisées par les pools d'applications. Il est recommandé de remplacer l'identité du pool d'applications par défaut par un principe de moindre privilège autre que le service réseau. En outre, il est recommandé d'attribuer à toutes les identités du pool d'applications un principal de moindre privilège unique.

Pour obtenir l'isolation dans IIS, les pools d'applications peuvent être exécutés en tant qu'identités distinctes. IIS peut être configuré pour utiliser automatiquement l'identité du pool d'applications si aucun compte d'utilisateur anonyme n'est configuré pour un site Web. Cela peut réduire considérablement le nombre de comptes nécessaires pour les sites Web et faciliter la gestion des comptes. Il est recommandé que l'identité du pool d'applications soit définie comme l'identité de l'utilisateur anonyme.

Le nom du compte du pool d'applications correspond au nom du pool d'applications. Les identités de pool d'applications ont été introduites dans Windows Server 2008 SP2. Il est recommandé de configurer les pools d'applications pour qu'ils s'exécutent en tant qu'ApplicationPoolIdentity, sauf s'il existe une raison sous-jacente pour laquelle le pool d'applications doit s'exécuter en tant que compte d'utilisateur final spécifié. Un exemple où cela est nécessaire est pour les fermes Web utilisant l'authentification Kerberos.

Raisonnement : Configuration des pools d'applications pour utiliser des identités uniques de moindre privilège telles que ApplicationPoolIdentity réduit les dommages potentiels que l'identité pourrait causer si l'application venait à être compromise.
De plus, cela simplifiera la configuration des pools d'applications et la gestion des comptes.

Audit : Pour vérifier que les pools d'applications ont été configurés pour s'exécuter sous ApplicationPoolIdentity à l'aide du gestionnaire IIS :
1. Ouvrir le gestionnaire IIS
2. Ouvrez le nœud Application Pools sous le nœud de la machine ; sélectionnez le pool d'applications à vérifier
3. Cliquez avec le bouton droit sur le pool d'applications et sélectionnez Paramètres avancés...

Sous la section Process Model, localisez l'option Identity et assurez-vous que ApplicationPoolIdentity est défini

Cette configuration est stockée dans le même fichier applicationHost.config pour les sites Web et les répertoires d'applications/virtuels, au bas du fichier, entouré de balises <location path="path/to/resource">tags.

Pour vérifier que tous les nouveaux pools d'applications utilisent ApplicationPoolIdentity, exécutez la commande suivante pour déterminer si la valeur par défaut du pool d'applications a été modifiée en ApplicationPoolIdentity :

Pour vérifier à l'aide d'AppCmd.exe, saisissez la commande suivante :
%systemroot%\system32\inetsrv\appcmd list config /section:applicationPools

OU

Pour vérifier à l'aide de PowerShell, saisissez la commande suivante :
Get-ChildItem -Path IIS:\AppPools\ |

```
Select-Object name, state, <#@{e={$_.processModel.password};l="password"}, #> @{e={$_.processModel.identityType};l="identityType"}
```

Correction : L'identité du pool d'applications par défaut peut être définie pour une application d'e-services à l'aide du gestionnaire IIS GUI, en utilisant les commandes AppCmd.exe dans une fenêtre de ligne de commande, en modifiant directement les fichiers de configuration ou en écrivant des scripts WMI. Effectuez les opérations suivantes pour remplacer l'identité par défaut par ApplicationPoolIdentity intégrée dans l'interface graphique du gestionnaire IIS :

1. Ouvrez l'interface graphique du gestionnaire IIS
2. Dans le volet des connexions, développez le nœud du serveur et cliquez sur Pools d'applications
3. Sur la page Pools d'applications, sélectionnez DefaultAppPool, puis cliquez sur Paramètres avancés dans le volet Actions
4. Pour la propriété Identity, cliquez sur le bouton '...' pour ouvrir la boîte de dialogue Identité du pool d'applications
5. Sélectionnez l'option Compte intégré, choisissez ApplicationPoolIdentity dans la liste ou saisissez un utilisateur d'application unique créé à cet effet.
6. Redémarrez IIS

Pour remplacer l'identité ApplicationPool par l'ApplicationPoolIdentity intégrée à l'aide d'AppCmd.exe, exécutez la commande suivante à partir d'une invite de commande :

Entrez la commande suivante dans AppCmd.exe pour configurer

```
%systemroot%\system32\inetsrv\appcmd set config /section:applicationPools /[name='<apppool name>'].processModel.identityType:ApplicationPoolIdentity
```

OU

Pour remplacer l'identité ApplicationPool par l'ApplicationPoolIdentity intégrée à l'aide de PowerShell :

```
Set-WebConfigurationProperty -pspath 'MACHINE/WEBROOT/APPHOST' -filter 'system.applicationHost/applicationPools/add[@name='<apppool name>']/processModel' -name 'identityType' -value 'ApplicationPoolIdentity'
```

L'exemple de code ci-dessus définira uniquement le DefaultAppPool.

Exécutez cette commande pour chaque pool d'applications configuré. En outre, ApplicationPoolIdentity peut devenir la valeur par défaut pour tous les pools d'applications à l'aide de l'action Définir les valeurs par défaut du pool d'applications sur le nœud Pools d'applications.
Si vous utilisez un utilisateur Windows personnalisé tel qu'un compte de service dédié, cet utilisateur devra être membre du groupe IIS_IUSRS. Le groupe IIS_IUSRS a accès à toutes les ressources système et de fichiers nécessaires afin qu'un compte, lorsqu'il est ajouté à ce groupe, puisse agir de manière transparente comme une identité de pool d'applications.

Valeur par défaut : Par défaut, le DefaultAppPool dans IIS est configuré pour utiliser le compte ApplicationPoolIdentity.

Règle 5 : S'assurer que des "pools d'applications uniques" sont définis pour les sites

La description : IIS a introduit une nouvelle fonctionnalité de sécurité appelée Application Pool Identities qui permet aux pools d'applications d'être exécutés sous des comptes uniques sans avoir besoin de créer et de gérer des comptes locaux ou de domaine. Il est recommandé que tous les sites s'exécutent sous des pools d'applications uniques et dédiés.

Raisonnement : En configurant les sites pour qu'ils s'exécutent dans des pools d'applications uniques, les applications gourmandes en ressources peuvent être affectées à leurs propres pools d'applications, ce qui peut améliorer les performances du serveur et des applications. Les autres pools ne sont pas affectés. Enfin, l'isolation des applications permet d'atténuer le risque potentiel qu'une application soit autorisée à accéder aux ressources d'une autre application. Il est également recommandé d'arrêter tout pool d'applications qui n'est pas utilisé ou qui a été créé par une installation telle que .Net 4.0.

Audit : La commande appcmd.exe suivante donnera une liste de toutes les applications configurées, sur quel site elles se trouvent, quel pool d'applications les dessert et sous quelle identité de pool d'applications elles s'exécutent :

```
%systemroot%\system32\inetsrv\appcmd list app
```

La sortie de cette commande ressemblera à ce qui suit : APP "Default Web Site/"

(applicationPool:DefaultAppPool)
Exécutez la commande ci-dessus et assurez-vous qu'un pool d'applications unique est attribué à chaque site répertorié

OU

Pour vérifier à l'aide de PowerShell, saisissez la commande suivante :
Get-Site Web | Select-Object Name, applicationPool

Correction :
La commande appcmd.exe suivante définira le pool d'applications pour une application donnée :

%systemroot%\system32\inetsrv\appcmd set app '<website name>/' /applicationpool:<apppool name>

La sortie de cette commande ressemblera à ce qui suit : Objet APP "Site Web par défaut/" modifié (applicationPool : DefaultAppPool)
Exécutez la commande ci-dessus pour vous assurer qu'un pool d'applications unique est attribué à chaque site répertorié

OU

Entrez la commande suivante dans PowerShell pour configurer :
Set-ItemProperty -Path 'IIS:\Sites\<website name>' -Name applicationPool -Value <apppool name>

OU

- Ouvrir le gestionnaire IIS
- Ouvrez le nœud Sites sous le nœud de la machine
- Sélectionnez le site à modifier
- Dans le volet Actions, sélectionnez Paramètres de base
- Cliquez sur la case Sélectionner... à côté de la zone de texte Pool d'applications
- Sélectionnez le pool d'applications souhaité
- Une fois sélectionné, cliquez sur OK

Valeur par défaut : Par défaut, tous les sites créés utiliseront le pool d'applications par défaut (DefaultAppPool).

Règle 6 : Assurez-vous que "l'identité du pool d'applications" est configurée pour identité de l'utilisateur

La description : Pour obtenir l'isolation dans IIS, les pools d'applications peuvent être exécutés en tant qu'identités distinctes. IIS peut être configuré pour utiliser automatiquement l'identité du pool d'applications si aucun compte d'utilisateur anonyme n'est configuré pour un site Web. Cela peut réduire considérablement le nombre de comptes nécessaires pour les sites Web et faciliter la gestion des comptes. Il est recommandé que l'identité du pool d'applications soit définie comme l'identité de l'utilisateur anonyme.

Raisonnement : La configuration de l'identité de l'utilisateur anonyme pour utiliser l'identité du pool d'applications permet d'assurer l'isolation du site - à condition que les sites soient configurés pour utiliser l'identité du pool d'applications. Puisqu'un principal unique exécutera chaque pool d'applications, il garantira que l'identité est le moindre privilège.
De plus, cela simplifiera la gestion du site.

Audit : Recherchez et ouvrez le fichier applicationHost.config et vérifiez que l'attribut userName de la balise anonymeAuthentication est défini sur une chaîne vide :

```
<system.webServer>
 <security>
  <authentication>
   <anonymousAuthentication userName="" />
  </authentication>
 </security>
</system.webServer>
```

Cette configuration est stockée dans le même fichier applicationHost.config pour les sites Web et les répertoires d'applications/virtuels, au bas du fichier, entouré de balises `<location path="path/to/resource">`tags.
Pour vérifier à l'aide de PowerShell, saisissez la commande suivante :

```
Get-WebConfiguration
system.webServer/security/authentication/anonymousAuthentication
-Recurse | where {$_.enabled -eq $true} | format-list location
```

Correction : L'identité de l'utilisateur anonyme peut être définie sur l'identité du pool d'applications à l'aide de l'interface graphique du gestionnaire IIS, à l'aide des commandes AppCmd.exe dans une fenêtre de ligne de commande, en modifiant directement les fichiers de configuration ou en écrivant des scripts WMI. Effectuez les opérations suivantes pour définir l'attribut username du nœud anonymeAuthentication dans l'interface graphique du gestionnaire IIS :

- Ouvrez l'interface graphique du gestionnaire IIS et accédez au serveur, site ou application d'e-services souhaité
- Dans Affichage des fonctionnalités, recherchez et double-cliquez sur l'icône Authentification
- Sélectionnez l'option Authentification anonyme et dans le volet Actions, sélectionnez Modifier...
- Choisissez Identité du pool d'applications dans la fenêtre modale, puis appuyez sur le bouton OK

OU

Pour utiliser AppCmd.exe pour configurer l'authentification anonyme au niveau du serveur, la commande ressemblerait à ceci :

```
%systemroot%\system32\inetsrv\appcmd set config
section:anonymousAuthentication /username:"" --password
```

OU

Entrez la commande suivante dans PowerShell pour configurer :

```
Set-ItemProperty -Path IIS:\AppPools\<apppool name> -Name
passAnonymousToken -Value True
```

Valeur par défaut : L'identité par défaut de l'utilisateur anonyme est le compte virtuel IUSR.

Règle 7 : Assurez-vous que la fonctionnalité WebDav est désactivée

La description : WebDAV est une extension du protocole HTTP qui permet aux clients de créer, déplacer et supprimer des fichiers et des ressources sur le serveur Web. Cette fonctionnalité est disponible dans IIS lorsque la fonction WebDAV est activée.

Raisonnement : WebDAV n'est pas largement utilisé et présente de sérieux problèmes de sécurité car il peut permettre aux clients de modifier des fichiers

non autorisés sur le serveur Web. Par conséquent, la fonctionnalité WebDav doit être désactivée.

Audit : Pour vérifier à l'aide de PowerShell, saisissez la commande suivante :
`Get-WindowsFeature Web-DAV-Publishing`

Vérifiez que l'état d'installation est disponible

Correction : Pour désactiver cette fonctionnalité à l'aide de PowerShell, saisissez la commande suivante :
`Remove-WindowsFeature Web-DAV-Publishing`

Vérifiez que le succès est vrai

Valeur par défaut : L'état par défaut de la publication WebDAV est désactivé

1- Configurer l'authentification et l'autorisation

Cette section contient des recommandations concernant les différentes couches d'authentification dans IIS.

Règle 1 : Assurez-vous que la "règle d'autorisation globale" est définie pour restreindre l'accès

La description : IIS a introduit l'autorisation d'URL, qui permet l'ajout de règles d'autorisation à l'URL réelle, au lieu de la ressource de système de fichiers sous-jacente, comme moyen de la protéger. Les règles d'autorisation peuvent être configurées au niveau du serveur, du site Web, du dossier (y compris les répertoires virtuels) ou du fichier. Le module natif d'autorisation d'URL s'applique à toutes les requêtes, qu'elles soient gérées par .NET ou d'autres types de fichiers (par exemple, des fichiers statiques ou des fichiers ASP). Il est recommandé de configurer l'autorisation d'URL pour n'accorder l'accès qu'aux principaux de sécurité nécessaires.

Raisonnement : La configuration d'une règle d'autorisation globale qui restreint l'accès garantira l'héritage des paramètres dans la hiérarchie des répertoires Web ; si ce contenu est copié ailleurs, les règles d'autorisation en découlent. Cela garantira que l'accès au contenu actuel et futur n'est accordé qu'aux responsables appropriés, atténuant ainsi le risque d'accès accidentel ou non autorisé.

Audit : Vérifiez une règle d'autorisation spécifiant aucun accès à tous les

utilisateurs à l'exception du groupe Administrateurs :
Pour vérifier à l'aide d'AppCmd.exe, saisissez la commande suivante :

```
%systemroot%\system32\inetsrv\appcmd list config -section:system.
webserver/security/authorization
```

OU

Pour vérifier à l'aide de PowerShell, saisissez la commande suivante :

```
Get-WebConfiguration -pspath 'IIS:\' -filter
'system.webServer/security/authorization'
```

OU

Au niveau du site de l'application d'e-services, vérifiez que la règle d'autorisation configurée a été appliquée :

- Se connecter aux services d'information Internet (Gestionnaire IIS)
- Sélectionnez l'application d'e-services où l'autorisation a été configurée
- Sélectionnez Règles d'autorisation et vérifiez que les règles configurées ont été ajoutées

Recherchez et ouvrez le fichier web.config pour le site/l'application/le contenu configuré :

```
<configuration>
 <system.webServer>
  <security>
   <authorization>
    <remove users="*" roles="" verbs="" />
    <add accessType="Allow" roles="administrators" />
   </authorization>
  </security>
 </system.webServer>
</configuration>
```

Correction : Pour configurer l'autorisation d'URL au niveau du serveur à l'aide des utilitaires de ligne de commande : saisissez la commande suivante dans AppCmd.exe pour configurer :

```
%systemroot%\system32\inetsrv\appcmd set config - section:system.
webServer/security/authorization /-"[users='*',roles='',verbs='']"
%systemroot%\system32\inetsrv\appcmd set config
```

-section:system.webServer/security/authorization
/+"[accessType='Allow',roles='Administrators']"

OU

Entrez la commande suivante dans PowerShell pour configurer :

Remove-WebConfigurationProperty -pspath 'MACHINE/WEBROOT/APPHOST' -filter "system.webServer/security/authorization" -nom "." -AtElement @{users='*';roles='';verbs=''}
Add-WebConfigurationProperty -pspath 'MACHINE/WEBROOT/APPHOST' -filter "system.webServer/security/authorization" -nom "." -évaluer @{accessType='Autoriser';roles='Administrateurs'}

OU

Pour configurer l'autorisation d'URL au niveau du serveur à l'aide du gestionnaire IIS :

- Se connecter aux services d'information Internet (Gestionnaire IIS)
- Sélectionnez le serveur
- Sélectionnez les règles d'autorisation
- Supprimer la règle "Autoriser tous les utilisateurs"
- Cliquez sur Ajouter une règle d'autorisation...
- Autoriser l'accès aux utilisateurs, groupes d'utilisateurs ou rôles autorisés sur toutes les applications d'e-services (par exemple, le groupe Administrateurs)

Valeur par défaut : Le paramètre par défaut au niveau du serveur est d'autoriser l'accès à tous les utilisateurs.

Règle 2 : S'assurer que l'accès aux fonctionnalités sensibles du site est limité aux mandants authentifiés uniquement

La description : IIS prend en charge les méthodes d'authentification basées sur les défis et sur la redirection de connexion. Les méthodes d'authentification basées sur la stimulation, telles que l'authentification Windows intégrée, exigent qu'un client réponde correctement à une stimulation lancée par le serveur. Une méthode d'authentification basée sur la redirection de connexion, telle que l'authentification par formulaire, repose sur la redirection

vers une page de connexion pour déterminer l'identité du principal. Les méthodes d'authentification basée sur le défi et d'authentification basée sur la redirection de connexion ne peuvent pas être utilisées conjointement.
Les serveurs/sites publics sont généralement configurés pour utiliser l'authentification anonyme. Cette méthode fonctionne généralement, à condition que le contenu ou les services soient destinés à être utilisés par le public. Lorsque des sites, des applications d'e-services ou des conteneurs de contenu spécifiques ne sont pas destinés à un usage public anonyme, un mécanisme d'authentification approprié doit être utilisé. L'authentification aidera à confirmer l'identité des clients qui demandent l'accès aux sites, aux applications d'e-services et au contenu. IIS fournit les modules d'authentification suivants par défaut :

- Authentification anonyme - permet aux utilisateurs anonymes d'accéder à des sites, des applications et/ou du contenu
- Authentification Windows intégrée - authentifie les utilisateurs à l'aide de NTLM ou protocoles Kerberos ; Kerberos v5 nécessite une connexion à Active Directory
- ASP.NET Impersonation - permet aux applications ASP.NET de s'exécuter dans un contexte de sécurité différent du contexte de sécurité par défaut d'une application
- Authentification par formulaires - permet à un utilisateur de se connecter à l'espace configuré avec un nom d'utilisateur et un mot de passe valides qui sont ensuite validés par rapport à une base de données ou à un autre magasin d'informations d'identification
- Authentification de base - nécessite un nom d'utilisateur et un mot de passe valides pour accéder au contenu
- Authentification par mappage de certificat client - permet l'authentification automatique des utilisateurs qui se connectent avec des certificats client qui ont été configurés ; nécessite SSL
- Authentification Digest - utilise le contrôleur de domaine Windows pour authentifier les utilisateurs qui demandent l'accès

Notez qu'aucun des modules d'authentification par challenge ne peut être utilisé en même temps que l'authentification par formulaire est activée pour certaines applications/contenus. L'authentification par formulaires ne s'appuie pas sur l'authentification IIS, de sorte que l'accès anonyme pour l'application ASP.NET peut être configuré si l'authentification par formulaires est utilisée.
Il est recommandé que les sites contenant des informations sensibles, des

données confidentielles ou des services Web non publics soient configurés avec un mécanisme d'authentification basé sur les informations d'identification.

Raisonnement : La configuration de l'authentification permet d'atténuer le risque que des utilisateurs non autorisés accèdent aux données et/ou aux services et, dans certains cas, de réduire les dommages potentiels pouvant être causés à un système.

Audit : Pour vérifier que le module d'authentification est activé pour l'application d'e-services ou un contenu spécifique, recherchez et ouvrez le fichier web.config relatif au contenu. Vérifiez que le fichier de configuration a maintenant un mode défini dans les balises <authentication>. L'exemple ci-dessous montre que l'authentification par formulaire est configurée, les cookies seront toujours utilisés et SSL est requis :

```
<systeme.web>
<authentification>
 <forms cookieless="UseCookies" requireSSL="true" />
</authentification>
</system.web>
```

OU

Pour vérifier à l'aide d'AppCmd.exe, saisissez la commande suivante :

```
%systemroot%\system32\inetsrv\appcmd list config -section:system.web/
authentication
```

OU

Pour vérifier à l'aide de PowerShell, saisissez la commande suivante :

```
Get-WebConfiguration system.webServer/security/authentication/* -Recurse |
Where-Object {$_.enabled -eq $true} | Format-Table
```

Correction : Lors de la première configuration d'un module d'authentification, chaque mécanisme doit être complètement configuré avant utilisation.
L'activation de l'authentification peut être effectuée à l'aide de l'interface utilisateur (UI), en exécutant les commandes AppCmd.exe dans une fenêtre de ligne de commande, en modifiant directement les fichiers de configuration ou en écrivant des scripts WMI. Pour vérifier qu'un mécanisme d'authentification est en place pour le contenu sensible à l'aide de l'interface graphique du gestionnaire IIS :

- Ouvrez IIS Manager et naviguez jusqu'au niveau avec du contenu sensible
- Dans Affichage des fonctionnalités, double-cliquez sur Authentification
- Sur la page Authentification, assurez-vous qu'un module d'authentification est activé, tandis que l'authentification anonyme est activée (l'authentification par formulaire peut également être anonyme)
- Si nécessaire, sélectionnez le module d'authentification souhaité, puis dans le volet Actions, cliquez sur Activer

OU

Entrez la commande suivante dans AppCmd.exe pour configurer :

```
%systemroot%\system32\inetsrv\appcmd set config section:system.web/authentication /mode:<Windows|Passport|Forms>
```

OU

Entrez la commande suivante dans PowerShell pour configurer :

```
Set-WebConfigurationProperty -pspath 'MACHINE/WEBROOT/APPHOST' -location '<website location>' -filter 'system.webServer/security/authentication/anonymousAuthentication' -name 'enabled' -value 'False'
Set-WebConfigurationProperty -pspath 'MACHINE/WEBROOT/APPHOST' -location '<website location>' -filter 'system.webServer/security/authentication/windowsAuthentication' -name 'enabled' -value 'True'
```

Valeur par défaut : L'installation par défaut d'IIS prend en charge l'authentification anonyme sans autre choix de méthodes supplémentaires.

Règle 3 : Assurez-vous que l'authentification par formulaires nécessite SSL

La description : L'authentification basée sur les formulaires peut transmettre les informations d'identification sur le réseau en texte clair. Il est donc impératif que le trafic entre le client et le serveur soit crypté à l'aide de SSL, en particulier dans les cas où le site est accessible au public. Il est recommandé que les communications avec toute partie d'un site utilisant l'authentification par formulaires soient cryptées à l'aide de SSL.

Remarque : En raison de vulnérabilités de sécurité identifiées, SSL n'est plus

considéré comme offrant une protection adéquate pour une information sensible.

Raisonnement : L'exigence de SSL pour l'authentification par formulaire protégera la confidentialité des informations d'identification pendant le processus de connexion, ce qui contribuera à atténuer le risque de vol d'informations sur les utilisateurs.

Audit : Pour vérifier que SSL est requis pour l'authentification par formulaire pour une application d'e-services un contenu spécifique, recherchez et ouvrez le fichier web.config pour le niveau auquel l'authentification par formulaire a été activée. Vérifiez la balise <forms requireSSL="true" /> :

```
<systeme.web>
 <authentication>
  <forms requireSSL="true" />
</authentication>
</system.web>
```

OU

Pour vérifier à l'aide d'AppCmd.exe, saisissez la commande suivante :

```
%systemroot%\system32\inetsrv\appcmd list config - section:system.web/
authentication
```

OU

Pour vérifier à l'aide de PowerShell, saisissez la commande suivante :

```
Get-WebConfigurationProperty -pspath 'MACHINE/WEBROOT/APPHOST/
Default Web Site' -filter 'system.web/authentication/forms' -name
'requireSSL' | Format-Table Name, Value
```

Correction :

- Ouvrez IIS Manager et accédez au niveau approprié
- Dans Affichage des fonctionnalités, double-cliquez sur Authentification
- Sur la page Authentification, sélectionnez Authentification par formulaires
- Dans le volet Actions, cliquez sur Modifier
- Cochez la case Nécessite SSL dans la section des paramètres des cookies, cliquez sur OK

OU

Entrez la commande suivante dans AppCmd.exe pour configurer :
%systemroot%\system32\inetsrv\appcmd set config section:system.web/authentication /mode:Forms

OU

Entrez la commande suivante dans PowerShell pour configurer :
Set-WebConfigurationProperty -pspath 'MACHINE/WEBROOT/APPHOST/Default Web Site' -filter 'system.web/authentication/forms' -name 'requireSSL' -value 'True'

Valeur par défaut : SSL n'est pas requis lorsque l'authentification par formulaire est activée.

Règle 4 : Assurez-vous que l'« authentification par formulaire » est configurée pour utiliser des cookies.

La description : L'authentification par formulaires peut être configurée pour conserver l'identifiant de session du visiteur du site dans un URI ou un cookie. Il est recommandé que l'authentification par formulaire soit configurée pour utiliser des cookies.

Raisonnement : L'utilisation de cookies pour gérer l'état de session peut aider à atténuer le risque de tentatives de détournement de session en empêchant ASP.NET d'avoir à déplacer les informations de session vers l'URL. Le déplacement des identifiants d'informations de session dans l'URL peut entraîner l'affichage des identifiants de session dans les journaux de proxy, l'historique de navigation et l'accès aux scripts clients via document.location .

Audit : Recherchez et ouvrez le fichier web.config pour l'application configurée. Vérifiez la présence de <forms cookieless="UseCookies" />.

```
<systeme.web>
 <authentication>
  <forms cookieless="UseCookies" requireSSL="true" timeout="30" />
 </authentification>
</system.web>
```

OU

Pour vérifier à l'aide d'AppCmd.exe, saisissez la commande suivante :
%systemroot%\system32\inetsrv\appcmd list config - section:system.web/

authentication

OU

Pour vérifier à l'aide de PowerShell, saisissez la commande suivante :
Get-WebConfigurationProperty -pspath 'MACHINE/WEBROOT/APPHOST/ /Default Web Site' -filter 'system.web/authentication/forms' -Recurse -name 'cookieless'

Correction :

- Ouvrez IIS Manager et accédez au niveau où l'authentification par formulaire est activée
- Dans Affichage des fonctionnalités, double-cliquez sur Authentification
- Sur la page Authentification, sélectionnez Authentification par formulaires
- Dans le volet Actions, cliquez sur Modifier
- Dans la section Paramètres des cookies, sélectionnez Utiliser les cookies dans le menu déroulant Mode

OU

Entrez la commande suivante dans AppCmd.exe pour configurer :
%systemroot%\system32\inetsrv\appcmd set config section:system.web/authentication /forms.cookieless:"UseCookies"

OU

Entrez la commande suivante dans PowerShell pour configurer :
Set-WebConfigurationProperty -pspath 'MACHINE/WEBROOT/APPHOST/Default Web Site' -filter 'system.web/authentication/forms' -name 'cookieless' -value 'UseCookies'

Valeur par défaut : Le paramètre par défaut pour le mode Cookie est Auto Detect qui n'utilisera les cookies que si le profil de l'appareil prend en charge les cookies.

Règle 5 : Assurez-vous que le "mode de protection des cookies" est configuré pour les formulaires authentification

La description : Le mode de protection des cookies définit la protection que les cookies d'authentification par formulaires recevront dans une application d'e-services configurée. Les quatre modes de protection des cookies définissables sont :

- Cryptage et validation - Spécifie que l'application utilise à la fois la validation et le cryptage des données pour aider à protéger le cookie ; cette option utilise l'algorithme de validation des données configuré (basé sur la clé de la machine) et triple-DES (3DES) pour le chiffrement, si disponible et si la clé est suffisamment longue (48 octets ou plus)
- Aucun - Spécifie que le cryptage et la validation sont désactivés pour les sites qui utilisent des cookies uniquement pour la personnalisation et ont des exigences de sécurité plus faibles
- Chiffrement - Spécifie que le cookie est chiffré à l'aide de Triple-DES ou DES, mais que la validation des données n'est pas effectuée sur le cookie ; les cookies utilisés de cette manière peuvent faire l'objet d'attaques en texte brut
- Validation - Spécifie qu'un schéma de validation vérifie que le contenu d'un cookie chiffré n'a pas été modifié en transit

Il est recommandé que le mode de protection des cookies chiffre et valide toujours les cookies d'authentification par formulaire.

Raisonnement : En cryptant et en validant le cookie, la confidentialité et l'intégrité des données contenues dans le cookie sont assurées. Cela permet d'atténuer le risque d'attaques telles que le détournement de session et l'usurpation d'identité.

Audit : Recherchez et ouvrez le fichier web.config pour l'application configurée. Vérifiez la présence de <forms protection="All" />.

```
<systeme.web>
 <authentication>
  <forms cookieless="UseCookies" protection="All" />
 </authentification>
</system.web>
```

La propriété protection="All" ne s'affichera que si le mode de protection des cookies a été défini sur quelque chose de différent, puis modifié sur Chiffrement et validation. Pour vraiment vérifier la propriété protection="All " dans le web.config, le mode de protection peut être modifié, puis modifié à nouveau. Inversement, la ligne protection="All" peut être ajoutée manuellement au web.config.

OU

Pour vérifier à l'aide de PowerShell, saisissez la commande suivante :

```
Get-WebConfigurationProperty -pspath 'MACHINE/WEBROOT/
```

APPHOST/<website name>' -filter 'system.web/authentication/forms' -name 'protection'

Correction : Le mode de protection des cookies peut être configuré à l'aide de l'interface utilisateur (UI), en exécutant
Appcmd.exe dans une fenêtre de ligne de commande, en modifiant directement les fichiers de configuration ou en écrivant des scripts WMI. Utilisation du gestionnaire IIS :

- Ouvrez IIS Manager et accédez au niveau où l'authentification par formulaire est activée
- Dans Affichage des fonctionnalités, double-cliquez sur Authentification
- Sur la page Authentification, sélectionnez Authentification par formulaires
- Dans le volet Actions, cliquez sur Modifier
- Dans la section Paramètres des cookies, vérifiez que le menu déroulant pour le mode de protection est défini pour Cryptage et validation

OU

Entrez la commande suivante dans PowerShell pour configurer :
Set-WebConfigurationProperty -pspath 'MACHINE/WEBROOT/APPHOST/<website name>' -filter 'system.web/authentication/forms' -name 'protection' -value 'All'

Valeur par défaut : Lorsque des cookies sont utilisés pour l'authentification par formulaires, le mode de protection des cookies par défaut est All, ce qui signifie que l'application chiffre et valide le cookie.

Règle 6 : S'assurer que la sécurité de la couche de transport pour l'« authentification de base » est configuré

La description : L'authentification de base peut transmettre les informations d'identification sur le réseau en texte clair. Il est donc impératif que le trafic entre le client et le serveur soit crypté, en particulier dans les cas où le site est accessible au public et il est recommandé que TLS soit configuré et requis pour tout site ou application utilisant l'authentification de base.

Raisonnement : Les informations d'identification envoyées en texte clair peuvent être facilement interceptées par un code ou des personnes malveillants. L'application de l'utilisation de Transport Layer Security contribuera à réduire

les risques de détournement d'informations d'identification.

Audit : Une fois que la sécurité de la couche de transport a été configurée et requise L'application d'e-services, seule l'adresse https:// sera disponible. Essayez de charger le site ou l'application pour laquelle l'authentification de base est configurée à l'aide de http://, les requêtes échoueront et IIS générera une erreur 403.4 - Interdit.

OU

Pour vérifier à l'aide de PowerShell, saisissez la commande suivante :
Get-WebConfigurationProperty -pspath 'MACHINE/WEBROOT/APPHOST' -location '<website name>' -filter 'system.webServer/security/access' -name 'sslFlags'

Correction :
Pour protéger l'authentification de base avec la sécurité de la couche de transport :

- Ouvrir le gestionnaire IIS
- Dans le volet Connexions à gauche, sélectionnez le serveur à configurer
- Dans le volet Connexions, développez le serveur, puis développez Sites et sélectionnez le site à configurer
- Dans le volet Actions, cliquez sur Liaisons ; la boîte de dialogue Liaisons de site s'affiche
- Si une liaison HTTPS est disponible, cliquez sur Fermer et voir ci-dessous "Pour exiger SSL"
- Si aucune liaison HTTPS n'est visible, procédez comme suit

Pour ajouter une liaison HTTPS :

- Dans la boîte de dialogue Liaisons de site, cliquez sur Ajouter ; la boîte de dialogue Ajouter une liaison de site s'affiche
- Sous Type, sélectionnez https
- Sous Certificat SSL, sélectionnez un certificat X.509
- Cliquez sur OK, puis fermez

Pour exiger SSL :

- Dans Affichage des fonctionnalités, double-cliquez sur Paramètres SSL
- Sur la page Paramètres SSL, sélectionnez Exiger SSL.

- Dans le volet Actions, cliquez sur Appliquer

OU

Entrez la commande suivante dans PowerShell pour configurer :

```
Set-WebConfigurationProperty -pspath 'MACHINE/WEBROOT/APPHOST'
-location '<website name' -filter 'system.webServer/security/access' -name
'sslFlags' -value 'Ssl'
```

Valeur par défaut : Transport Layer Security n'est pas activé par défaut lorsque l'authentification de base est configurée.

Règle 7 : Assurez-vous que 'passwordFormat' n'est pas défini sur clair

La description : L'élément <credentials> de l'élément <authentication> permet des définitions facultatives de nom et de mot de passe pour les comptes d'utilisateur du gestionnaire IIS dans le fichier de configuration. L'authentification basée sur les formulaires utilise également ces éléments pour définir les utilisateurs. IIS Manager Les utilisateurs peuvent utiliser l'interface d'administration pour se connecter aux sites et applications dans lesquels ils ont reçu une autorisation. Notez que l'élément <credentials> s'applique uniquement lorsque le fournisseur par défaut, ConfigurationAuthenticationProvider, est configuré en tant que fournisseur d'authentification. Il est recommandé de définir passwordFormat sur une valeur autre que Clear, telle que SHA1.

Raisonnement : Les identifiants d'authentification doivent toujours être protégés pour réduire le risque de vol des identifiants d'authentification.

Audit : Recherchez et ouvrez le fichier de configuration de l'application configurée. Vérifiez que l'élément d'informations d'identification n'est pas présent :

```
<configuration>
 <systeme.web>
  <authentication mode="Forms">
   <forms name="SampleApp" loginUrl="/login.aspx">
    < credentials passwordFormat="SHA1">
     <user
      name="<em>UserName1</em>"
```

```
    password="<em>SHA1EncryptedPassword1</em>"/>
   <user
    name="<em>UserName2</em>"
    password="<em>SHA1EncryptedPassword2</em>"/>
  </ credentials
 </forms>
</authentication>
</system.web>
</configuration>
```

OU

Pour vérifier à l'aide de PowerShell, saisissez la commande suivante :

```
Get-WebConfigurationProperty -pspath 'MACHINE/WEBROOT/
APPHOST/<xebsite name>' -filter 'system.web/authentication/forms/
credentials' -name 'passwordFormat'
```

Correction :

Le mode d'authentification est configurable dans machine.config , web.config au niveau de la racine ou web.config au niveau de l'application d'e-services :

- Localisez et ouvrez le fichier de configuration où les informations d'identification sont stockées
- Trouver l'élément <credentials>
- S'il est présent, assurez-vous que passwordFormat n'est pas défini sur Clear
- Remplacez passwordFormat par SHA1

Les mots de passe en texte clair devront être remplacés par la version hachée appropriée.

OU

Entrez la commande suivante dans PowerShell pour configurer :

```
Set-WebConfigurationProperty -pspath 'MACHINE/WEBROOT/
APPHOST/<website name>' -filter 'system.web/authentication/forms/
credentials' -name 'passwordFormat' -value 'SHA1'
```

Valeur par défaut : méthode passwordFormat par défaut est SHA1.

Règle 8 : S'assurer que les "informations d'identification" ne sont pas stockées dans les fichiers de configuration

La description : L'élément <credentials> de l'élément <authentication> permet des définitions facultatives de nom et de mot de passe pour les comptes d'utilisateur du gestionnaire IIS dans le fichier de configuration. L'authentification basée sur les formulaires utilise également ces éléments pour définir les utilisateurs. IIS Manager Les utilisateurs peuvent utiliser l'interface d'administration pour se connecter aux sites et application d'e-servicess dans lesquels ils ont reçu une autorisation. Notez que l'élément <credentials> s'applique uniquement lorsque le fournisseur par défaut, ConfigurationAuthenticationProvider, est configuré en tant que fournisseur d'authentification. Il est recommandé d'éviter de stocker les mots de passe dans le fichier de configuration, même sous forme de hachage.

Raisonnement : Les identifiants d'authentification doivent toujours être protégés pour réduire le risque de vol des identifiants d'authentification. Pour des raisons de sécurité, il est recommandé de ne pas stocker les informations d'identification de l'utilisateur dans les fichiers de configuration IIS.

Audit : Recherchez et ouvrez le fichier de configuration de l'application d'e-services configurée. Vérifiez que l'élément credentials n'est pas présent :

```
<configuration>
 <systeme.web>
  < authentication mode="Forms">
   <forms name="SampleApp" loginUrl="/login.aspx">
   </forms>
  </authentification>
 </system.web>
</configuration>
```

OU

Pour vérifier à l'aide de PowerShell, saisissez la commande suivante :

```
Get-WebConfigurationProperty -pspath 'MACHINE/WEBROOT/
APPHOST/<website name' -filter 'system.web/authentication/forms/
credentials' -name 'passwordFormat'
```

Correction : Le mode d'authentification est configurable dans machine.

config, web.config au niveau de la racine ou web.config au niveau de l'application :

- Localisez et ouvrez le fichier de configuration où les informations d'identification sont stockées
- Trouver l'élément <credentials>
- Le cas échéant, supprimez la section

Cela supprimera toutes les références aux utilisateurs stockés dans les fichiers de configuration.

OU

Entrez la commande suivante dans PowerShell pour configurer :
Remove-WebConfigurationProperty -pspath 'MACHINE/WEBROOT/APPHOST/<website name>' -filter 'system.web/authentication/forms/credentials' -name '.'

Valeur par défaut : méthode passwordFormat par défaut est SHA1.

2- Recommandations de configuration ASP.NET

Cette section contient des recommandations spécifiques à ASP.NET.

Règle 1 : S'assurer que la "méthode de déploiement au détail" est définie

La description : Le commutateur <deployment retail> est destiné à être utilisé par les serveurs IIS de production. Ce commutateur est utilisé pour aider les applications d'e-services à s'exécuter avec les meilleures performances possibles et le moins possible de fuites d'informations de sécurité en désactivant la capacité de l'application à générer une sortie de trace sur une page, en désactivant la capacité d'afficher des messages d'erreur détaillés aux utilisateurs finaux et en désactivant le commutateur de débogage. Souvent, les commutateurs et les options axés sur les développeurs, tels que le suivi des demandes ayant échoué et le débogage, sont activés pendant le développement actif. Il est recommandé que la méthode de déploiement sur tout serveur de production soit définie sur retail .

Raisonnement : L'utilisation du commutateur spécialement conçu pour les serveurs IIS de production éliminera le risque de fuites d'informations vitales sur les applications d'e-services et le système qui se produiraient autrement

si le traçage ou le débogage devaient être laissés activés, ou si les erreurs personnalisées devaient être laissées de côté.

Audit : Après le prochain redémarrage d'IIS, ouvrez le fichier machine.config et vérifiez que <deployment retail="true" /> reste défini sur true .

```
<systeme.web>
  <deployment retail="true" />
</system.web>
```

Correction :

- Ouvrez le fichier machine.config situé dans : %systemroot%\Microsoft.NET\Framework<bitness (si ce n'est pas le 32 bits)>\<framework version>\CONFIG
- Ajoutez la ligne <deployment retail="true" /> dans la section <system.web>
- Si les systèmes sont en 64 bits, faites de même pour le fichier machine.config situé dans : %systemroot%\Microsoft.NET\Framework<bitness (si ce n'est pas le 32 bits)>\<framework version>\CONFIG

Valeur par défaut : La balise <deployment retail> n'est pas incluse dans machine.config par défaut.

Règle 2 : Assurez-vous que le "débogage" est désactivé

La description : Les développeurs activent souvent le mode de débogage pendant le développement ASP.NET actif afin qu'ils n'aient pas à vider continuellement le cache de leur navigateur chaque fois qu'ils modifient un gestionnaire de ressources. Le problème surviendrait si cela était laissé "activé" ou défini sur "vrai". La sortie de débogage de la compilation est affichée à l'utilisateur final, permettant aux personnes malveillantes d'obtenir des informations détaillées sur les applications d'e-services.
Il s'agit d'une recommandation de défense en profondeur en raison du <deployment retail="true" /> dans le fichier de configuration machine.config qui remplace tous les paramètres de débogage. Il est recommandé de désactiver le débogage.

Raisonnement : Définir <compilation debug> sur false garantit que les informations d'erreur détaillées ne s'affichent pas par inadvertance lors de l'utilisation de l'application d'e-services en direct, atténuant ainsi le risque que des fuites d'informations sur l'application ne tombent entre des mains peu

scrupuleuses.

Audit : Recherchez et ouvrez le fichier web.config relatif au serveur ou à l'application d'e-services spécifique qui a été configuré. Localisez le commutateur <compilation debug> et vérifiez qu'il est défini sur false.

```
<configuration>
 <systeme.web>
  <compilation debug="false" />
 </system.web>
</configuration>
```

OU

Pour vérifier à l'aide de PowerShell, saisissez la commande suivante :
Get-WebConfigurationProperty -pspath 'MACHINE/WEBROOT/APPHOST/<website name>' -filter "system.web/compilation" -name "debug" | format-list Name, Value

Correction : Pour utiliser l'interface utilisateur pour effectuer cette modification :

- Ouvrez IIS Manager et naviguez sur le serveur, le site ou l'application d'e-services souhaité
- Dans Affichage des fonctionnalités, double-cliquez sur Compilation .NET
- Sur la page Compilation .NET, dans la section Comportement, assurez-vous que le champ Debug est défini sur False
- Lorsque vous avez terminé, cliquez sur Appliquer dans le volet Actions

Remarque : Le commutateur <compilation debug> ne sera pas présent dans le fichier web.config à moins qu'il n'ait été ajouté manuellement ou qu'il n'ait été précédemment configuré à l'aide de l'interface graphique du gestionnaire IIS.

OU

Entrez la commande suivante dans PowerShell pour configurer :
Set-WebConfigurationProperty -pspath 'MACHINE/WEBROOT/APPHOST/<website name>' -filter "system.web/compilation" -name "debug" -value "False"

Valeur par défaut : La compilation des binaires de débogage n'est pas activée par défaut.

Règle 3 : Assurez-vous que les messages d'erreur personnalisés ne sont pas désactivés

La description : Lorsqu'une application ASP.NET échoue et provoque une erreur de serveur interne HTTP/1.x 500, ou qu'une configuration de fonctionnalité (telle que le filtrage des demandes) empêche l'affichage d'une page, un message d'erreur est généré. Les administrateurs peuvent choisir si l'application d'e-services doit ou non afficher un message convivial pour le client, un message d'erreur détaillé pour le client ou un message d'erreur détaillé pour localhost uniquement. La balise <customErrors> dans le fichier web.config a trois modes :

- Activé : spécifie que les erreurs personnalisées sont activées. Si aucun attribut defaultRedirect n'est spécifié, les utilisateurs voient une erreur générique. Les erreurs personnalisées sont affichées aux clients distants et à l'hôte local
- Désactivé : spécifie que les erreurs personnalisées sont désactivées. Les erreurs ASP.NET détaillées sont présentées aux clients distants et à l'hôte local
- RemoteOnly : spécifie que les erreurs personnalisées sont affichées uniquement pour les clients distants et que les erreurs ASP.NET sont affichées pour l'hôte local. Ceci est la valeur par défaut

Il s'agit d'une recommandation de défense en profondeur en raison du <deployment retail="true" /> dans le fichier machine.config qui remplace tous les paramètres de customErrors à désactiver. Il est recommandé que customErrors soit toujours réglé sur On ou RemoteOnly.

Raisonnement : customErrors peut être défini sur On ou RemoteOnly sans divulguer des informations détaillées sur l'application d'e-services au client. S'assurer que customErrors n'est pas défini sur Off aidera à atténuer le risque que des personnes malveillantes apprennent des informations détaillées sur les erreurs d'application et la configuration du serveur.

Audit : Recherchez et ouvrez le fichier web.config pour l'application/le site et vérifiez que la balise a soit <customErrors mode="RemoteOnly" /> ou <customErrors mode="On" /> défini.

OU

Pour vérifier à l'aide de PowerShell, saisissez la commande suivante :
Get-WebConfigurationProperty -pspath 'MACHINE/WEBROOT/APPHOST/<website name' -filter "system.web/customErrors" -name "mode"

Correction : customErrors peut être défini pour un serveur, un site ou une application d'e-services à l'aide de l'interface graphique du gestionnaire IIS, à l'aide des commandes AppCmd.exe dans une fenêtre de ligne de commande, en modifiant directement les fichiers de configuration ou en écrivant des scripts WMI. Effectuez les opérations suivantes pour définir le mode customErrors sur RemoteOnly ou On pour un site Web dans l'interface graphique du gestionnaire IIS :

- Ouvrez l'interface graphique du gestionnaire IIS et accédez au site à configurer
- Dans l'affichage des fonctionnalités, recherchez et double-cliquez sur l'icône Pages d'erreur .NET
- Dans le volet Actions, cliquez sur Modifier les paramètres de la fonctionnalité
- Dans la boîte de dialogue modale, choisissez On ou Remote Only pour les paramètres de mode
- Cliquez sur OK

OU

Entrez la commande suivante dans PowerShell pour configurer :
Set-WebConfigurationProperty -pspath 'MACHINE/WEBROOT/APPHOST/Default Web Site' -filter "system.web/customErrors" -name "mode" -value "RemoteOnly"

Valeur par défaut : La valeur par défaut est <customErrors mode= "RemoteOnly" />.

Règle 4 : Assurez-vous que les erreurs détaillées HTTP IIS ne s'affichent pas à distance

La description : Les pages d'erreur d'un site Web sont souvent configurées pour afficher des informations d'erreur détaillées à des fins de dépannage lors des tests ou du déploiement initial. Pour empêcher les utilisateurs non autorisés de visualiser ces informations privilégiées, les pages d'erreur détaillées

ne doivent pas être vues par les utilisateurs distants. Ce paramètre peut être modifié dans le paramètre d'attribut errorMode pour les pages d'erreur d'un site Web. Par défaut, l'attribut errorMode est défini dans le fichier Web.config pour l'application d'e-services et se trouve dans l'élément <httpErrors> du

Section <system.webServer> . Il est recommandé d'empêcher l'affichage à distance des erreurs personnalisées.

Raisonnement : Les informations contenues dans les messages d'erreur personnalisés peuvent fournir des indices sur le fonctionnement des applications d'e-services, ouvrant des vecteurs d'attaque inutiles. S'assurer que les erreurs personnalisées ne sont jamais affichées à distance peut aider à atténuer le risque que des personnes malveillantes obtiennent des informations sur le fonctionnement de l'application.

Audit : L'attribut errorMode est défini dans le fichier Web.config du site Web ou de l'application dans l'élément <httpErrors> de la section <system.webServer> . Accédez au fichier web.config et vérifiez que errorMode est défini sur DetailLocalOnly ou Custom:

```
<systeme.web>
 <system.webServer>
  <httpErrors errorMode="DetailedLocalOnly">
  </httpErrors>
 </system.webServer>
</system.web>
```

OU

Pour vérifier à l'aide de PowerShell, saisissez la commande suivante :

```
Get-WebConfigurationProperty -pspath 'MACHINE/WEBROOT/
APPHOST/<website name>'
-filter "system.webServer/httpErrors" -name "errorMode"
```

Correction :

La section suivante décrit comment modifier l'attribut errorMode en DetailLocalOnly ou Custom pour un site Web à l'aide du gestionnaire IIS :

- Ouvrir IIS Manager avec des privilèges administratifs
- Dans le volet Connexions à gauche, développez le serveur, puis développez le dossier Sites

- Sélectionnez l'application d'e-services à configurer
- Dans Affichage des fonctionnalités, sélectionnez Pages d'erreur, dans le volet Actions, sélectionnez Ouvrir la fonctionnalité
- Dans le volet Actions, sélectionnez Modifier les paramètres de la fonctionnalité
- Dans la boîte de dialogue Modifier les paramètres des pages d'erreur, sous Réponses aux erreurs, sélectionnez soit Pages d'erreur personnalisées, soit Erreurs détaillées pour les requêtes locales et pages d'erreur personnalisées pour les requêtes distantes
- Cliquez sur OK et quittez la boîte de dialogue Modifier les paramètres des pages d'erreur

OU

Entrez la commande suivante dans PowerShell pour configurer :
Set-WebConfigurationProperty -pspath 'MACHINE/WEBROOT/APPHOST/<website name>' -filter "system.webServer/httpErrors" -name "errorMode" -value "DetailedLocalOnly"

Valeur par défaut : Le errorMode par défaut est DetailLocalOnly.

Règle 5 : Assurez-vous que le traçage de la pile ASP.NET n'est pas activé

La description : L'élément de trace configure le service de traçage de code ASP.NET qui contrôle la manière dont les résultats de la trace sont collectés, stockés et affichés. Lorsque le suivi est activé, chaque demande de page génère des messages de suivi qui peuvent être ajoutés à la sortie de la page ou stockés dans un journal de suivi de l'application.
Il s'agit d'une recommandation de défense en profondeur en raison du <deployment retail="true" /> dans le fichier machine.config qui remplace tous les paramètres de suivi de pile ASP.NET qui restent activés. Il est recommandé de désactiver le traçage de pile ASP.NET.

Raisonnement : Dans un site Web actif, le traçage ne doit pas être activé car il peut afficher des informations de configuration sensibles et des informations détaillées sur le traçage de la pile à toute personne qui consulte les pages du site. Si nécessaire, l'attribut localOnly peut être défini sur true pour afficher les informations de trace uniquement pour les requêtes localhost. S'assurer que le suivi de la pile ASP.NET n'est pas activé contribuera à atténuer le risque que des personnes malveillantes apprennent des informations détaillées sur

le suivi de la pile.

Audit : Le traçage est paramétrable à plusieurs niveaux :

- Machine.config
- Web.config de niveau racine
- Web.config au niveau de l'application d'e-services
- Web.config au niveau du répertoire virtuel ou physique
- Niveau de page ASP.Net individuel

Vérifiez que le traçage ASP.NET n'est pas activé, via une base par page dans l'application d'e-services. Assurez-vous que l'attribut de trace n'est pas activé :

```
Trace="true"
```

Sur une base d'application comme dans le web.config, assurez-vous que le traçage n'est pas activé comme :

```
<configuration>
 <systeme.web>
  <trace enabled="true">
 </system.web>
</configuration>
```

OU

Pour vérifier à l'aide de PowerShell, saisissez la commande suivante :

```
Get-WebConfigurationProperty -pspath 'MACHINE/WEBROOT/
APPHOST/<website name>' -filter "system.web/trace" -name "enabled" |
Format-List Name, Value
```

Correction :

- Assurez -vous que <deployment retail="true" /> est activé dans machine. config.
- Supprimez toutes les références d'attribut au traçage ASP.NET en supprimant les attributs trace et trace enable.

Par page :

Supprimez toute référence à :

```
Trace="True"
```

Par candidature :

```
<configuration>
```

```
<systeme.web>
 <trace enabled="true">
 </system.web>
</configuration>
```

OU

Entrez la commande suivante dans PowerShell pour configurer :

```
Set-WebConfigurationProperty -pspath 'MACHINE/WEBROOT/
APPHOST/<website name>' -filter "system.web/trace" -name "enabled" -value
"False"
```

Valeur par défaut : La valeur par défaut du traçage ASP.NET est off.

Règle 6 : Assurez-vous que le mode « httpcookie » est configuré pour l'état de la session

La description : Un cookie de session associe les informations de session aux informations client pour cette session, qui peuvent être la durée de la connexion d'un utilisateur à un site. Le cookie est transmis dans un en-tête HTTP avec toutes les requêtes entre le client et le serveur.
Les informations de session peuvent également être stockées dans l'URL. Cependant, le stockage des informations de session de cette manière a des implications sur la sécurité qui peuvent ouvrir des vecteurs d'attaque tels que le détournement de session. Une méthode efficace utilisée pour empêcher les attaques de détournement de session consiste à forcer les applications d'e-services à utiliser des cookies pour stocker le jeton de session. Ceci est accompli en définissant l'attribut cookieless du nœud sessionState sur UseCookies ou False qui à son tour gardera les données d'état de session hors de l'URI. Il est recommandé de configurer l'état de la session sur UseCookies.

Raisonnement : Les cookies qui ont été correctement configurés aident à atténuer le risque d'attaques telles que les tentatives de détournement de session en empêchant ASP.NET d'avoir à déplacer les informations de session vers l'URL ; le déplacement des informations de session dans l'URI entraîne l'affichage des ID de session dans les journaux de proxy et est accessible au script client via document.location .

Audit : Recherchez et ouvrez le fichier web.config pour l'application/le site

et vérifiez que la balise sessionState est configurée pour utiliser des cookies :

```
<systeme.web>
 <sessionState cookieless="UseCookies" />
</system.web>
```

OU

Pour vérifier à l'aide de PowerShell, saisissez la commande suivante :

```
Get-WebConfigurationProperty -pspath 'MACHINE/WEBROOT/
APPHOST/<website name>' -filter "system.web/sessionState" -name "mode"
```

Correction : SessionState peut être défini sur UseCookies à l'aide de l'interface graphique du gestionnaire IIS, à l'aide des commandes AppCmd.exe dans une fenêtre de ligne de commande, en modifiant directement les fichiers de configuration ou en écrivant scripts WMI. Effectuez les opérations suivantes pour définir l'attribut sans cookie du nœud sessionState sur UseCookies dans l'interface graphique du gestionnaire IIS :

- Ouvrez l'interface graphique du gestionnaire IIS et naviguez sur l'application d'e-services souhaité
- Dans l'affichage des fonctionnalités, recherchez et double-cliquez sur l'icône État de la session
- Dans la section Paramètres des cookies, choisissez Utiliser les cookies dans le menu déroulant Mode
- Dans le volet Actions, cliquez sur Appliquer

Pour utiliser AppCmd.exe pour configurer sessionState au niveau du serveur, la commande ressemblerait à ceci :

```
%systemroot%\system32\inetsrv\appcmd set config /commit:WEBROOT
/section:sessionState /cookieless:UseCookies /cookieName:ASP.NET_
SessionID /timeout:20
```

Lorsque Appcmd.exe est utilisé pour configurer l'élément <sessionstate> au niveau global dans IIS, le commutateur /commit:WEBROOT doit être inclus afin que les modifications de configuration soient apportées au fichier racine web.config au lieu de ApplicationHost.config .

OU

Entrez la commande suivante dans PowerShell pour configurer :

```
Set-WebConfigurationProperty -pspath 'MACHINE/WEBROOT/
```

```
APPHOST/<website name>' -filter "system.web/sessionState" -name "mode"
-value "StateServer"
```

Valeur par défaut : Par défaut, IIS conserve les données d'état de session pour une application d'e-services de code managé dans le processus de travail où l'application s'exécute, par exemple In Process.

Règle 7 : Assurez-vous que les "cookies" sont définis avec l'attribut HttpOnly

La description : L'attribut httpOnlyCookies du nœud httpCookies détermine si IIS définira l'indicateur HttpOnly sur les cookies HTTP qu'il définit. Le drapeau HttpOnly indique à l'agent utilisateur que le cookie ne doit pas être accessible par un script côté client (c'est-à-dire document.cookie). Il est recommandé de définir l'attribut httpOnlyCookies sur true.

Raisonnement : Lorsque les cookies sont définis avec l'indicateur HttpOnly, ils ne sont pas accessibles par les scripts côté client exécutés dans le navigateur de l'utilisateur. Empêcher les scripts côté client d'accéder au contenu des cookies peut réduire la probabilité qu'une attaque de script intersite se matérialise en un détournement de session réussi.

Audit : Après le prochain redémarrage d'IIS, recherchez et ouvrez le fichier web.config de l'application dans laquelle les cookies httpOnly ont été activés. Vérifiez que l'attribut httpOnlyCookies est défini sur true : <httpCookies httpOnlyCookies="true" />.

Correction :

- Localisez et ouvrez le fichier web.config de l'application d'e-services
- Ajoutez la balise <httpCookies httpOnlyCookies="true" /> dans <system.web> :

```
<configuration>
 <systeme.web>
 <httpCookies httpOnlyCookies="true" />
 </system.web>
</configuration>
```

Définir la valeur de l'attribut httpOnlyCookies de l'élément httpCookies sur true ajoutera le drapeau HttpOnly à tous les cookies définis par l'application d'e-services. Toutes les versions modernes des navigateurs reconnaissent

l'attribut HttpOnly ; les anciennes versions les traiteront comme des cookies normaux ou les ignoreront simplement complètement.

Valeur par défaut : Par défaut, ASP.NET 2.0 ne force pas les cookies à httpOnly.

Règle 8 : Assurez-vous que la « méthode de validation MachineKey - .Net 3.5 » est configurée

La description : L'élément machineKey du web.config ASP.NET spécifie l'algorithme et les clés qu'ASP.NET utilisera pour le chiffrement. La fonctionnalité Clé de la machine peut être gérée pour spécifier les paramètres de hachage et de chiffrement pour les services d'application tels que l'état d'affichage, l'authentification par formulaires, l'appartenance et les rôles, et l'identification anonyme.
Les méthodes de validation suivantes sont disponibles :

- Advanced Encryption Standard (AES) est relativement facile à mettre en œuvre et nécessite peu de mémoire. AES a une taille de clé de 128, 192 ou 256 bits. Cette méthode utilise la même clé privée pour chiffrer et déchiffrer les données, alors qu'une méthode à clé publique doit utiliser une paire de clés
- Message Digest 5 (MD5) est utilisé pour la signature numérique des applications d'e-services. Cette méthode produit un résumé de message de 128 bits, qui est une forme compressée des données d'origine
- Secure Hash Algorithm (SHA1) est considéré comme plus sûr que MD5 car il produit un résumé de message de 160 bits
- Triple Data Encryption Standard (TripleDES) est une variante mineure de Data Encryption Standard (DES). Il est trois fois plus lent que le DES normal mais peut être plus sécurisé car il a une taille de clé de 192 bits. Si les performances ne sont pas une considération primordiale, envisagez d'utiliser TripleDES

Il est recommandé de configurer les méthodes AES ou SHA1 pour une utilisation au niveau global.

Raisonnement : La définition de la propriété de validation sur AES assurera la protection de la confidentialité et de l'intégrité de l'état de la vue. AES est l'algorithme de chiffrement le plus puissant pris en charge par la propriété de validation. La définition de la propriété de validation sur SHA1 fournira une protection d'intégrité à l'état de la vue. SHA1 est l'algorithme de hachage le plus puissant pris en charge par la propriété de validation.

Audit : Pour vérifier la méthode de validation de la clé machine à l'aide du gestionnaire IIS :

- Ouvrez IIS Manager et accédez au niveau qui a été configuré, le WEBROOT ou le serveur dans ce cas
- Dans la vue des fonctionnalités, double-cliquez sur Machine Key
- Sur la page Clé de la machine, vérifiez que SHA1 est sélectionné dans la liste déroulante des méthodes de validation

Correction : Le chiffrement de la clé machine peut être défini à l'aide de l'interface utilisateur, en exécutant les commandes Appcmd.exe , en modifiant directement les fichiers de configuration ou en écrivant des scripts WMI. Pour définir le chiffrement de la clé machine au niveau global à l'aide d'une commande appcmd.exe :

```
%systemroot%\system32\inetsrv\appcmd set config /commit:WEBROOT
/section:machineKey /validation:SHA1
```

Remarque : lorsque Appcmd.exe est utilisé pour configurer l'élément <machineKey> au niveau global dans IIS, le commutateur /commit:WEBROOT doit être inclus afin que les modifications de configuration soient apportées au fichier racine web.config au lieu de ApplicationHost.config .

Valeur par défaut : La méthode de validation par défaut de la clé machine est SHA1.

Règle 9 : Assurez-vous que la « méthode de validation MachineKey - .Net 4.5 » est configurée

La description : L'élément machineKey du web.config ASP.NET spécifie l'algorithme et les clés qu'ASP.NET utilisera pour le chiffrement. La fonctionnalité Clé de la machine peut être gérée pour spécifier les paramètres de hachage et de chiffrement pour les services d'application tels que l'état d'affichage, l'authentification par formulaires, l'appartenance et les rôles, et l'identification anonyme.

Les méthodes de validation suivantes sont disponibles :

- Advanced Encryption Standard (AES) est relativement facile à mettre en œuvre et nécessite peu de mémoire. AES a une taille de clé de 128, 192 ou 256 bits. Cette méthode utilise la même clé privée pour chiffrer et déchiffrer les données, alors qu'une méthode à clé publique doit utiliser une paire de clés
- Message Digest 5 (MD5) est utilisé pour la signature numérique des

applications d'e-services. Cette méthode produit un résumé de message de 128 bits, qui est une forme compressée des données d'origine
- Secure Hash Algorithm (SHA1) est considéré comme plus sûr que MD5 car il produit un résumé de message de 160 bits
- Triple Data Encryption Standard (TripleDES) est une variante mineure de Data Encryption Standard (DES). Il est trois fois plus lent que le DES normal mais peut être plus sécurisé car il a une taille de clé de 192 bits. Si les performances ne sont pas une considération primordiale, envisagez d'utiliser TripleDES
- Secure Hash Algorithm (SHA-2) est une famille de deux fonctions de hachage similaires, avec différentes tailles de bloc appelées SHA-256 et SHA-512. Ils diffèrent par la taille du mot ; SHAS-256 utilisait des mots de 32 bits et SHA-512 des mots de 64 bits.

Il est recommandé de configurer les méthodes SHA-2 pour une utilisation au niveau global.

Raisonnement : SHA-2 est l'algorithme de hachage le plus puissant pris en charge par la propriété de validation. Il doit donc être utilisé comme méthode de validation pour MachineKey dans .Net 4.5.

Audit : Pour vérifier la méthode de validation de la clé machine à l'aide du gestionnaire IIS :
- Ouvrez IIS Manager et accédez au niveau qui a été configuré, le WEBROOT ou le serveur dans ce cas
- Dans la vue des fonctionnalités, double-cliquez sur Machine Key
- Sur la page Clé de la machine, vérifiez que HMACSHA256 est sélectionné dans la liste déroulante des méthodes de validation

OU

Pour vérifier à l'aide de PowerShell, saisissez la commande suivante :

```
Get-WebConfigurationProperty -pspath 'MACHINE/WEBROOT' -filter "system.web/machineKey" -name "validation"
```

Correction : Le chiffrement de la clé machine peut être défini à l'aide de l'interface utilisateur, en exécutant les commandes Appcmd.exe, en modifiant directement les fichiers de configuration ou en écrivant des scripts WMI. Pour définir le chiffrement de la clé machine au niveau global à l'aide d'une commande appcmd.exe :

```
%systemroot%\system32\inetsrv\appcmd set config /commit:WEBROOT /section:machineKey /validation:HMACSHA256
```

Remarque : lorsque Appcmd.exe est utilisé pour configurer l'élément <machineKey> au niveau global dans IIS, le commutateur /commit:WEBROOT doit être inclus afin que les modifications de configuration soient apportées au fichier racine web.config au lieu de ApplicationHost.config .

OU

Entrez la commande suivante dans PowerShell pour configurer :

```
Set-WebConfigurationProperty -pspath 'MACHINE/WEBROOT' -filter "system.web/machineKey" -name "validation" -value "AES"
```

Valeur par défaut : La méthode de validation par défaut de la clé machine est SHA256.

Règle 10 : S'assurer que le niveau de confiance .NET global est configuré

La description : Cela s'applique uniquement à .Net 2.0. Les versions futures ont cessé de prendre en charge cette fonctionnalité.
Le niveau de confiance d'une application d'e-services détermine les autorisations accordées par la stratégie de sécurité d'accès au code (CAS) ASP.NET. CAS définit deux catégories de confiance : confiance totale et confiance partielle. Une application d'e-services qui dispose d'autorisations de confiance totale peut accéder à tous les types de ressources sur un serveur et effectuer des opérations privilégiées, tandis que les applications d'e-services qui s'exécutent avec une confiance partielle ont différents niveaux d'autorisations d'exploitation et d'accès aux ressources.
Les valeurs possibles pour la propriété Level de la classe TrustSection sont :
Complet : spécifie des autorisations illimitées et accorde à l'application d'e-services ASP.NET des autorisations pour accéder à toute ressource soumise à la sécurité du système d'exploitation ; toutes les opérations privilégiées sont prises en charge

Élevé : spécifie un niveau élevé de sécurité d'accès au code qui empêche l'application d'e-services d'effectuer les actions suivantes :
- Appeler du code non managé o Appeler les composants réparés
- Écrire dans le journal des événements
- Accéder aux files d'attente Microsoft Windows Message Queuing
- Accéder aux sources de données ODBC, OLD DB ou Oracle

Moyen : spécifie un niveau moyen de sécurité d'accès au code, ce qui signifie

qu'en plus des restrictions pour Élevé, l'application d'e-services ASP.NET ne peut effectuer aucune des opérations suivantes :
- Accéder aux fichiers en dehors du répertoire de l'application d'e-services o Accéder au registre

Bas : spécifie un niveau bas de sécurité d'accès au code, ce qui signifie qu'en plus des restrictions pour Moyen, l'application d'e-services ne peut pas effectuer l'une des actions suivantes :
- Écrire dans le système de fichiers
- Appelez la méthode System.Security.CodeAccessPermission.Assert pour étendre les autorisations aux ressources
- Minimal : spécifie un niveau minimal de sécurité d'accès au code, ce qui signifie que l'application d'e-services n'a que l'autorisation d'exécution

Il est recommandé de définir le niveau de confiance .NET global sur Moyen ou inférieur.

Raisonnement : Le CAS détermine les autorisations accordées à l'application d'e-services sur le serveur. La définition d'un niveau de confiance minimal compatible avec les applications d'e-services limitera les dommages potentiels qu'une application d'e-services compromise pourrait causer à un système.

Audit : Pour vérifier le niveau de confiance .NET global à l'aide du gestionnaire IIS :
- Ouvrez IIS Manager et accédez au niveau qui a été configuré, le serveur dans cet exemple
- Dans la vue des fonctionnalités, double-cliquez sur Niveaux de confiance .NET
- Sur la page Niveaux de confiance .NET, vérifiez que Moyen (web_mediumtrust.config) est sélectionné dans la liste déroulante Niveau de confiance

OU

Pour vérifier à l'aide de PowerShell, saisissez la commande suivante :

```
Get-WebConfigurationProperty -pspath 'MACHINE/WEBROOT' -filter "system.web/trust" -name "level"
```

Correction :
Le niveau de confiance peut être défini à l'aide de l'interface utilisateur, en exécutant les commandes Appcmd.exe, en modifiant directement les fichiers de configuration ou en écrivant des scripts WMI. Pour définir le niveau de confiance .Net sur Moyen au niveau du serveur à l'aide d'une commande

appcmd.exe :
%systemroot%\system32\inetsrv\appcmd set config /commit:WEBROOT /section:trust /level:Medium

Lorsque Appcmd.exe est utilisé pour configurer l'élément au niveau global dans IIS, le commutateur /commit:WEBROOT doit être inclus afin que les modifications de configuration soient apportées au fichier racine web.config au lieu de ApplicationHost.config .

OU

Entrez la commande suivante dans PowerShell pour configurer :
Set-WebConfigurationProperty -pspath 'MACHINE/WEBROOT' -filter "system.web/trust" -name "level" -value "Medium"

Valeur par défaut : Par défaut, les applications d'e-services ASP.NET s'exécutent avec le paramètre de confiance totale.

Règle 11 : Assurez-vous que l'en-tête X-Powered-By est supprimé

La description : Les en-têtes x-powered-by peuvent spécifier la technologie sous-jacente utilisée par une application d'e-services. Les attaquants peuvent effectuer une reconnaissance sur un site Web en utilisant ces en-têtes de réponse. Cet en-tête pourrait être utilisé pour cibler des attaques pour des vulnérabilités connues spécifiques associées à la technologie sous-jacente. La suppression de cet en-tête empêchera le ciblage de votre application d'e-services pour des exploits spécifiques par des attaquants non déterminés.

Raisonnement : Bien que ce ne soit pas le seul moyen d'identifier un site via les en-têtes de réponse, cela le rend plus difficile et empêche certains attaquants potentiels.

Audit : Pour vérifier à l'aide d'AppCmd.exe, saisissez la commande suivante :
%systemroot%\system32\inetsrv\appcmd.exe list config -section:system.webServer/httpProtocol

Correction : Entrez la commande suivante dans AppCmd.exe pour configurer :
%systemroot%\system32\inetsrv\appcmd.exe set config -section:system.webServer/httpProtocol /-"customHeaders.[name='X-Powered-By']" /commit:apphost

OU

Entrez la commande suivante dans PowerShell pour configurer :
Remove-WebConfigurationProperty -pspath 'MACHINE/WEBROOT/APPHOST' -filter "system.webserver/httpProtocol/customHeaders" -name "." -AtElement @{name='XPowered-By'}

Règle 12 : Assurez-vous que l'en-tête du serveur est supprimé

La description : L'en-tête du serveur peut spécifier la technologie sous-jacente utilisée par une application d'e-services. Les attaquants peuvent effectuer une reconnaissance sur un site Web en utilisant ces en-têtes de réponse. Cet en-tête pourrait être utilisé pour cibler des attaques pour des vulnérabilités connues spécifiques associées à la technologie sous-jacente. La suppression de cet en-tête empêchera le ciblage de votre application d'e-services pour des exploits spécifiques par des attaquants non déterminés.

Raisonnement : Bien que ce ne soit pas le seul moyen d'identifier un site via les en-têtes de réponse, cela le rend plus difficile et empêche certains attaquants potentiels. La directive de suppression d'en-tête de serveur est une nouvelle fonctionnalité d'IIS 10 qui peut aider à atténuer ce risque.

Audit : Pour vérifier à l'aide d'AppCmd.exe, saisissez la commande suivante :
%systemroot%\system32\inetsrv\appcmd.exe list config -section:system.webServer/security/requestFiltering

OU

Pour vérifier à l'aide de PowerShell, saisissez la commande suivante :
Get-WebConfigurationProperty -pspath machine/webroot/apphost -filter 'system.webserver/security/requestfiltering ' -name 'removeServerHeader'

Correction : Entrez la commande suivante pour utiliser AppCmd.exe pour configurer :
%systemroot%\system32\inetsrv\appcmd.exe set config -section:system.webServer/security/requestFiltering /removeServerHeader:"True" /commit:apphost

OU

Entrez la commande suivante dans PowerShell pour configurer :

```
Set-WebConfigurationProperty -pspath 'MACHINE/WEBROOT/
APPHOST/' -filter "system.webServer/security/requestFiltering" -name
"removeServerHeader" value "True"
```

Impact : Cela supprimera l'en-tête du serveur.

Valeur par défaut : Microsoft IIS/10.0

3- Filtrage des requêtes et autres modules de restriction

Introduit dans IIS 7.0 pour la première fois, le filtrage des demandes est un module puissant qui fournit un ensemble configurable de règles qui permet aux administrateurs d'autoriser ou de rejeter les types de demandes qu'ils déterminent comme devant être autorisées ou rejetées au niveau du serveur de l'application d'e-services.
Les versions antérieures d'Internet Information Services fournissaient l'outil UrlScan, qui était fourni en tant que module complémentaire pour permettre aux administrateurs système d'appliquer des politiques de sécurité plus strictes sur leurs serveurs Web. Toutes les fonctionnalités de base d'URLScan ont été intégrées au module de filtrage des demandes. En raison de la nature proche des fonctionnalités de ces deux outils, une référence aux paramètres URLScan hérités sera faite le cas échéant.
IIS 8 a également introduit des modules pour les restrictions d'adresses IP dynamiques. Ce module peut être configuré pour bloquer automatiquement l'accès au site Web en fonction de règles spécifiques.
Remarque : le filtrage des demandes et les restrictions IP et de domaine doivent être activés en tant que service de rôle sous IIS afin de configurer l'une de ses fonctionnalités.

Règle 1 : Assurez-vous que 'maxAllowedContentLength' est configuré

La description : Le filtre de requête maxAllowedContentLength est la taille maximale de la requête http, mesurée en octets, qui peut être envoyée d'un client au serveur. La configuration de cette valeur permet de restreindre la taille totale de la demande à une valeur configurée. Il est recommandé de limiter la taille globale des requêtes à une valeur maximale adaptée au e-services.

Raisonnement : La définition d'une valeur appropriée qui a été testée

pour le filtre maxAllowedContentLength réduira l'impact qu'une requête anormalement volumineuse aurait autrement sur IIS et/ou les applications d'e-services. Cela permet de garantir la disponibilité du contenu et des services Web, et peut également aider à atténuer le risque d'attaques de type débordement de mémoire tampon dans les composants non gérés.

Audit : En cas de dépassement de la valeur configurée définie pour le filtre de demande, IIS lancera un code d'état 404.13.
Pour vérifier manuellement la modification, recherchez et ouvrez le fichier web.config de l'application d'e-services dans lequel le filtre de demande a été défini. Assurez-vous que la valeur définie pour maxAllowedContentLength est celle qui a été définie. L'exemple de 28,6 Mo maximum afficherait :

```
<configuration>
 <system.webServer>
  <security>
   <requestFiltering>
    <requestLimits
     maxAllowedContentLength="30000000" />
   </requestFiltering>
  </security>
 </system.webServer>
</configuration>
```

OU

Pour vérifier à l'aide de PowerShell, saisissez la commande suivante :

```
Get-WebConfigurationProperty -pspath 'MACHINE/WEBROOT/APPHOST'
-filter
"system.webServer/security/requestFiltering/requestLimits" -name
"maxAllowedContentLength"
```

Correction :
Le filtre de demande MaxAllowedContentLength peut être défini pour une application d'e-services à l'aide de l'interface graphique du gestionnaire IIS, à l'aide des commandes AppCmd.exe dans une fenêtre de ligne de commande et/ou en modifiant directement les fichiers de configuration. Pour configurer à l'aide de l'interface graphique du gestionnaire IIS :

- ☑ Ouvrir le gestionnaire des services d'information Internet (IIS)

- Dans le volet Connexions, cliquez sur l'application d'e-services à configurer
- Dans le volet Accueil, double-cliquez sur Filtrage des demandes
- Cliquez sur Modifier les paramètres de fonctionnalité... dans le volet Actions
- Dans la section Limites de la demande, saisissez la longueur maximale du contenu en octets qui permettra aux applications d'e-services de conserver leur fonctionnalité prévue, par exemple 3 000 000 (env. 28,6 Mo)

Entrez la commande suivante dans AppCmd.exe pour configurer :

```
%systemroot%\system32\inetsrv\appcmd set config /section:requestfiltering /requestLimits.maxAllowedContentLength:30000000
```

OU

Entrez la commande suivante dans PowerShell pour configurer :

```
Set-WebConfigurationProperty -pspath 'MACHINE/WEBROOT/APPHOST' -filter "system.webServer/security/requestFiltering/requestLimits" -name "maxAllowedContentLength" -value 30000000
```

Valeur par défaut : Lorsque le filtrage des demandes est installé sur un système, la valeur par défaut est : maxAllowedContentLength="30000000", soit environ 28,6 Mo.

Règle 2 : Assurez-vous que le "filtre de requête maxURL" est configuré

La description : L'attribut maxURL de la propriété <requestLimits> est la longueur maximale (en octets) dans laquelle une URL demandée peut être (hors chaîne de requête) pour qu'IIS l'accepte.
La configuration de ce filtre de requêtes permet aux administrateurs de limiter la longueur des requêtes que le serveur acceptera. Il est recommandé de limiter la longueur de l'URL.

Raisonnement : Avec un filtre de demande correctement configuré limitant la quantité de données acceptées dans l'URL, les risques de comportements d'application indésirables affectant la disponibilité du contenu et des services sont réduits.

Audit : IIS enregistrera un état HTTP 404.14 si l'URL demandée a été rejetée

car elle dépasse la longueur définie dans le filtre.
Pour vérifier manuellement la modification, recherchez et ouvrez le fichier web.config de l'application d'e-services dans lequel le filtre de demande a été défini. Vérifiez la valeur définie pour maxURL.

```
<configuration>
 <system.webServer>
  <security>
   <requestFiltering>
    <requestLimits maxURL="4096" />
   </requestFiltering>
  </security>
 </system.webServer>
</configuration>
```

OU

Pour vérifier à l'aide de PowerShell, saisissez la commande suivante :

```
Get-WebConfigurationProperty -pspath 'MACHINE/WEBROOT/APPHOST'
-filter
"system.webServer/security/requestFiltering/requestLimits" -name "maxUrl"
```

Correction : Le filtre de requête MaxURL peut être défini pour un serveur, un site Web ou une application à l'aide de l'interface graphique du gestionnaire IIS, à l'aide des commandes AppCmd.exe dans une fenêtre de ligne de commande et/ou en modifiant directement les fichiers de configuration. Pour configurer à l'aide de l'interface graphique du gestionnaire IIS :

- Ouvrir le gestionnaire des services d'information Internet (IIS)
- Dans le volet Connexions, cliquez sur la connexion, le site, l'application ou l'annuaire à configurer
- Dans le volet Accueil, double-cliquez sur Filtrage des demandes
- Cliquez sur Modifier les paramètres de fonctionnalité... dans le volet Actions
- Sous la section Limites de la demande, entrez la longueur maximale de l'URL en octets qui a été testée avec des applications Web

Entrez la commande suivante dans AppCmd.exe pour configurer :

```
%systemroot%\system32\inetsrv\appcmd set config /section:requestfiltering
/requestLimits.maxURL:4096
```

OU

Entrez la commande suivante dans PowerShell pour configurer :

```
Set-WebConfigurationProperty -pspath 'MACHINE/WEBROOT/APPHOST'
-filter "system.webServer/security/requestFiltering/requestLimits" -name
"maxUrl" value 4096
```

Valeur par défaut : Lorsque Request Filtering est installé sur un système, la valeur par défaut de maxURL="4096".

Règle 3 : Assurez-vous que le « filtre de requête MaxQueryString » est configuré

La description : Le filtre de requête MaxQueryString décrit la limite supérieure de la longueur de la chaîne de requête que le serveur IIS configuré autorisera pour les sites Web ou les applications. Il est recommandé de toujours établir des valeurs pour limiter la quantité de données pouvant être acceptées dans la chaîne de requête.

Raisonnement : Avec un filtre de demande correctement configuré limitant la quantité de données acceptées dans la chaîne de requête, les risques de comportements d'application indésirables tels que les échecs du pool d'applications sont réduits.

Audit : Si une demande est rejetée car elle dépasse la valeur définie dans le filtre de demande maxQueryString , un état HTTP 404.15 est consigné dans le fichier journal IIS.
Pour vérifier manuellement la modification, recherchez et ouvrez le fichier web.config du site Web ou de l'application d'e-services dans laquelle le filtre a été défini. Assurez-vous que la valeur définie pour maxQueryString est celle qui a été configurée.

```
<configuration>
 <system.webServer>
  <security>
   <requestFiltering>
    <requestLimits
     maxQueryString="2048" />
   </requestFiltering>
```

```
  </security>
 </system.webServer>
</configuration>
```

OU

Pour vérifier à l'aide de PowerShell, saisissez la commande suivante :

```
Get-WebConfigurationProperty -pspath 'MACHINE/WEBROOT/APPHOST'
-filter
"system.webServer/security/requestFiltering/requestLimits" -name
"maxQueryString"
```

Correction : Le filtre de demande MaxQueryString peut être défini pour un serveur, un site Web ou une application d'e-services à l'aide de l'interface graphique du gestionnaire IIS, à l'aide des commandes AppCmd.exe dans une fenêtre de ligne de commande et/ou en modifiant directement les fichiers de configuration. Pour configurer à l'aide de l'interface graphique du gestionnaire IIS :

- Ouvrir le gestionnaire des services d'information Internet (IIS)
- Dans le volet Connexions, accédez à la connexion, au site, à l'application d'e-services ou au répertoire à configurer
- Dans le volet Accueil, double-cliquez sur Filtrage des demandes
- Cliquez sur Modifier les paramètres de fonctionnalité... dans le volet Actions
- Sous la section Limites de la demande, entrez une limite supérieure sûre dans la zone de texte Chaîne de requête maximale (octets)

Entrez la commande suivante dans AppCmd.exe pour configurer :

```
%systemroot%\system32\inetsrv\appcmd set config /section:requestfiltering
/requestLimits.maxQueryString:2048
```

OU

Entrez la commande suivante dans PowerShell pour configurer :

```
Set-WebConfigurationProperty -pspath 'MACHINE/WEBROOT/APPHOST'
-filter
"system.webServer/security/requestFiltering/requestLimits" -name
"maxQueryString" -value 2048
```

Valeur par défaut : Lorsque le filtrage des demandes est installé sur un système, la valeur par défaut est maxQueryString="2048".

Règle 2 : S'assurer que les caractères non ASCII dans les URL ne sont pas autorisés

La description : Cette fonctionnalité est utilisée pour autoriser ou rejeter toutes les demandes adressées à IIS qui contiennent des caractères non ASCII. Lors de l'utilisation de cette fonctionnalité, le filtrage des demandes refusera la demande si des caractères de poids fort sont présents dans l'URL. L'équivalent UrlScan est AllowHighBitCharacters. Il est recommandé de rejeter, dans la mesure du possible, les demandes contenant des caractères non ASCII.

Raisonnement : Cette fonctionnalité peut aider à se défendre contre les attaques de canonisation, en réduisant la surface d'attaque potentielle des serveurs, des sites et/ou des applications.

Audit : Si une demande est rejetée car elle contient un caractère de poids fort, un état HTTP 404.12 est consigné dans le fichier journal IIS.
Pour vérifier manuellement la modification, recherchez et ouvrez le fichier web.config du site Web ou de l'application d'e-services dans lequel le filtre de demande a été défini. Assurez-vous que la valeur définie pour le filtre est fausse, en tant que telle :

```
<configuration>
 <system.webServer>
  <security>
   <requestFiltering
    allowHighBitCharacters="false">
   </requestFiltering>
  </security>
 </system.webServer>
</configuration>
```

OU

Pour vérifier à l'aide de PowerShell, saisissez la commande suivante :

```
Get-WebConfigurationProperty -pspath 'MACHINE/WEBROOT/
APPHOST' -filter 'system.webServer/security/requestFiltering' -name
'allowHighBitCharacters'
```

Correction : Le filtre de demande AllowHighBitCharacters peut être défini pour un serveur, un site Web ou une application d'e-services à l'aide de

l'interface graphique du gestionnaire IIS, à l'aide des commandes AppCmd.exe dans une fenêtre de ligne de commande et/ou en modifiant directement les fichiers de configuration. Pour configurer à l'aide de l'interface graphique du gestionnaire IIS :

- Ouvrir le gestionnaire des services d'information Internet (IIS)
- Dans le volet Connexions, accédez à la connexion, au site, à l'application d'e-services ou au répertoire à configurer
- Dans le volet Accueil, double-cliquez sur Filtrage des demandes
- Cliquez sur Modifier les paramètres de fonctionnalité... dans le volet Actions
- Dans la section Général, décochez Autoriser les caractères de poids fort

Remarque : l'interdiction des caractères ASCII à bits élevés dans l'URL peut avoir un impact négatif sur la fonctionnalité des sites nécessitant une prise en charge des langues internationales. Entrez la commande suivante dans AppCmd.exe pour configurer :

```
%systemroot%\system32\inetsrv\appcmd set config /section:requestfiltering
/allowHighBitCharacters:false
```

OU

Entrez la commande suivante dans PowerShell pour configurer :

```
Set-WebConfigurationProperty -pspath 'MACHINE/WEBROOT/
APPHOST' -filter "system.webServer/security/requestFiltering" -name
"allowHighBitCharacters" value « False »
```

Valeur par défaut : Lorsque le filtrage des demandes est installé sur un système, le comportement par défaut consiste à autoriser les caractères de poids fort dans l'URI.

Règle 5 : S'assurer que les demandes à double codage seront rejetées

La description : Cette fonctionnalité de filtrage des demandes empêche les attaques qui reposent sur des demandes à double codage et s'applique si un attaquant soumet une demande à double codage à IIS. Lorsque le filtre de demandes à double codage est activé, IIS passe par un processus à deux itérations de normalisation de la demande. Si la première normalisation diffère de la seconde, la demande est rejetée et le code d'erreur est enregistré en tant que 404.11. Le filtre de requêtes à double encodage était le VerifyNormalization

dans UrlScan. Il est recommandé de rejeter les demandes à double codage.

Raisonnement : Cette fonctionnalité aidera à prévenir les attaques qui s'appuient sur des URL qui ont été conçues pour contenir des requêtes à double codage.

Audit : Si une demande est rejetée parce qu'elle contient une demande à double codage, un état http 404.11 est consigné dans le fichier journal IIS.
Pour vérifier manuellement la modification, recherchez et ouvrez le fichier web.config du site Web ou de l'application d'e-services dans lequel le filtre de demande a été défini. Assurez-vous que la valeur définie pour allowDoubleEscaping est false :

```
<configuration>
 <system.webServer>
  <security>
   <requestFiltering
    allowDoubleEscaping="false">
   </requestFiltering>
  </security>
 </system.webServer>
</configuration>
```

OU

Pour vérifier à l'aide de PowerShell, saisissez la commande suivante :

```
Get-WebConfigurationProperty -pspath 'MACHINE/WEBROOT/APPHOST'
-filter
"system.webServer/security/requestFiltering" -name "allowDoubleEscaping"
```

Correction : Le filtre de demande allowDoubleEscaping peut être défini pour un serveur, un site Web ou une application d'e-services à l'aide de l'interface graphique du gestionnaire IIS, à l'aide des commandes AppCmd. exe dans une fenêtre de ligne de commande et/ou en modifiant directement les fichiers de configuration. Pour configurer à l'aide de l'interface graphique du gestionnaire IIS :

- Ouvrir le gestionnaire des services d'information Internet (IIS)
- Dans le volet Connexions, sélectionnez le site, l'application d'e-services ou l'annuaire à configurer

- Dans le volet Accueil, double-cliquez sur Filtrage des demandes
- Cliquez sur Modifier les paramètres de fonctionnalité... dans le volet Actions
- Dans la section Général, décochez Autoriser la double échappement

Si un nom de fichier dans une URL inclut "+", alors allowDoubleEscaping doit être défini sur true pour autoriser la fonctionnalité.

Entrez la commande suivante dans AppCmd.exe pour configurer :

```
%systemroot%\system32\inetsrv\appcmd set config /section:requestfiltering /allowDoubleEscaping:false
```

OU

Entrez la commande suivante dans PowerShell pour configurer :

```
Set-WebConfigurationProperty -pspath 'MACHINE/WEBROOT/APPHOST' -filter "system.webServer/security/requestFiltering" -name "allowDoubleEscaping" value "True"
```

Valeur par défaut : Lorsque le filtrage des demandes est installé sur un système, le comportement par défaut consiste à ne pas autoriser les demandes codées en double.

Règle 6 : Assurez-vous que la « méthode de suivi HTTP » est désactivée

La description : La méthode HTTP TRACE renvoie le contenu des requêtes HTTP client dans le corps d'entité de la réponse TRACE. Les attaquants pourraient tirer parti de ce comportement pour accéder à des informations sensibles, telles que des données d'authentification ou des cookies, contenues dans les en-têtes HTTP de la requête. Une telle façon d'atténuer cela est d'utiliser l'élément <verbs> du <requestFiltering> collection. L'élément <verbs> remplace les [AllowVerbs] et Fonctionnalités [DenyVerbs] dans UrlScan. Il est recommandé de refuser la méthode HTTP TRACE.

Raisonnement : Les attaquants peuvent abuser de la fonctionnalité HTTP TRACE pour accéder aux informations des en-têtes HTTP telles que les cookies et les données d'authentification. Ce risque peut être atténué en n'autorisant pas le verbe TRACE.

Audit : IIS renvoie une erreur HTTP 404.6 au client lorsque le filtrage des demandes bloque une demande HTTP en raison d'un verbe HTTP refusé. Pour

vérifier manuellement la modification, accédez au fichier web.config pour lequel la modification a été apportée et vérifiez la configuration ci-dessous :

```
<configuration>
 <system.webServer>
  <security>
   <requestFiltering>
    <verbs>
     <add verb="TRACE" allow="false" />
    </verbs>
   </requestFiltering>
  </security>
 </system.webServer>
</configuration>
```

Pour afficher ce filtre de requêtes à l'aide d'une commande AppCmd.exe , exécutez la commande suivante à une invite de commandes avec élévation de privilèges :

```
%systemroot%\system32\inetsrv\appcmd listconfig /section:requestfiltering
```

Correction :

- Ouvrir le gestionnaire des services d'information Internet (IIS)
- Dans le volet Connexions, sélectionnez le site, l'application d'e-services ou l'annuaire à configurer
- Dans le volet Accueil, double-cliquez sur Filtrage des demandes
- Dans le volet Request Filtering, cliquez sur l'onglet HTTP verbs, puis cliquez sur Deny Verb... dans le volet Actions
- Dans la boîte de dialogue Deny Verb, entrez le TRACE, puis cliquez sur OK

Entrez la commande suivante dans AppCmd.exe pour configurer :

```
%systemroot%\system32\inetsrv\appcmd set config /section:requestfiltering
/+verbs.[verb='TRACE',allowed='false']
```

OU

Entrez la commande suivante dans PowerShell pour configurer :

```
Add-WebConfigurationProperty -pspath 'MACHINE/WEBROOT/APPHOST'
-filter
"system.webServer/security/requestFiltering/verbs" -name "." -value @
{verb='TRACE';allowed='False'}
```

Valeur par défaut : Le verbe TRACE n'est pas filtré par défaut.

Règle 7 : S'assurer que les extensions de fichiers non répertoriées ne sont pas autorisées

La description : Le filtre de demande FileExtensions permet aux administrateurs de définir des extensions spécifiques que leur ou leurs serveurs Web autoriseront et refuseront. La propriété allowUnlisted couvrira toutes les autres extensions de fichier non explicitement autorisées ou refusées. Souvent, des extensions telles que .config , .bat , .exe , pour n'en nommer que quelques-uns, ne doivent jamais être servis. Les options AllowExtensions et DenyExtensions sont les équivalents UrlScan. Il est recommandé que toutes les extensions soient interdites au niveau le plus global possible, seules celles nécessaires étant autorisées.

Raisonnement : L'interdiction de toutes les extensions de fichier, à l'exception des extensions nécessaires, peut réduire considérablement la surface d'attaque des applications d'e-services et des serveurs.

Audit : Lorsqu'IIS rejette une demande basée sur un filtre d'extensions de fichier, le code d'erreur consigné est 404.7. Pour vérifier manuellement la modification, recherchez et ouvrez le fichier web.config du site Web ou de l'application d'e-services dans lequel le filtre de demande a été défini. Assurez -vous que <fileExtensions allowUnlisted="false"> . Le web.config suivant interdira toutes les demandes de fichiers qui n'ont pas .asp , .aspx ou .html comme extension :

```
<configuration>
 <system.webServer>
  <security>
   <requestFiltering>
    <fileExtensions allowUnlisted="false">
     <add fileExtension=".asp" allow="true" />
     <add fileExtension=".aspx" allow="true" />
     <add fileExtension=".html" allow="true" />
    </fileExtensions>
   </requestFiltering>
  </security>
 </system.webServer>
```

</configuration>

OU

Pour vérifier à l'aide d'AppCmd.exe, saisissez la commande suivante :
%systemroot%\system32\inetsrv\appcmd list config /section:requestfiltering

OU

Pour vérifier à l'aide de PowerShell, entrez la commande suivante
Get-WebConfigurationProperty -pspath 'MACHINE/WEBROOT/APPHOST'
-filter
"system.webServer/security/requestFiltering/fileExtensions" -neme
« allowUnlisted »

Correction : Le filtre de demande allowUnlisted peut être défini pour un serveur, un site Web ou une application d'e-services à l'aide de l'interface graphique du gestionnaire IIS, à l'aide des commandes AppCmd.exe dans une fenêtre de ligne de commande et/ou en modifiant directement les fichiers de configuration. Pour configurer au niveau du serveur à l'aide de l'interface graphique du gestionnaire IIS :

- Ouvrir le gestionnaire des services d'information Internet (IIS)
- Dans le volet Connexions, sélectionnez le serveur
- Dans le volet Accueil, double-cliquez sur Filtrage des demandes
- Cliquez sur Modifier les paramètres de fonctionnalité... dans le volet Actions
- Dans la section Général, décochez Autoriser les extensions de nom de fichier non répertoriées

Entrez la commande suivante dans AppCmd.exe pour configurer :
%systemroot%\system32\inetsrv\appcmd set config /section :requestfiltering
/fileExtensions.allowunlisted :false

OU

Entrez la commande suivante dans PowerShell pour configurer :
Set-WebConfigurationProperty -pspath 'MACHINE/WEBROOT/APPHOST'
-filter
« system.webServer/security/requestFiltering/fileExtensions » -name
« allowUnlisted » -value « False »

Valeur par défaut : La configuration par défaut du filtrage des demandes permet de demander toutes les extensions de fichiers non répertoriées.

Règle 8 : S'assurer que le gestionnaire n'a pas le droit d'écrire et de scénariser/exécuter

La description : Les mappages de gestionnaires peuvent être configurés pour accorder des autorisations à Read, Write , Script ou Execute en fonction de l'utilisation – lire du contenu statique, télécharger des fichiers, exécuter des scripts, etc. Il est recommandé d'accorder à un gestionnaire Execute/Script ou Write autorisations, mais pas les deux.

Raisonnement : En autorisant à la fois les autorisations d'exécution/de script et d' écriture , un gestionnaire peut exécuter du code malveillant sur le serveur cible. S'assurer que ces deux autorisations ne sont jamais ensemble contribuera à réduire le risque d'exécution de code malveillant sur le serveur.

Audit : Ouvrez le fichier ApplicationHost.config dans %systemroot%\system32\inetsrv\config. Recherchez la section <handlers> et vérifiez que l'attribut accessPolicy ne contient pas Write lorsque Script ou Execute sont présents. Voici un exemple acceptable :

```
<system.webserver>
 <handlers accessPolicy="Lire, Script">
 </handlers>
</system.webserver>
```

OU

Pour vérifier à l'aide de PowerShell, saisissez la commande suivante :

```
Get-WebConfigurationProperty -pspath 'MACHINE/WEBROOT/APPHOST'
-filter "system.webServer/handlers" -name "accessPolicy"
```

Correction : L'attribut accessPolicy dans la section <handlers> de l'un ou l'autre des
ApplicationHost.config (à l'échelle du serveur) ou web.config (site ou application d'e-services) ne doit pas avoir Write présent lorsque Script ou Execute sont présents. Pour résoudre ce problème pour un serveur Web, l'attribut de la section <handlers> du fichier ApplicationHost.config du serveur doit être modifié manuellement. Pour modifier le fichier ApplicationHost.config à l'aide du Bloc-notes, procédez comme suit :

- Ouvrir le Bloc-notes en tant qu'administrateur
- Ouvrez le fichier ApplicationHost.config dans %systemroot%\system32\inetsrv\config

- Modifiez l'attribut accessPolicy de la section <handlers> afin que Write ne soit pas présent lorsque Script ou Execute sont présents

Entrez la commande suivante dans AppCmd.exe pour configurer :

```
%systemroot%\system32\inetsrv\appcmd set config /section:handlers /
accessPolicy:Read,Script
```

OU

Entrez la commande suivante dans PowerShell pour configurer :

```
Set-WebConfigurationProperty -pspath 'MACHINE/WEBROOT/APPHOST'
-filter "system.webServer/handlers" -name "accessPolicy" -value "Read,Script"
```

Remarque : Cette modification de configuration ne peut pas être effectuée à l'aide du Gestionnaire IIS.

Valeur par défaut : Les gestionnaires par défaut accessPolicy sont Read, Script.

Règle 9 : Assurez-vous que 'notListedIsapisAllowed' est défini sur faux

La description : L'attribut notListedIsapisAllowed est un paramètre au niveau du serveur situé dans le ApplicationHost.config dans l'élément <isapiCgiRestriction> du Section <system.webServer> sous <security> . Cet élément garantit que les utilisateurs malveillants ne peuvent pas copier des fichiers binaires ISAPI non autorisés sur le serveur Web, puis les exécuter. Il est recommandé de définir notListedIsapisAllowed sur false.

Raisonnement : Restreindre cet attribut à false permet d'empêcher l'exécution d'extensions ISAPI potentiellement malveillantes.

Audit : Ouvrez le fichier ApplicationHost.config dans %systemroot%\system32\inetsrv\config . Vérifiez que l'attribut notListedIsapisAllowed dans l'élément <isapiCgiRestriction> est défini sur false :

```
<system.webServer>
 <security>
  <isapiCgiRestriction notListedIsapisAllowed="false">
  </isapiCgiRestriction>
```

```
</security>
</system.webServer>
```

OU

Pour vérifier à l'aide de PowerShell, saisissez la commande suivante :

```
Get-WebConfigurationProperty -pspath 'MACHINE/WEBROOT/APPHOST'
-filter
"system.webServer/security/isapiCgiRestriction" -name
"notListedIsapisAllowed"
```

Correction : Pour utiliser IIS Manager pour définir l'attribut notListedIsapisAllowed sur false :

- Ouvrir le gestionnaire IIS en tant qu'administrateur
- Dans le volet Connexions à gauche, sélectionnez le serveur à configurer
- Dans Affichage des fonctionnalités, sélectionnez Restrictions ISAPI et CGI ; dans le volet Actions, sélectionnez Ouvrir la fonctionnalité
- Dans le volet Actions, sélectionnez Modifier les paramètres de la fonctionnalité
- Dans la boîte de dialogue Modifier les paramètres de restrictions ISAPI et CGI, décochez la case Autoriser les modules ISAPI non spécifiés, si elle est cochée
- Cliquez sur OK

Entrez la commande suivante dans AppCmd.exe pour configurer :

```
%systemroot%\system32\inetsrv\appcmd.exe set config section:system.
webServer/security/isapiCgiRestriction /notListedIsapisAllowed:false
```

OU

Entrez la commande suivante dans PowerShell pour configurer :

```
Set-WebConfigurationProperty -pspath 'MACHINE/WEBROOT/APPHOST'
-filter
"system.webServer/security/isapiCgiRestriction" -name
"notListedIsapisAllowed" -value "False"
```

Valeur par défaut : La valeur par défaut de notListedIsapisAllowed est false.

Règle 10 : Assurez-vous que 'notListedCgisAllowed' est défini sur faux

La description : Lattribut notListedCgisAllowed est un paramètre au niveau du serveur situé dans le ApplicationHost.config dans l'élément <isapiCgiRestriction> du Section <system.webServer> sous <security> . Cet élément garantit que les utilisateurs malveillants ne peuvent pas copier des fichiers binaires CGI non autorisés sur le serveur Web, puis les exécuter. Il est recommandé de définir notListedCgisAllowed sur false.

Raisonnement : Restreindre cet attribut à false aidera à empêcher l'exécution d'extensions CGI non répertoriées, y compris des scripts CGI potentiellement malveillants.

Audit : Recherchez et ouvrez le fichier ApplicationHost.config et vérifiez que l'attribut notListedCgisAllowed dans l'élément <isapiCgiRestriction> est défini sur false :

```
<system.webServer>
 <security>
 <isapiCgiRestriction notListedCgisAllowed="false">
 </isapiCgiRestriction>
 </security>
</system.webServer>
```

OU

Pour vérifier à l'aide de PowerShell, saisissez la commande suivante :

```
Get-WebConfigurationProperty -pspath 'MACHINE/WEBROOT/
APPHOST' -filter "system.webServer/security/isapiCgiRestriction" -name
"notListedCgisAllowed"
```

Correction :

Pour définir l'attribut notListedCgisAllowed sur false à l'aide du gestionnaire IIS :

- Ouvrir le gestionnaire IIS en tant qu'administrateur
- Dans le volet Connexions à gauche, sélectionnez le serveur à configurer
- Dans Affichage des fonctionnalités, sélectionnez Restrictions ISAPI et CGI ; dans le volet Actions, sélectionnez Ouvrir la fonctionnalité
- Dans le volet Actions, sélectionnez Modifier les paramètres de la fonctionnalité
- Dans la boîte de dialogue Modifier les paramètres de restrictions ISAPI et CGI, décochez la case Autoriser les modules CGI non spécifiés
- Cliquez sur OK

Entrez la commande suivante dans AppCmd.exe pour configurer :
%systemroot%\system32\inetsrv\appcmd.exe set config section:system.webServer/security/isapiCgiRestriction /notListedCgisAllowed:false

OU

Entrez la commande suivante dans PowerShell pour configurer :
Set-WebConfigurationProperty -pspath 'MACHINE/WEBROOT/APPHOST' -filter "system.webServer/security/isapiCgiRestriction" -name "notListedCgisAllowed" -value "False"

Valeur par défaut : La valeur par défaut de notListedCgisAllowed est false.

Règle 11 : Assurez-vous que les « restrictions d'adresse IP dynamique » sont activées

La description : La fonctionnalité IIS Dynamic IP Address Restrictions peut être utilisée pour contrecarrer les attaques DDos. Ceci est complémentaire aux listes de restrictions d'adresses IP et de noms de domaine qui peuvent être gérées manuellement dans IIS. En revanche, le filtrage dynamique des adresses IP permet aux administrateurs de configurer le serveur pour bloquer l'accès aux adresses IP qui dépassent le seuil de demande spécifié. L'action par défaut Refuser l'action pour les restrictions consiste à renvoyer une réponse Interdit au client.

Raisonnement : Le filtrage dynamique des adresses IP permet aux administrateurs de configurer le serveur pour bloquer l'accès aux adresses IP qui dépassent le nombre spécifié de requêtes ou la fréquence des requêtes. Assurez-vous de recevoir la page Interdit une fois le blocage appliqué.

Audit : Accédez au serveur Web suffisamment de fois pour déclencher la restriction IP en fonction des paramètres saisis.

OU

Pour vérifier à l'aide de PowerShell, saisissez la commande suivante :
Get-WebConfigurationProperty -pspath 'MACHINE/WEBROOT/APPHOST' -filter "system.webServer/security/dynamicIpSecurity/denyByConcurrentRequests" -name "enabled"
Get-WebConfigurationProperty -pspath 'MACHINE/WEBROOT/APPHOST'

-filter "system.webServer/security/dynamicIpSecurity/denyByConcurrentRequests" -name "maxConcurrentRequests"

Correction : Ouvrez le gestionnaire IIS.

- Ouvrez la fonction Adresse IP et restrictions de domaine.
- Cliquez sur Modifier les paramètres de restrictions dynamiques.
- Vérifiez l'adresse IP de refus en fonction du nombre de demandes simultanées et l'adresse IP de refus en fonction du nombre de demandes sur une période de temps. Les valeurs peuvent être ajustées selon les besoins de votre environnement spécifique.

OU

Entrez la commande suivante dans PowerShell pour configurer :

```
Set-WebConfigurationProperty -pspath 'MACHINE/WEBROOT/APPHOST' -filter "system.webServer/security/dynamicIpSecurity/denyByConcurrentRequests" -name "enabled" -value "True"
Set-WebConfigurationProperty -pspath 'MACHINE/WEBROOT/APPHOST' -filter "system.webServer/security/dynamicIpSecurity/denyByConcurrentRequests" -name "maxConcurrentRequests" -value < number of requests>
```

Valeur par défaut : Par défaut, les restrictions IP dynamiques ne sont pas activées.

4- Recommandations de journalisation IIS

Cette section contient des recommandations concernant la journalisation IIS qui n'ont pas été abordées dans la section Configurations de base.

Règle 1 : S'assurer que l'emplacement du journal Web IIS par défaut est déplacé

La description : IIS enregistrera des informations relativement détaillées sur chaque demande. Ces journaux sont généralement le premier élément examiné dans une réponse de sécurité et peuvent être les plus précieux. Les utilisateurs malveillants en sont conscients et essaieront souvent de

supprimer les preuves de leurs activités. Il est donc recommandé de remplacer l'emplacement par défaut des fichiers journaux IIS par un lecteur non système restreint.

Raisonnement : Déplacer la journalisation IIS vers un lecteur non système restreint contribuera à atténuer le risque que les journaux soient modifiés, supprimés ou perdus de manière malveillante en cas de panne du lecteur système.

Audit : Pour vérifier que les journaux Web sont consignés au nouvel emplacement, ouvrez l'Explorateur Windows et naviguez jusqu'au chemin qui a été défini. Selon la façon dont la journalisation a été configurée, il y aura soit :

- Un dossier contenant des fichiers .log ou
- Fichiers .log à la racine du répertoire spécifié

OU

Pour vérifier à l'aide de PowerShell, saisissez la commande suivante :

```
Get-WebConfigurationProperty -pspath 'MACHINE/WEBROOT/APPHOST'
-filter "system.applicationHost/sites/siteDefaults/logFile" -name "directory"
```

Correction : Le déplacement de l'emplacement du journal par défaut peut être facilement accompli à l'aide de la fonction de journalisation dans le

Interface utilisateur de gestion IIS, AppCmd.exe ou PowerShell.

Entrez la commande suivante dans AppCmd.exe pour configurer :

```
%systemroot%\system32\inetsrv\appcmd set config -section:sites
siteDefaults.logfile.directory:< new log location>
```

OU

Entrez la commande suivante dans PowerShell pour configurer :

```
Set-WebConfigurationProperty -pspath 'MACHINE/WEBROOT/APPHOST'
-filter
"system.applicationHost/sites/siteDefaults/logFile" -name "directory" -value
<new log location>
```

Il est préférable de déplacer les magasins de fichiers journaux vers un lecteur ou une partition non système distinct de l'endroit où les applications Web s'exécutent et/ou le contenu est servi. En outre, les autorisations NTFS au niveau des dossiers doivent être définies de la manière la plus restrictive possible ;

Les administrateurs et SYSTEM sont généralement les seuls principaux nécessitant un accès.
Bien que les journaux IIS standard puissent être déplacés et modifiés à l'aide du gestionnaire IIS, des modules complémentaires d'outils de gestion supplémentaires sont nécessaires pour gérer les journaux générés par d'autres fonctionnalités IIS, telles que le filtrage des demandes et la journalisation avancée IIS. Ces modules complémentaires peuvent être obtenus à l'aide du programme d'installation de la plate-forme Web ou sur le site de Microsoft. L'emplacement de journalisation HTTPErr peut être modifié en ajoutant une clé de registre.

Valeur par défaut : L'emplacement par défaut des journaux Web dans IIS est : %SystemDrive%\inetpub\logs\LogFiles.

Règle 2 : Assurez-vous que la journalisation IIS avancée est activée

La description : IIS Advanced Logging est un module qui offre une flexibilité dans la journalisation des demandes et des données client. Il fournit des contrôles qui permettent aux entreprises de spécifier quels champs sont importants, d'ajouter facilement des champs supplémentaires et de fournir des politiques relatives au remplacement des fichiers journaux et au filtrage des demandes. Les en-têtes de requête/réponse HTTP, les variables de serveur et les champs côté client peuvent être facilement enregistrés avec une configuration mineure dans la console de gestion IIS.

Raisonnement : De nombreux champs disponibles dans Advanced Logging peuvent fournir des données et des détails détaillés en temps réel qui ne peuvent pas être obtenus autrement. Les développeurs et les professionnels de la sécurité peuvent utiliser ces informations pour identifier et corriger les vulnérabilités des applications/modèles d'attaque.

Audit : Accédez à l'emplacement des journaux avancés et vérifiez que les fichiers .log sont en cours de génération. Notez que les journaux seront écrits sur le disque après une période de temps indéterminée. Ils peuvent être écrits dans leur répertoire spécifié immédiatement si, dans la définition de journal, les options Publier les événements en temps réel et Écrire sur le disque sont sélectionnées.

Correction : La journalisation avancée IIS peut être configurée pour les serveurs, les sites Web et les répertoires dans le gestionnaire IIS. Pour activer la journalisation avancée à l'aide de l'interface utilisateur :

- Ouvrir le gestionnaire des services d'information Internet (IIS)
- Cliquez sur le serveur dans le volet Connexions
- Double-cliquez sur l'icône Journalisation sur la page d'accueil
- Cliquez sur Sélectionner les champs

Les champs qui seront consignés doivent être configurés à l'aide du bouton Ajouter ou modifier des champs. Remarque : Il peut y avoir des problèmes de performances en fonction de l'étendue de la configuration.

Valeur par défaut : La journalisation avancée IIS est activée par défaut.

Règle 3 : Assurez-vous que la « journalisation ETW » est activée

La description : IIS introduit une nouvelle méthode de journalisation. Les administrateurs peuvent désormais envoyer des informations de journalisation à Event Tracing for Windows (ETW)

Raisonnement : IIS vide les informations de journalisation sur le disque. Par conséquent, avant IIS, les administrateurs n'ont pas accès aux informations de journalisation en temps réel. Les fichiers journaux textuels peuvent également être difficiles et longs à traiter. En activant ETW, les administrateurs ont accès aux outils de requête standard pour afficher les informations de journalisation en temps réel.

Audit : À l'aide de Message Analyzer, configurez la requête pour Microsoft-Windows-IIS-Logging. Vérifiez que vous voyez les données de journalisation en direct en accédant au site Web.

Correction : Pour configurer la journalisation ETW :

- Ouvrir le gestionnaire IIS
- Sélectionnez le serveur ou le site pour activer ETW
- Sélectionnez Journalisation.
- Assurez-vous que le format du fichier journal est W3C.
- Sélectionnez à la fois le fichier journal et l'événement ETW
- Enregistrez vos paramètres.

5- Requêtes FTP

Cette section contient un paramètre de configuration crucial pour l'exécution du protocole de transfert de fichiers (FTP).

Règle 1 : S'assurer que les requêtes FTP sont cryptées

La description : Le nouveau service de publication FTP pour IIS prend en charge l'ajout d'un certificat SSL à un site FTP. L'utilisation d'un certificat SSL avec un site FTP est également appelée FTP-S ou FTP sur Secure Socket Layers (SSL). FTP-S est une norme RFC (RFC 4217) où un certificat SSL est ajouté à un site FTP et permet ainsi d'effectuer des transferts de fichiers sécurisés.

Raisonnement : En utilisant SSL, la transmission FTP est cryptée et sécurisée de point à point et tout le trafic FTP ainsi que les informations d'identification sont ainsi protégés contre l'interception.

Audit : Pour vérifier à l'aide de PowerShell, saisissez les commandes suivantes :

```
Get-WebConfigurationProperty -pspath 'MACHINE/WEBROOT/APPHOST'
-filter
"system.applicationHost/sites/siteDefaults/ftpServer/security/ssl" -name
"controlChannelPolicy"
Get-WebConfigurationProperty -pspath 'MACHINE/WEBROOT/APPHOST'
-filter
"system.applicationHost/sites/siteDefaults/ftpServer/security/ssl" -name
"dataChannelPolicy"
```

La sortie doit être SslRequire pour les deux commandes.

Correction : Pour configurer FTP sur SSL au niveau du serveur à l'aide d'AppCmd.exe ou de PowerShell : Entrez la commande suivante dans AppCmd.exe pour configurer :

```
%systemroot%\system32\inetsrv\appcmd.exe set config section:system.
applicationHost/sites
/siteDefaults.ftpServer.security.ssl.controlChannelPolicy:"SslRequire"
/siteDefaults.ftpServer.security.ssl.dataChannelPolicy:"SslRequire" /
commit:apphost
```

OU

Entrez les commandes suivantes dans PowerShell pour configurer :

```
Set-WebConfigurationProperty -pspath 'MACHINE/WEBROOT/APPHOST'
-filter
"system.applicationHost/sites/siteDefaults/ftpServer/security/ssl" -name
"controlChannelPolicy" -value "SslRequire"
Set-WebConfigurationProperty -pspath 'MACHINE/WEBROOT/APPHOST'
-filter
"system.applicationHost/sites/siteDefaults/ftpServer/security/ssl" -name
"dataChannelPolicy" -value "SslRequire"
```

Valeur par défaut : Par défaut, les sites FTP ne sont pas compatibles SSL.

Règle 2 : Assurez-vous que les restrictions de tentative de connexion FTP sont activées

La description : IIS a introduit une fonctionnalité de sécurité réseau intégrée pour bloquer automatiquement les attaques FTP par force brute. Cela peut être utilisé pour empêcher un client malveillant de tenter une attaque par force brute sur un compte découvert, tel que le compte administrateur local.

Raisonnement : Les attaques FTP par force brute réussies peuvent permettre à un utilisateur autrement non autorisé d'apporter des modifications aux données qui ne devraient pas être faites. Cela pourrait permettre à l'utilisateur non autorisé de modifier le code du site Web en téléchargeant un logiciel malveillant ou même en modifiant la fonctionnalité d'éléments tels que les paiements en ligne.

Audit : Pour vérifier à l'aide d'AppCmd.exe, saisissez la commande suivante :

```
%systemroot%\system32\inetsrv\appcmd.exe list config -section:system.
ftpServer/security/authentication
```

La sortie doit inclure denyByFailure = true

OU

Pour vérifier à l'aide de PowerShell, saisissez la commande suivante :

```
Get-WebConfigurationProperty -pspath 'MACHINE/WEBROOT/APPHOST'
-filter "system.ftpServer/security/authentication/denyByFailure" -name
"enabled"
```

Correction :
Pour configurer les restrictions de tentative de connexion FTP au niveau du serveur à l'aide d'AppCmd.exe ou de PowerShell :
Entrez la commande suivante dans AppCmd.exe pour configurer :
%systemroot%\system32\inetsrv\appcmd.exe set config -section:system.ftpServer/security/authentication /denyByFailure.enabled:"True" /commit:apphost

OU

Entrez la commande suivante dans PowerShell pour configurer :
Set-WebConfigurationProperty -pspath 'MACHINE/WEBROOT/APPHOST' -filter "system.ftpServer/security/authentication/denyByFailure" -name "enabled" valeur "True"

Valeur par défaut : Par défaut, cette fonction n'est pas activée lorsque FTP est installé.

6- Chiffrement des transports

Cette section contient des recommandations pour la configuration des protocoles IIS et des suites de chiffrement.
Pour les protocoles de sécurité (SSL, TLS), il existe 2 chemins de registre qui contrôlent un état de protocole dans le système d'exploitation : le client TLS et le serveur TLS. Un serveur Web agit normalement en tant que serveur TLS en ce sens qu'il fournit du contenu Web aux clients. Dans certains cas, un serveur Web est configuré en tant que "client". Un exemple de serveur agissant en tant que client peut être vu lorsqu'il y a génération de contenu dynamique. Le serveur Web interroge un serveur de base de données distant pour renvoyer un contenu spécifique à la demande d'un utilisateur. Dans cette configuration, le serveur Web agit en tant que client TLS. Dans de tels cas, le protocole de serveur TLS configuré et les préférences de suite de chiffrement prévalent sur ceux du client. Ce comportement est la raison pour laquelle, pour le benchmark IIS, nous exigeons des paramètres de protocole spécifiques pour un serveur TLS et ne recommandons que des paramètres pour les clients TLS. Si les clés de registre SSLv3 ne sont pas définies, les valeurs par défaut du système d'exploitation prévalent.
Par exemple, pour désactiver le protocole SSLv3 sur le serveur TLS, vous devez

définir la clé de registre suivante sur 0 :
HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SS L 3.0\Server\Enabled
Pour empêcher un client d'émettre la commande Hello sur ce protocole hérité, le registre suivant doit être défini sur 0 :
HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SS L 3.0\Client\Enabled
Le fait que la clé soit nommée Enabled peut prêter à confusion. Le réglage de la valeur sur 0 ou 1 définit en fait l'état du protocole. 0 étant désactivé et 1 étant activé.
Voici quelques détails sur le fonctionnement des paramètres de registre "Enabled" et "DisabledByDefault". L'article suivant, Comment limiter l'utilisation de certains algorithmes cryptographiques et protocoles dans Schannel.dll , fournit des informations supplémentaires relatives au contrôle de ces protocoles et chiffrements.
L'utilisation du paramètre de registre "Enabled = 0" désactive le protocole d'une manière qui ne peut pas être remplacée par les paramètres de l'application d'e-services. C'est le seul moyen robuste d'empêcher l'utilisation du protocole et aucun paramètre supplémentaire n'est requis. Dans le même temps, l'utilisation du paramètre de registre "DisabledByDefault" empêche uniquement ce protocole d'émettre la commande Hello sur ce protocole lorsqu'une connexion SSL avec un serveur est initiée. Ce paramètre de niveau O/S peut être remplacé par une application d'e-services qui possède un codage TLS spécifique à l'application. Un exemple de cela peut être illustré en définissant le protocole dans une ligne de code dans votre application .Net 4.5 : ServicePointManager.SecurityProtocol =
SecurityProtocolType.Tls12. Cela peut remplacer le paramètre O/S si la clé DisabledByDefault est présente. "DisabledByDefault" est utile dans le cas où vous souhaitez avoir un certain contrôle sur les paramètres système, mais également autoriser une application d'e-services à spécifier explicitement les protocoles qu'elle souhaite utiliser.
Enabled ne fonctionne fortement que dans le cas négatif ("Enabled = 0"). Si "Enabled=1" ou n'est pas défini, alors "DisabledByDefault" sera prioritaire dans le cas où l'application d'e-services prend les valeurs par défaut du système. "Enabled=1" est également remplacé par les drapeaux de protocole spécifiques à l'application.

Règle 1 : Assurez-vous que l'en-tête HSTS est défini

La description : HTTP Strict Transport Security (HSTS) permet à un site d'informer l'agent utilisateur de communiquer avec le site uniquement via HTTPS. Cet en-tête prend deux paramètres : max-age, "précise le nombre de secondes, après la réception du champ d'en-tête STS, pendant lesquelles l'agent utilisateur considère l'hôte (de qui le message a été reçu) comme un hôte HSTS connu HTTPS]" ; et includeSubDomains. includeSubDomains est une directive facultative qui définit la façon dont cette stratégie est appliquée aux sous-domaines. Si includeSubDomains est inclus dans l'en-tête, il fournit la définition suivante : cette politique HSTS s'applique également à tous les hôtes dont les noms de domaine sont des sous-domaines du nom de domaine de l'hôte HSTS connu.

Raisonnement : HTTP Strict Transport Security (HSTS) est une norme simple et largement prise en charge pour protéger les visiteurs en garantissant que leurs navigateurs se connectent toujours à un site Web via HTTPS. HSTS existe pour éliminer le besoin de la pratique courante et non sécurisée consistant à rediriger les utilisateurs des URL http:// vers https://. HSTS s'appuie sur l'agent utilisateur/navigateur pour appliquer le comportement requis. Tous les principaux navigateurs le supportent. Si le navigateur ne prend pas en charge HSTS, il sera ignoré.

Lorsqu'un navigateur sait qu'un domaine a activé le HSTS, il fait deux choses :

1. Utilise toujours une connexion https://, même en cliquant sur un lien http:// ou après avoir tapé un domaine dans la barre d'adresse sans spécifier de protocole.
2. Supprime la possibilité pour les utilisateurs de cliquer sur les avertissements concernant les certificats non valides.

Un domaine indique aux navigateurs qu'il a activé HSTS en renvoyant un en-tête HTTP via une connexion HTTPS.

Audit : L'âge maximum recommandé est de 8 minutes (480 secondes) ou plus. Toute valeur supérieure à 0 est acceptable. Effectuez les opérations suivantes dans IIS Manager pour afficher les en-têtes d'hôte configurés pour le serveur :

1. Ouvrir le gestionnaire IIS
2. Dans le volet Connexions, sélectionnez votre serveur

3. Dans le volet Affichage des fonctionnalités, double-cliquez sur En-têtes de réponse HTTP
4. Vérifier qu'une entrée existe nommée Strict-Transport-Security
5. Double-cliquez sur Strict-Transport-Security et vérifiez que la case Value: contient une valeur supérieure à 0
6. Cliquez sur OK.

Effectuez les opérations suivantes dans IIS Manager pour afficher les en-têtes d'hôte configurés pour le site Web :

1. Ouvrir le gestionnaire IIS
2. Dans le volet Connexions, développez l'arborescence et sélectionnez Site Web
3. Dans le volet Affichage des fonctionnalités, double-cliquez sur En-têtes de réponse HTTP
4. Vérifier qu'une entrée existe nom Strict-Transport-Security
5. Double-cliquez sur Strict-Transport-Security et vérifiez que la case Value : contient une valeur supérieure à 0
6. Cliquez sur OK.

Correction : Toute valeur supérieure à 0 répond à cette recommandation. Les exemples ci-dessous sont spécifiques à 8 minutes mais peuvent être ajustés pour répondre à vos besoins.

Pour définir l'en-tête HTTP au niveau du serveur à l'aide d'une commande AppCmd.exe, exécutez la commande suivante à partir d'une invite de commandes avec élévation de privilèges :

```
%systemroot%\system32\inetsrv\appcmd.exe set config -
section:system.webServer/httpProtocol /+"customHeaders.
[name='StrictTransport-Security',value='max-age=480; preload']"
```

Pour définir l'en-tête HTTP et inclure des sous-domaines au niveau du serveur à l'aide d'une commande AppCmd.exe, exécutez la commande suivante à partir d'une invite de commandes avec élévation de privilèges :

```
%systemroot%\system32\inetsrv\appcmd.exe set config -
section:system.webServer/httpProtocol /+"customHeaders.[name='Strict-
Transport-Security',value='max-age=480; inclure les sous-domaines ;
preload']"
```

Pour définir l'en-tête HTTP au niveau du site Web à l'aide d'une commande

AppCmd.exe, exécutez la commande suivante à partir d'une invite de commandes avec élévation de privilèges :

```
%systemroot%\system32\inetsrv\appcmd.exe set config "<em>Website"</em> section:system.webServer/httpProtocol /+"customHeaders.[name='StrictTransport-Security',value='max-age =480 ; preload']"
```

Pour définir l'en-tête HTTP et inclure des sous-domaines au niveau du site Web à l'aide d'une commande AppCmd.exe, exécutez la commande suivante à partir d'une invite de commande élevée :

```
%systemroot%\system32\inetsrv\appcmd.exe set config "<em>Website"</em> section:system.webServer/httpProtocol /+"customHeaders.[name='Strict-Transport-Security',value='max-age=480; includeSubDomains; preload']"
```

Règle 2 : Assurez-vous que SSLv2 est désactivé

La description : Ce protocole n'est pas considéré comme cryptographiquement sécurisé.

Raisonnement : La désactivation des protocoles faibles aidera à garantir la confidentialité et l'intégrité des données en transit.

Audit : Procédez comme suit pour vérifier que SSL 2.0 est désactivé.

- Assurez-vous que la clé suivante est définie sur $_0$.

```
HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 2.0\Serveur:Enabled
HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 2.0\Client:Enabled
```

- Assurez-vous que la clé suivante est définie sur $_1$.

```
HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 2.0\Server:DisabledByDefault
HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 2.0\Client:DisabledByDefault
```

Pour vérifier à l'aide de PowerShell, saisissez la commande suivante :

```
Get-ItemProperty -path
```

'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\
Protocol s\SSL2.0\Server' -name 'Enabled'

Get-ItemProperty -path

'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\
Protocol s\SSL 2.0\Client' -name 'Enabled'

Get-ItemProperty -path

'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\
Protocol s\SSL 2.0\Server' -name 'DisabledByDefault'

Get-ItemProperty -path

'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\
Protocol s\SSL 2.0\Client' -name 'DisabledByDefault'

Correction : Effectuez les opérations suivantes pour désactiver SSL 2.0 :

- Réglez la clé suivante sur $_0$.

HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\
Protocols\SSL 2.0\Server : Enabled
HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\
Protocols\SSL 2.0\Client : Enabled

- Réglez la clé suivante sur $_1$.

HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\
Protocols\SSL 2.0\Server:DisabledByDefault
HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\
Protocols\SSL 2.0\Client :DisabledByDefault

Pour désactiver l'utilisation de PowerShell, saisissez la commande suivante :

New-Item
'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\
Protocols\ SSL 2.0\Server' -Force | Out-Null

New-Item
'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\

```
Protocols\ SSL 2.0\Client' -Force | Out-Null

New-ItemProperty -path
'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\
Protocols\SSL 2.0\Server' -name 'Enabled' -value '0' -PropertyType 'DWord'
-Force | Out-Null

New-ItemProperty -path
'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\
Protocols\SSL 2.0\Client' -name 'Enabled' -value '0' -PropertyType 'DWord'
-Force | Out-Null

New-ItemProperty -path
'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\
Protocols\SSL 2.0\Server' -name 'DisabledByDefault' -value '1' -PropertyType
'DWord' Force | Out-Null

New-ItemProperty -path
'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\
Protocols\SSL 2.0\Client' -name 'DisabledByDefault' -value '1' -PropertyType
'DWord' Force | Out-Null
```

Valeur par défaut : Enabled

Règle 3 : Assurez-vous que SSLv3 est désactivé

Ladescription: Ceprotocolen'estpasconsidérécommecryptographiquement sécurisé. Il est recommandé de le désactiver.

Raisonnement : La désactivation des protocoles faibles aidera à garantir la confidentialité et l'intégrité des données en transit.

Audit : Procédez comme suit pour vérifier que SSL 3.0 est désactivé :

- Assurez-vous que la clé suivante est définie sur $_{0}$.

```
HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\
Protocols\SSL 3.0\Serveur:Enabled
```

HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\Client:Enabled

- Assurez-vous que la clé suivante est définie sur 1.

HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\Server:DisabledByDefault

HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\Client:DisabledByDefault

Pour vérifier à l'aide de PowerShell, saisissez la commande suivante :

```
Get-ItemProperty -path
'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\Server' -name 'Enabled'

Get-ItemProperty -path
'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\Client' -name 'Enabled'

Get-ItemProperty -path
'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\Server' -name 'DisabledByDefault'

Get-ItemProperty -path 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\Client' -name 'DisabledByDefault'
```

Correction : Effectuez les actions suivantes pour désactiver SSL 3.0 :

- Réglez la clé suivante sur 0.

HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\Serveur : Enabled

HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\Client : Enabled

- Réglez la clé suivante sur 1.

HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\

Protocols\SSL 3.0\Server:DisabledByDefault

HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\Client:DisabledByDefault

Pour désactiver l'utilisation de PowerShell, saisissez la commande suivante :

New-Item

'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\ SSL 3.0\Server' -Force | Out-Null

New-Item

'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\ SSL 3.0\Client' -Force | Out-Null

New-ItemProperty -path

'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\

SSL 3.0\Server' -name 'Enabled' -value '0' -PropertyType 'DWord' -Force | Out-Null

New-ItemProperty -path

'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\ SSL 3.0\Client' -name 'Enabled' -value '0' -PropertyType 'DWord' -Force | Out-Null

New-ItemProperty -path

'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\Server' -name 'DisabledByDefault' -value '1' -PropertyType 'DWord' Force | Out-Null

New-ItemProperty -path

'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\Client' -name 'DisabledByDefault' -value '1' -PropertyType 'DWord' Force | Out-Null

Valeur par défaut : Enabled

Règle 4 : Assurez-vous que TLS 1.0 est désactivé

La description : La norme PCI Data Security Standard 3.1 recommande de désactiver "early TLS" avec SSL :
SSL et les premiers TLS ne sont pas considérés comme une cryptographie forte et ne peuvent pas être utilisés comme contrôle de sécurité après le 30 juin 2016.

Raisonnement : La désactivation des protocoles faibles aidera à garantir la confidentialité et l'intégrité des données en transit.

Audit : Procédez comme suit pour vérifier que TLS 1.0 est désactivé :

- Assurez-vous que la clé suivante est définie sur 0.

```
HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\
Protocols\TLS 1.0\Server:Enabled
```

```
HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\
Protocols\TLS 1.0\Client:Enabled
```

- Assurez-vous que la clé suivante est définie sur 1.

```
HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\
Protocols\TLS 1.0\Server:DisabledByDefault
```

```
HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\
Protocols\TLS 1.0\Client :DisabledByDefault
```

Pour vérifier à l'aide de PowerShell, saisissez la commande suivante :

```
Get-ItemProperty -path
'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\
Protocols\TLS 1.0\Server' -name 'Enabled'
```

```
Get-ItemProperty -path
'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\
Protocols\TLS 1.0\Client' -name 'Activé'
```

```
Get-ItemProperty -path
'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\
```

```
Protocols\TLS 1.0\Server' -name 'DisabledByDefault'

Get-ItemProperty -chemin
'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\
Protocols\TLS 1.0\Client' -name 'DisabledByDefault'
```

Correction : Procédez comme suit pour désactiver TLS 1.0 :

- Réglez la clé suivante sur 0.

```
HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\
Protocols\TLS 1.0\Server:Enabled

HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\
Protocols\TLS 1.0\Client:Enabled
```

- Réglez la clé suivante sur 1.

```
HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\
Protocols\TLS 1.0\Server:DisabledByDefault

HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\
Protocols\TLS 1.0\Client:DisabledByDefault
```

Pour désactiver l'utilisation de PowerShell, saisissez la commande suivante :

```
New-Item
'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\
Protocols\TLS 1.0\Server' -Force | Out-Null

New-Item
'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\
Protocols\TLS 1.0\Client' -Force | Out-Null

New-ItemProperty -path
'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\
Protocols\TLS 1.0\Server' -name 'Enabled' -value '0' -PropertyType 'DWord'
-Force | Out-Null

New-ItemProperty -path
'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\
Protocols\TLS 1.0\Client' -name 'Enabled' -value '0' -PropertyType 'DWord'
```

```
-Force | Out-Null

New-ItemProperty -path
'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\
Protocols\TLS 1.0\Server' -name 'DisabledByDefault' -value '1' -PropertyType
'DWord' -Forcer | Out-Null

New-ItemProperty -path
'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\
Protocols\TLS 1.0\Client' -name 'DisabledByDefault' -value '1' -PropertyType
'DWord' Force | Out-Null
```

Règle 5 : Assurez-vous que TLS 1.1 est désactivé

La description : TLS 1.1 est requis pour la rétrocompatibilité. Assurez-vous de tester entièrement votre application d'e-services pour vous assurer que la rétrocompatibilité n'est pas nécessaire. Si c'est le cas, créez des exceptions si nécessaire pour la compatibilité descendante.

Raisonnement : La désactivation des protocoles faibles aidera à garantir la confidentialité et l'intégrité des données en transit.

Audit : Procédez comme suit pour vérifier que TLS 1.1 est désactivé :

- Assurez-vous que la clé suivante est définie sur $_{0}$.

```
HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\
Protocols\TLS 1.1\Server:Enabled

HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\
Protocols\TLS 1.1\Client:Enabled
```

- Assurez-vous que la clé suivante est définie sur $_{1}$.

```
HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\
Protocols\TLS 1.1\Server:DisabledByDefault

HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\
Protocols\TLS 1.1\Client:DisabledByDefault
```

Pour vérifier à l'aide de PowerShell, saisissez la commande suivante :

```
Get-ItemProperty -path
'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\
Protocols\TLS 1.1\Server' -name 'Enabled'

Get-ItemProperty -path
'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\
Protocols\TLS 1.1\Client' -name 'Enabled'

Get-ItemProperty -path
'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\
Protocols\TLS 1.1\Server' -name 'DisabledByDefault'

Get-ItemProperty -path
'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\
Protocols\TLS 1.1\Client' -name 'DisabledByDefault'
```

Correction : Procédez comme suit pour désactiver TLS 1.1 :

- Réglez la clé suivante sur $_0$.

```
HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\
Protocols\TLS 1.1\Server : Enabled

HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\
Protocols\TLS 1.1\Client:Enabled
```

- Réglez la clé suivante sur $_1$.

```
HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\
Protocols\TLS 1.1\Server:DisabledByDefault

HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\
Protocols\TLS 1.1\Client:DisabledByDefault
```

Pour désactiver l'utilisation de PowerShell, saisissez la commande suivante :

```
New-Item
'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\
Protocols\TLS 1.1\Server' -Force | Out-Null
```

```
New-Item
'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\
Protocols\TLS 1.1\Client' -Force | Out-Null

New-ItemProperty -path
'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\
Protocols\TLS 1.1\Server' -name 'Enabled' -value '0' -PropertyType 'DWord'
-Force | Out-Null

New-ItemProperty -path
'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\
Protocols\
TLS 1.1\Client' -name 'Enabled' -value '0' -PropertyType 'DWord' -Force | Out-
Null

New-ItemProperty -path
'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\
Protocols\TLS 1.1\Server' -name 'DisabledByDefault' -value '1' -PropertyType
'DWord' -Forcer | Out-Null

New-ItemProperty -path
'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\
Protocols\TLS 1.1\Client' -name 'DisabledByDefault' -value '1' -PropertyType
'DWord' Force | Out-Null
```

Règle 6 : Assurez-vous que TLS 1.2 est activé

La description : TLS 1.2 est le protocole le plus récent et le plus mature pour protéger la confidentialité et l'intégrité du trafic HTTP.

Raisonnement : L'activation de ce protocole contribuera à assurer la confidentialité et l'intégrité des données en transit.

Audit : Procédez comme suit pour vérifier que TLS 1.2 est activé :

- Assurez-vous que la clé suivante est définie sur 1.

```
HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\
Protocols\TLS 1.2\Server:Enabled
```

- Assurez-vous que la clé suivante est définie sur 0.

HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Server:DisabledByDefault

Pour vérifier à l'aide de PowerShell, saisissez la commande suivante :

```
Get-ItemProperty -path 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocol s\TLS 1.2\Server' -name 'Enabled'

Get-ItemProperty -path 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocol s\TLS 1.2\Server' -name 'DisabledByDefault'
```

Correction : Procédez comme suit pour activer TLS 1.2 :

- Réglez la clé suivante sur 1.

HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Server:Enabled

- Réglez la clé suivante sur 0.

HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Server:DisabledByDefault

Pour activer l'utilisation de PowerShell, saisissez la commande suivante :

```
New-Item 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Server' -Force | Out-Null

New-ItemProperty -path 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Server' -name 'Enabled' -value '1' -PropertyType 'DWord' -Force | Out-Null

New-ItemProperty -path 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Server' -name 'DisabledByDefault' -value '0' -PropertyType 'DWord' Force | Out-Null
```

Règle 7 : Assurez-vous que les suites de chiffrement NULL sont désactivées (notées)

La description : Le chiffrement NULL n'assure pas la confidentialité ou l'intégrité des données. Il est recommandé de désactiver le chiffrement NULL.

Raisonnement : En désactivant le chiffrement NULL, il y a une meilleure chance de maintenir la confidentialité et l'intégrité des données.

Audit : Effectuez les opérations suivantes pour vérifier que le chiffrement NULL est désactivé :

- Assurez-vous que la clé suivante est définie sur 0.

```
HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\
Ciphers\NULL : Enabled
```

Pour vérifier à l'aide de PowerShell, saisissez la commande suivante :

```
Get-ItemProperty -path
'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\
Ciphers\NULL' -name 'Enabled'
```

Correction :

Effectuez les opérations suivantes pour désactiver le chiffrement NULL :

- Réglez la clé suivante sur 0.

```
HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\
Ciphers\NULL:Enabled
```

Pour désactiver l'utilisation de PowerShell, saisissez la commande suivante :

```
New-Item
'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\
Ciphers\NULL' -Force | Out-Null

New-ItemProperty -path 'HKLM:\SYSTEM\CurrentControlSet\Control\
SecurityProviders\SCHANNEL\Ciphers\NULL' -name 'Enabled' -value '0'
-PropertyType 'DWord' -Force | Out-Null
```

Règle 8 : S'assurer que les suites de chiffrement DES sont désactivées

La description : DES est un chiffrement à clé symétrique faible. Il est recommandé de le désactiver.

Raisonnement : En désactivant DES, il y a une meilleure chance de maintenir la confidentialité et l'intégrité des données.

Audit : Procédez comme suit pour vérifier que le chiffrement DES 56/56 est désactivé :

- Assurez-vous que la clé suivante est définie sur 0.

```
HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\DES 56/56:Enabled
```

Pour vérifier à l'aide de PowerShell, saisissez la commande suivante :

```
Get-ItemProperty -path 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\DES 56/56' -name 'Enabled'
```

Correction :

Procédez comme suit pour désactiver le chiffrement DES 56/56 :

- Réglez la clé suivante sur 0.

```
HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\DES 56/56:Enabled
```

Pour désactiver l'utilisation de PowerShell, saisissez la commande suivante :

```
(Get-Item 'HKLM:\').OpenSubKey('SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers', $true).CreateSubKey('DES 56/56')

New-ItemProperty -path

'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\DES 56/56' -name 'Enabled' -value '0' -PropertyType 'DWord' -Force | Out-Null
```

Règle 9 : S'assurer que les suites de chiffrement RC4 sont désactivées

La description : RC4 est un chiffrement de flux qui a connu des attaques pratiques. Il est recommandé de désactiver RC4. Le seul chiffrement RC4 activé par défaut sur Server 2012 et 2012 R2 est RC4 128/128.

Raisonnement : L'utilisation de RC4 peut augmenter la capacité d'un adversaire à lire les informations sensibles envoyées via SSL/TLS.

Audit : Procédez comme suit pour vérifier que les chiffrements RC4 40/128, RC4 56/128, RC4 64/128, RC4 128/128 ont été désactivés.

- Assurez-vous que les clés suivantes sont définies sur 0.

```
HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 40/128:Enabled
```

```
HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 56/128:Enabled
```

```
HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 64/128:Enabled
```

```
HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 128/128:Enabled
```

Pour vérifier à l'aide de PowerShell, saisissez les commandes suivantes :

```
Get-ItemProperty -path 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 40/128' -name 'Enabled'
```

```
Get-ItemProperty -path 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 56/128' -name 'Enabled'
```

```
Get-ItemProperty -path 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 64/128' -name 'Enabled'
```

```
Get-ItemProperty -path 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 128/128' -name 'Enabled'
```

Correction : Procédez comme suit pour désactiver les chiffrements RC4 40/128, RC4 56/128, RC4 64/128, RC4 128/128 :

- Réglez les touches suivantes sur 0.

```
HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 40/128:Enabled
HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 56/128:Enabled
HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 64/128:Enabled
HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 128/128:Enabled
```

Pour désactiver l'utilisation de PowerShell, saisissez les commandes suivantes :

```
(Get-Item 'HKLM:\').OpenSubKey('SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers', $true).CreateSubKey('RC4 40/128')

New-ItemProperty -path 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 40/128' -name 'Enabled' -value '0' -PropertyType 'DWord' -Force | Out-Null

(Get-Item 'HKLM:\').OpenSubKey('SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers', $true).CreateSubKey('RC4 56/128')

New-ItemProperty -path 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 56/128' -name 'Enabled' -value '0' -PropertyType 'DWord' -Force | Out-Null

(Get-Item 'HKLM:\').OpenSubKey('SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers', $true).CreateSubKey('RC4 64/128')

New-ItemProperty -path 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 64/128' -name 'Enabled' -value '0' -PropertyType 'DWord' -Force |
```

```
Out-Null
(Get-Item
'HKLM:\').OpenSubKey('SYSTEM\CurrentControlSet\Control\SecurityProviders\
SCHANNEL\Ciphers', $true).CreateSubKey('RC4 128/128')
New-ItemProperty -path
'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\
Ciphers\RC4 128/128' -name 'Enabled' -value '0' -PropertyType 'DWord' -Force
| Out-Null
```

Règle 10 : Assurez-vous que la suite de chiffrement AES 128/128 est désactivée

La description : L'activation d'AES 128/128 peut être nécessaire pour la compatibilité client. Activez ou désactivez cette suite de chiffrement en conséquence.

Raisonnement : Cet élément est noté pour les raisons suivantes et doit être désactivé :

- L'activation d'AES 256/256 est recommandée.
- Ce chiffrement ne souffre pas d'attaques pratiques connues.

Audit : Procédez comme suit pour vérifier que le chiffrement AES 128/128 est désactivé :

- Assurez-vous que la clé suivante est définie sur 0.

```
HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\
Ciphers\AES 128/128:Enabled
```

Pour vérifier à l'aide de PowerShell, saisissez la commande suivante :

```
Get-ItemProperty -path
'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\
Ciphers\AE S 128/128' -name 'Enabled'
```

Correction : Procédez comme suit pour désactiver le chiffrement AES 128/128 :

- Réglez la clé suivante sur 0.

HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\AES 128/128:Enabled

Pour désactiver l'utilisation de PowerShell, saisissez la commande suivante :

```
(Get-Item 'HKLM:\').OpenSubKey('SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers', $true).CreateSubKey('AES 128/128')

New-ItemProperty -path 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\AES 128/128' -name 'Enabled' -value '0' -PropertyType 'DWord' -Force | Out-Null
```

Règle 11 : Assurez-vous que la suite de chiffrement AES 256/256 est activée

La description : AES 256/256 est la suite de chiffrement la plus récente et la plus mature pour protéger la confidentialité et l'intégrité du trafic HTTP. L'activation d'AES 256/256 est recommandée. Ceci est activé par défaut sur Server 2012 et 2012 R2.

Raisonnement : L'activation de ce chiffrement contribuera à garantir la confidentialité et l'intégrité des données en transit.

Audit : Procédez comme suit pour vérifier que le chiffrement AES 256/256 est activé :

- Assurez-vous que la clé suivante est définie sur 1.

HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\AES 256/256:Enabled

Pour vérifier à l'aide de PowerShell, saisissez la commande suivante :

```
Get-ItemProperty -path 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\AES 256/256' -name 'Enabled'
```

Correction : Procédez comme suit pour activer le chiffrement AES 256/256 :

- Réglez la clé suivante sur 1.

HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\AES 256/256:Enabled

Pour désactiver l'utilisation de PowerShell, saisissez la commande suivante :

```
(Get-Item 'HKLM:\').OpenSubKey('SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers', $true).CreateSubKey('AES 256/256')

New-ItemProperty -path 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\AE S 256/256' -name 'Enabled' -value '1' -PropertyType 'DWord' -Force | Out-Null
```

Règle 12 : S'assurer que la commande de la suite de chiffrement TLS est configurée

La description : Les suites de chiffrement sont une combinaison nommée d'algorithmes d'authentification, de chiffrement, de code d'authentification de message et d'échange de clé utilisés pour les paramètres de sécurité d'une connexion réseau utilisant le protocole TLS. Les clients envoient une liste de chiffrements et une liste de chiffrements qu'ils prennent en charge par ordre de préférence à un serveur. Le serveur répond ensuite avec la suite de chiffrement qu'il sélectionne dans la liste des suites de chiffrement du client.

Raisonnement : Les suites de chiffrement doivent être classées du plus fort au plus faible afin de garantir que la configuration la plus sécurisée est utilisée pour le chiffrement entre le serveur et le client.

TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384

TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256

Évitez les combinaisons de chiffrement qui ne fournissent pas Perfect Forward Secrecy ou utilisent une fonction de hachage faible, utilisez-les uniquement si vous devez prendre en charge la rétrocompatibilité et en bas de la liste et vous devrez créer des exceptions pour les éléments qui font que cela devient hors de conformité :

TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (utilise SHA-1)

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (utilise SHA-1)

TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (utilise SHA-1) TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (utilise SHA-1)

TLS_RSA_WITH_AES_256_GCM_SHA384 (absence de Perfect Forward Secrecy)

TLS_RSA_WITH_AES_128_GCM_SHA256 (absence de Perfect Forward Secrecy)

TLS_RSA_WITH_AES_256_CBC_SHA256 (absence de Perfect Forward Secrecy)

TLS_RSA_WITH_AES_128_CBC_SHA256 (absence de Perfect Forward Secrecy)

TLS_RSA_WITH_AES_256_CBC_SHA (utilise SHA-1, manque de Perfect Forward Secrecy)

TLS_RSA_WITH_AES_128_CBC_SHA (utilise SHA-1, manque de Perfect Forward Secrecy)

Remarque : Compatibilité HTTP/2 : les 4 premiers chiffres (en gras) dans la liste des parties supérieures sont compatibles avec HTTP/2

Audit : Effectuez les opérations suivantes pour vérifier que l'ordre de la suite de chiffrement TLS est configuré correctement :

- ☑ Assurez-vous que la clé suivante est définie sur

TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384, TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384,TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 .

HKLM\SOFTWARE\Policies\Microsoft\Cryptography\Configuration\SSL\00010002 : Functions

Pour vérifier à l'aide de PowerShell, saisissez la commande suivante :

Get-ItemProperty -path

'HKLM:\SOFTWARE\Policies\Microsoft\Cryptography\Configuration\SSL\00010002' name 'Functions'

Correction : Effectuez les opérations suivantes pour configurer l'ordre de la suite de chiffrement TLS :

- Réglez la clé suivante sur

TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384, TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384,TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,TLS_ECDHE_RSA_WITH_AES_128_CBC6 .

HKLM\SOFTWARE\Policies\Microsoft\Cryptography\Configuration\SSL\00010002 :Functions

Pour configurer l'ordre de la suite de chiffrement TLS à l'aide de PowerShell, saisissez la commande suivante :

```
Get-Item
'HKLM:\SOFTWARE\Policies\Microsoft\Cryptography\Configuration\SSL\00010002' Forcer | Out-Null

New-ItemProperty -path
'HKLM:\SOFTWARE\Policies\Microsoft\Cryptography\Configuration\SSL\00010002' name 'Functions' -value 'TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384,TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256' -PropertyType 'MultiString' -Force | Out-Null
```

Impact : L'ordre de chiffrement est important pour s'assurer que les chiffrements les plus sûrs sont répertoriés en premier et seront appliqués sur les chiffrements les plus faibles lorsque cela est possible.

3.4.5. ANNEXE 5 GUIDE TECHNIQUE DE DURCISSEMENT D'UN SERVEUR APACHE D'UN E-SERVICE

Introduction

Ce guide pratique est conçu pour renforcer et sécuriser Apache Tomcat Server avec les meilleures pratiques. La configuration par défaut d'Apache peut exposer des informations sensibles, ce qui aide le pirate à se préparer à une attaque contre l'application

Une bonne connaissance des commandes Tomcat & UNIX est obligatoire.

Remarques

Il est nécessaire de disposer d'un outil pour examiner les en-têtes HTTP à des fins de vérification. Cela peut se faire de deux manières.

S'il s'agit de tester une application d'un e-service accessible sur Internet, il faut utiliser les outils d'en-tête HTTP suivants pour vérifier l'implémentation.

Il est recommandé de faire une sauvegarde de tout fichier qu'on est susceptible de modifier.

Nous appellerons le dossier d'installation de Tomcat comme $tomcat tout au long de ces directives.

Passons en revue les procédures de durcissement et de sécurisation.

Règle 1 : Supprimer la bannière du serveur

La suppression de la bannière du serveur de l'en-tête HTTP est l'une des premières choses à faire pour le durcissement d'Apache.Avoir une bannière expose la version utilisée et conduit à une vulnérabilité de fuite d'informations. Masquons les détails du serveur et de la version de l'en-tête du serveur.

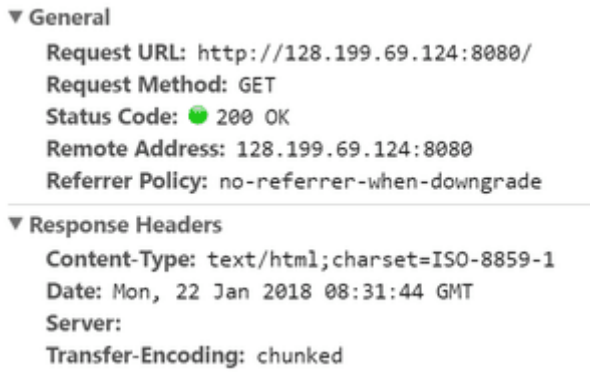
- Aller dans le dossier $tomcat/conf
- Modifier server.xml en utilisant vi
- Ajouter ce qui suit au port du connecteur

```
Server =" "
```

Ex: –

```
<Connector port="8080" protocol="HTTP/1.1"
connectionTimeout="20000"
Server =" "
redirectPort="8443" />
```

Enregistrer le fichier et redémarrez Tomcat. Maintenant, lorsque vous accédez à une application, vous devriez voir une valeur vide pour l'en-tête du serveur.



Règle 2 : Démarrage de Tomcat avec un gestionnaire de sécurité

Il est recommandé d'exécuter Tomcat avec un gestionnaire de sécurité. Le gestionnaire de sécurité permet de se protèger contre une applet non approuvée s'exécutant dans votre navigateur.
Il s'agit juste de démarrer tomcat avec l'argument -security comme suit.

```
[[email protected] bin]# ./startup.sh -security
Using CATALINA_BASE: /opt/tomcat
Using CATALINA_HOME: /opt/tomcat
Using CATALINA_TMPDIR: /opt/tomcat/temp
Using JRE_HOME: /usr
Using CLASSPATH: /opt/tomcat/bin/bootstrap.jar:/opt/tomcat/bin/tomcat-juli.jar
Using Security Manager
Tomcat started.
[[email protected] bin]#
```

Regles 3 : Activer SSL/TLS

Le traitement des requêtes Web via HTTPS est essentiel pour protéger les données entre le client et Tomcat. Afin de rendre votre application d'un e-services accessible via HTTPS, il faut implémenter un certificat SSL.
En supposant que vous ayez déjà un magasin de clés prêt avec le certificat, vous pouvez ajouter la ligne ci-dessous dans le fichier server.xml sous la section Port du connecteur.

```
SSLEnabled="true" scheme="https" keystoreFile="ssl/bloggerflare.jks" keystorePass="chandan"
clientAuth="false" sslProtocol="TLS"
```

Modifier le nom et le mot de passe du fichier Keystore avec le vôtre.
Si vous avez besoin d'aide avec le processus keystore & CSR, reportez-vous à ce guide.

Règle 4 : Appliquer HTTPS

Ceci n'est applicable que lorsque SSL est activé. Sinon, cela cassera l'application. Une fois que vous avez activé SSL, il serait bon de forcer la redirection de toutes les requêtes HTTP vers HTTPS pour une communication sécurisée entre l'utilisateur et le serveur Tomcat.

- Aller dans le dossier $tomcat/conf
- Modifier web.xml en utilisant vi
- Ajouter la syntaxe suivante avant

```
<security-constraint>
<web-resource-collection>
<web-resource-name>Protected Context</web-resource-name>
<url-pattern>/*</url-pattern>
</web-resource-collection>
<user-data-constraint>
<transport-guarantee>CONFIDENTIAL</transport-guarantee>
</user-data-constraint>
</security-constraint>
```

- Enregistrez le fichier et redémarrez le Tomcat

Règle 5 : Ajouter le drapeau Secure & HttpOnly au cookie

Il est possible de voler ou de manipuler la session des e-services et les cookies sans disposer d'un cookie sécurisé. C'est un drapeau qui est injecté dans l'en-tête de la réponse.
Cela se fait en ajoutant sous la ligne dans la section session-config du fichier web.xml

```
<cookie-config>
<http-only>true</http-only>
<secure>true</secure>
</cookie-config>
```

Ci-dessous la capture d'écran de la configuration :

```
<!-- ==================== Default Session Configuration ================= -->
<!-- You can set the default session timeout (in minutes) for all newly   -->
<!-- created sessions by modifying the value below.                       -->

  <session-config>
      <session-timeout>30</session-timeout>
      <cookie-config>
              <http-only>true</http-only>
              <secure>true</secure>
      </cookie-config>
  </session-config>
```

Enregistrez le fichier et redémarrez Tomcat pour examiner l'en-tête de réponse HTTP.

Règle 6 : Exécuter Tomcat à partir d'un compte non privilégié

Il est bon d'utiliser un utilisateur distinct non privilégié pour Tomcat. L'idée ici est de protéger les autres services en cours d'exécution au cas où l'un des comptes serait compromis.

- Créez un utilisateur UNIX, nommé tomcat

```
useradd tomcat
```

- Arrêter le Tomcat s'il est en cours d'exécution
- Changer la propriété de $tomcat en utilisateur tomcat

```
chown -R tomcat:tomcat tomcat/
```

Démarrez Tomcat et assurez-vous qu'il fonctionne avec l'utilisateur tomcat

Règle 7 : Supprimer les applications par défaut/indésirables

Par défaut, Tomcat est livré avec les applications Web suivantes, qui peuvent ou non être requises dans un environnement de production.
Elles peuvent être supprimées pour garder Tomcat sécuriser et éviter tout risque de sécurité connue avec les configurations par défaut de Tomcat.

- ROOT – Page d'accueil par défaut
- Documents – Documentation Tomcat
- Exemples – JSP et servlets pour la démonstration
- Manager, host-manager – Administration Tomcat

Ils sont disponibles dans le dossier $tomcat/webapps

```
[[email protected] webapps]# ls -lt
drwxr-xr-x 14 tomcat tomcat 4096 Sep 29 15:26 docs
drwxr-xr-x 7 tomcat tomcat 4096 Sep 29 15:26 examples
drwxr-xr-x 5 tomcat tomcat 4096 Sep 29 15:26 host-manager
drwxr-xr-x 5 tomcat tomcat 4096 Sep 29 15:26 manager
drwxr-xr-x 3 tomcat tomcat 4096 Sep 29 15:26 ROOT
[[email protected] webapps]#
```

Règle 8 : Modifier le port et la commande SHUTDOWN

Par défaut, Tomcat est configuré pour être arrêté sur le port 8005.

```
Chandans # telnet localhost 8005
Trying ::1... telnet:
connect to address ::1:
Connection refused Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
SHUTDOWN Connection closed by foreign host.
Chandans #
```

Il est recommandé de changer le port d'arrêt de tomcat et la commande par

défaut en quelque chose d'imprévisible.

- Modifiez les éléments suivants dans server.xml

```
<Server port="8005" shutdown="SHUTDOWN">
```

8005 – Changer pour un autre port inutilisé

ARRÊT – Plus compliqué

Ex-

```
<Server port="8867" shutdown="NOTGONNAGUESS">
```

Règle 9 : Remplacer les pages 404, 403, 500 par défaut

Avoir une page par défaut pour les erreurs de serveur introuvables, expose les détails de la version du serveur.
Regardons la page 404 par défaut.

HTTP Status 404 - /adf

---

type **Status report**
message **/adf**
description **The requested resource is not available.**

Apache Tomcat/ 7.0.82

Pour corriger cette faille, vous pouvez d'abord créer une page d'erreur simple et configurer web.xml pour rediriger vers une page d'erreur générale.

- Allez dans $tomcat/webapps/$application
- Créer un fichier error.jsp à l'aide de l'éditeur vi

```
<html>
<head>
<title>Error Page</title>
</head>
<body> That's an error! </body>
</html>
```

- Aller dans le dossier $tomcat/conf
- Ajouter ce qui suit dans le fichier web.xml. Assurez-vous d'ajouter avant la syntaxe

```
<error-page>
<error-code>404</error-code>
<location>/error.jsp</location>
</error-page>
<error-page>
<error-code>403</error-code>
<location>/error.jsp</location>
</error-page>
<error-page>
<error-code>500</error-code>
<location>/error.jsp</location>
</error-page>
```

- Redémarrez le serveur Tomcat pour le tester

Il est également recommandé de le faire pour java.lang.Exception. Cela aidera à ne pas exposer les informations de version de tomcat en cas d'exception java lang.

Il suffit juste d'ajouter ce qui suit dans web.xml et redémarrez le serveur Tomcat.

```
<error-page>
<exception-type>java.lang.Exception</exception-type>
<location>/error.jsp</location>
</error-page>
```

3.4.6. ANNEXE 6 GUIDE TECHNIQUE DE DURCISSEMENT D'UN SERVEUR LINUX

Introduction

Le présent document spécifie les techniques de durcissement d'un serveur linux basé sur l'état de l'art. Il définit les bonnes pratiques que l'administrateur système doit implémenter pour renforcer la sécurité matérielle et logicielle du serveur.

Les aspects traités dans ce guide sont communs à tous les systèmes GNU/LINUX indépendamment de la distribution utilisée (Debian, RedHat, etc.) et de la fonction remplie (Messagerie, Web, DNS, etc.).

Les recommandations présentées dans ce document ne sauraient donc aucunement avoir un caractère exhaustif. Il s'agit simplement d'énoncer les principaux axes de durcissement à explorer afin de protéger un serveur linux contre les activités malveillantes.

1. Sécurité relative à un système GNU/Linux

1.1. Installation

Le durcissement d'un serveur Linux commence dès la phase de l'installation du système. Généralement, Il faut éviter de procéder à une installation par défaut. Il faut tout d'abord décider quelle en sera l'utilisation (serveur Web, DNS, messagerie, etc.) avant de déterminer des règles à mettre en place pour le sécuriser. Ci-après les principaux aspects à prendre en considération lors de l'installation du système linux.

Partitionnement du disque : Le partitionnement est une étape clef de l'installation de GNU/Linux et de la prise en compte des supports de stockage de données. Il est important de bien choisir le partitionnement à adopter en vue d'obtenir un niveau de sécurité plus élevé.
La méthode de partitionnement varie en fonction de l'utilisation du serveur. Tout dépendra des services à offrir par ce serveur, de l'espace disque disponible et des applicatifs nécessaires à son fonctionnement. Généralement, il convient

de procéder au partitionnement suivant :

- Les arborescences de répertoires modifiables par un utilisateur, telles que ***/home, /tmp*** et ***/var/tmp***, doivent être sur des partitions distinctes ;
- Toute partition qui peut fluctuer, par exemple ***/var*** (surtout ***/var/log***) devrait être également sur une partition distincte ;
- Toute partition qui peut contenir des installations des logiciels ne faisantpas partie de la distribution (des applications tierces) devrait être sur une partition distincte (par exemple ***/opt***) ;
- Le répertoire ***/boot*** qui contient les fichiers indispensables au démarrage peut être mis dans une partition à part.

R 1	Implémenter un schéma de partitionnement permettant de : – Eviter la saturation ; – Simplifier la sauvegarde ; Appliquer les options de montage

En créant des partitions différentes pour les répertoires cités ci-dessus, les données peuvent être séparées et regroupées. Et dans le cas où un incident in- attendu se produit, seules les données de la partition concernée seront endommagées.

Droits lors du montage des partitions : Les partitions peuvent être montées avec certaines options (par exemple : ro, nodev, noexec, nosuid, etc.) qui limitent les droits attribués aux fichiers systèmes. Les options de montage sont définies dans le fichier '/etc/fstab'. Elles peuvent être la cible de certains comportements malveillants en cas de mauvaise configuration. Il est recommandé à cet effet d'ap- pliquer les options de montage appropriées au niveau du fichier /etc/ fstab dans les conditions suivantes :

- Les supports de stockage amovibles doivent être montés en ***nodev***, ***noexec***,***nosuid***, pour éviter à tout programme d'être exécuté à partir du périphé- rique externe.

- Les partitions de stockage temporaire comme ***/tmp***, ***/var/tmp*** et ***/dev/shm*** doivent être montés en ***nodev, noexec, nosuid ;***

- Monter le répertoire ***/home*** de préférence en nodev, noexec, nosuid ;

- Pour éviter toute modification non autorisée sur les fichiers du démarrage,la partition ***/boot*** ne doit pas être montée par défaut.

R 2	Implémenter les options de montages nécessaires et suffisantes adaptées au contexte d'emploi.

Ajout et suppression des composants logiciels : Lors de l'installation d'un serveur linux, il est conseillé d'opter pour les composants logiciels appropriés sur la base de la fonction du serveur. Les outils inutiles installés sur la machine pourraient être exploités par des personnes malveillantes pour compromettre le système.

A titre d'exemple, la présence d'outils de développement (compilateurs) ou de langages interprétés pourrait faciliter la tâche d'un attaquant dans la compilation et l'exécution de codes malveillants sur le serveur. En général, il est conseillé d'éviter l'installation par défaut des groupes de paquetage 'Software Development' ainsi que ceux relatifs au 'web server'.

De même, il est généralement conseillé d'opter pour l'utilisation de l'invite de commande au lieu des outils graphiques. En effet, en plus des failles de X Windows, l'environnement graphique est souvent lourd en termes de ressources matérielles.

R 3	Lors de l'installation et quand le système le permet, il faut décocher les paquetages associés aux applications inutiles pour le serveur : – Compilateurs ; – Logiciels de développement ; – Serveurs non nécessaires (exemple : le Serveur X) ; – Tout environnement graphique.

R 4	Supprimer les programmes inutiles pour le contexte d'utilisation du serveur notamment les services générant une grande quantité de dépendances.

Ne pas se connecter à Internet avant la fin complète de la configuration :
Certains services peuvent avoir des vulnérabilités non corrigées dans les paquets utilisés pour l'installation (exemple : utilisation d'anciennes versions de CD d'installation). Dans ce cas, si le système est connecté à internet, il sera exposé à des attaques avant même la fin de l'installation. Il est recommandé à cet effet de consulter la rubrique support de la distribution utilisée, de télécharger les derniers paquetages corrigeant les failles de sécurité et de les appliquer avant de se connecter à internet.
Dans le cas où l'installation nécessite l'accès à internet, il est recommandé de mettre en place des règles de pare-feu pour limiter l'accès au système pendant l'installation.

R 5	Protéger le serveur par un Pare-feu si l'utilisation de l'internet s'avère – nécessaire lors de l'installation du système linux.

1.2. Elimination des services inutiles

L'élimination des services inutiles en écoute sur le réseau permet de réduire la surface d'attaque et d'améliorer la sécurité globale du système. En outre cela offre plus d'espace en termes de mémoire et une optimisation des performances. Pour ce faire, il convient de lister tout d'abord les services (systèmes et réseaux) et les programmes installés :
Identifier les processus : Pour afficher tous les processus qui tournent sur la machine en temps réel, utiliser la commande :

```
#ps - aux
```

Identifier les ports réseaux utilisés : Afin d'identifier les différents ports ouverts, taper la commande :

```
#netstat -a
```

Identifier les services : Pour lister les services qui se lancent automatiquement avec le démarrage du système, utiliser la commande:

```
#chkconfig –list
```

L'équivalent de cette commande sous Debian/Ubuntu est :

```
#sysv-rc-conf –list
```

Après l'installation, il convient d'identifier les services et les programmes installés pour désactiver ceux qui sont inutiles :

Arrêter les services en exécution en utilisant la commande :

```
#service SERVICE stop
```

Arrêter le démarrage automatique des services en utilisant la commande :

```
# chkconfig –levels 2345 SERVICE off
ou
# systemctl disable SERVICE.service
```

R 6	Désactiver les services inutiles en écoute sur le réseau.

1.3. Patch et mise à niveau du système

L'application régulière des mises à jour est l'une des actions importantes pour sécuriser le système.

L'administrateur du serveur doit compléter son installation en téléchargeant au fur et à mesure les mises à jour les plus récentes de chacun des composants du système d'exploitation et de les appliquer. Un retard dans l'application d'un correctif est très souvent à l'origine de la compromission de la machine.

De même il convient de s'assurer que les applications installées sur le système sont à jour et de procéder à l'application des correctifs dans le cas échéant.

R 7	Une mise à jour régulière du système et des applications installées dessus est indispensable : – Créer, documenter et mettre en place une procédure de patch ; – Identifier régulièrement les vulnérabilités et les patches manquants ; – Installer les correctifs et les mises à jour à partir du site web officielde la distribution utilisée ; Si des correctifs ne sont pas encore disponibles, désactiver les services qui sont en relation avec la vulnérabilité si cela est possible

1.4. Configuration des paramètres réseaux

Certains paramètres de la configuration réseau IP du système doivent être modifiés de manière à renforcer sa robustesse vis-à-vis des attaques potentielles. Comme c'est souvent le cas, les paramètres par défaut permettent de prendre nativement en charge beaucoup de fonctionnalités. Pour une configuration appropriée des paramètres réseaux, il convient de procéder comme suit :

Interface réseau : Il est fortement recommandé de désactiver toute interface réseau non utilisée. Lorsque le serveur comporte plusieurs interfaces réseau, il est conseillé de spécialiser celles-ci pour dissocier les différents types de flux métiers et les flux d'administration. Il convient alors d'imposer que les services soient en écoute uniquement sur les interfaces adaptées.

IPv6 : Il est fortement recommandé de désactiver le support d'IPv6 s'il n'est pas encore utilisé. Ceci peut être fait à partir du fichier /etc/sysctl.conf en ajoutant ces lignes en fin du fichier :

```
net.ipv6.conf.all.disable_ipv6=1
net.ipv6.conf.default.disable_ipv6=1
 net.ipv6.conf.lo.disable_ipv6=1
```

Sécurisation du réseau pendant l'amorçage : Durant l'amorçage, le système lit et applique des paramètres du KERNEL trouvés dans le fichier /etc/sysctl.

conf.
Il convient de le configurer afin de sécuriser quelques options du réseau au ni- veau du noyau. Cette configuration sera appliquée sur l'ensemble des interfaces activées. Voici quelques paramètres à configurer au niveau du fichier /etc/sysctl.conf

# Ignorer les broadcasts ICMP Net.ipv4.icmp.echo_ignore_broadcasts = 1 # Ignorer les erreurs ICMP erronées
Net.ipv4.icmp_ignore_bogus_error_responses = 1
# Ne pas accepter les redirections ICMP (empêche les attaques main in the middle)
Net.ipv4.conf.all.accept_redirects = 0
# N'accepter les redirections ICMP que pour les passerelles de la liste des passerelles par
# défaut (activé par défaut)
Net.ipv4.conf.all.secure_redirects = 1
#Ne pas accepter les redirections ICMP (ce n'est pas un routeur)
Net.ipv4.conf.all.send_redirects = 0
# Ne pas faire suivre les paquets IP (ce n'est pas un routeur)
# Remarque : assurez-vousque /etc/network/options contient « ip_forward=no »
Net.ipv4.conf.all.forwarding = 0
# Activer les TCP Syn Cookies : Remarque : assurez-vous que /etc/net- work/options contient
# « syncookies=yes »
Net.ipv4.tcp_syncookies = 1
# Enregistrer les paquets usurpés Net.ipv4.conf.all.log_martians = 1
# Activer la vérification d'adresse source pour toutes les interfaces pour empêcher certaines
# attaques par usurpation
# Remarque : assurez-vous que /etc/network/options contient « spoofprotect=yes »
Net.ipv4.conf.all.rp_filter = 1
# Ne pas accepter les paquets de routage source IP (ce n'est pas un routeur)
Net.ipv4.conf.all.accept_source_route = 0
# Désactiver les touches magiques (magic-sysrq key)
Kernel.sysrq =0

```
# Diminuer la valeur de temps par défaut de « tcp_fin_timeout connection »
Net.ipv4.tcp_fin_timeout = 15
# Diminuer la valeur de temps par défaut de « tcp_keepalive_ time connection
»
Net.ipv4.tcp_keepalive_time=1880 #Désactiver tcp_windows_scaling Net.ipv4.
tcp_windows_scaling=0 #Désactiver tcp_sack Net.ipv4.tcp_sack=0
#Désactiver tcp_timestamps
Net.ipv4.tcp_timestamps=0
```

Note : il faut redémarrer le service réseau après chaque modification sur le fichier /etc/sysctl.conf

R 8	Désactiver toutes les interfaces inutiles au démarrage et n'activer que celles dont le besoin se pose.
R 9	Spécialiser les interfaces réseaux pour dissocier les flux métiers et les flux d'administration.
R 10	Désactiver le support d'IPv6 s'il n'est pas encore utilisé.
R 11	Configurer les paramètres du kernel afin de mettre en place toutes les options réseaux nécessaires.

2. Sécurité locale du système

2.1. Gestion des comptes et des utilisateurs

Linux est un système d'exploitation multi-utilisateurs, tous les utilisateurs doivent posséder un compte usager pour pouvoir y accéder. De plus ils doivent être identifiés afin d'assurer la confidentialité.

La gestion des comptes représente une partie primordiale dans la sécurité des systèmes. Avec une mauvaise gestion des utilisateurs et de leurs droits, de nombreux systèmes pourraient être corrompus. Il est donc crucial de mettre en place les techniques appropriées de gestion des comptes utilisateurs pour protéger l'accès au système.

Le super-utilisateur (root) : C'est le compte le plus important sur le système, son UID égal à 0. Ce compte dispose des droits d'accès administratifs. Il est re-

commandé de désactiver le compte root entièrement et d'ajouter des comptes d'administration nominatifs qui peuvent effectuer les tâches d'administrations en utilisant la commande sudo suivie d'une authentification.

Pour des distributions comme Ubuntu/Debian l'accès direct au compte root est désactivé par défaut, l'utilisateur devrait utiliser la commande sudo pour effectuer toute tâche administrative. En revanche, pour des distributions comme Fedora/Redhat, il est toujours possible de s'authentifier en tant que root. Il convient à cet effet de créer un autre compte et d'ajouter cet utilisateur au groupe wheel par la commande :

```
#usermod -G wheel Nom_du_compte
```

Ensuite décommenter dans le fichier /etc/sudoers la ligne qui contient :

```
%wheel ALL=(ALL) ALL
```

Finalement, il faut se connecter avec le nouveau compte et désactiver le compte root à l'aide de la commande sudo :

```
# su - Nom_du_compte
$ sudo usermode -L root
```

Les comptes systèmes : On trouve sur le système une série de comptes génériques (par exemple : bin, daemon, sync, apache, etc.). Les UIDs compris entre 1 et 499 sont généralement utilisés pour ces comptes. Il convient de bloquer l'exécution du Shell à partir de ces comptes. Pour ce faire, il faut tout d'abord lister les comptes avec leurs UIDs ainsi que leurs Shells en utilisant la commande :

```
# awk -F : 'print $1 " :" $3 " :" $7' /etc/passwd
```

Ensuite, identifier ceux possédant un UID inférieur à 500 et différent de 0 et puis désactiver leur accès au Shell :

Sous RHEL/Fedora : # usermod -s /sbin/nologin Nom_du_compte Sous Ubuntu/Debian : # usermod -s /bin/false Nom_du_compte

Les comptes ordinaires : Ce sont les comptes permettant à des utilisateurs standards de se connecter au système. L'UID de ces comptes sera un nombre supérieur ou égal à 500. Il convient de vérifier périodiquement que tous les comptes utilisateurs possèdent un mot de passe. Pour les comptes non utilisés, il convient de les désactiver à l'aide de la commande :

#usermod –L Nom_du_compte

D'une manière générale, il est fortement recommandé de :

R 12	Désactiver tous les comptes non utilisés.
R 13	S'assurer que tous les comptes possèdent un mot de passe non vide.
R 14	Supprimer tous les comptes non root avec le UID = 0, puisqu'avec un tel UID, le propriétaire du compte a les mêmes droits que le compteroot.
R 15	Désactiver l'exécution du Shell pour tous les comptes non Root et ne l'activer qu'en cas de besoin justifié.
R 16	Eviter l'utilisation des comptes ayant les droits root dans des activités autre que l'administration du système.
R 17	Mettre à la disposition des utilisateurs des comptes nominatifs et uniques et attribuer les droits d'accès selon le principe du moindre privilège.

2.2. Sécurité des mots de passe

Une bonne gestion des mots de passe permet un accès sécurisé au système. Le mot de passe ne doit pas être vide et doit systématiquement respecter une politique de complexité.

Sous Linux, le système est configuré de manière à ce que l'algorithme MD5 et les mots de passe masqués soient utilisés. Il est fortement recommandé de ne pas modifier ces paramètres. L'utilisation de l'option des mots de passe masqués permet de stocker ces derniers dans le fichier **/etc/shadow** lisible uniquement par le root, et non pas dans le fichier **/etc/passwd** accessible en lecture pour tous les utilisateurs.

Pour fixer le nombre minimum de caractères que le mot de passe doit contenir ainsi que la période de sa validité. Ajouter au fichier **/etc/login.defs :**

```
PASS_MIN_LEN 12
PASS_MAX_DAYS 90
```

Le cryptage MD5 impose des mots de passe de plus de 8 caractères, contrairement à DES (data encryption standard), ancien format de chiffrement qui limite les mots
de passe à huit caractères et donc génère des mots de passe faibles.
Utilisation de l'algorithme SHA-512 pour le hachage : Lorsque cela est possible et pour certaines distributions de linux, il convient de renforcer davantage la sécurité des mots de passe en utilisant le SHA-512 au lieu de MD5. Pour ce faire ajouter au fichier **/etc/login.defs :**

```
MD5_CRYPT_ENAB no
ENCRYPT_METHOD SHA512
```

Sécurité des mots de passe dans PAM : L'administrateur peut améliorer l'authentification des utilisateurs sur le système par la configuration de PAM (Plug- gable Authentication Modules). Le module **pam_cracklib** permet d'accepter ou de rejeter un mot de passe si celui-ci se trouve dans un dictionnaire (/usr/lib/crack- lib.pwd). Il permet aussi de vérifier que le mot de passe n'est pas réutilisé. Pour paramétrer ce module ajouter la ligne suivante dans le fichier :

- Sous RHEL/ Fedora :/etc/pam.d/system-auth
- Sous Ubuntu /Debian : /etc/pam.d/commonpassword

```
password required pam_cracklib.so retry=3 minlen=12
difok=3 lcredit=-1ucredit=-2 dcredit=-2 ocredit=-1
```

retry : Le nombre de tentative ; **minlen :** La longueur imposée ; **difok :** Le nombre de caractères existant dans l'ancien mot de passe et que l'on ne peut pas retrouver dans le nouveau ;
lcredit, ucredit, dcredit et **ocredit** correspondent respectivement au nombre de caractères minuscules, majuscules, numériques et autres. La valeur négative signifie le nombre minimum de caractère requit. La valeur positive en revanche signifie le nombre maximum de caractères. L'activation du module PAM **cracklib** oblige les utilisateurs à utiliser des mots de passe forts.

R 18	Définir les règles de choix des mots de passe. Le mot de passe doit : – Comprendre au moins 12 caractères ; – Ne pas contenir des informations personnelles (le nom d'utilisateur, la date de naissance, le nom de la société, etc.) ; – Ne pas contenir des mots du dictionnaire ; – Etre complètement différent des mots de passe précédents ; – Inclure une combinaison de lettres majuscules et minuscules, des caractères spéciaux et des chiffres ; – Doit être changé régulièrement (entre 60 et 90 jours).

R 19	Utiliser des mots de passe différents pour les comptes d'administration pour chaque hôte.

Note : En plus de l'utilisation du module PAM cracklib pour la création des mots de passe forts, il est toujours conseillé de recourir à des programmes de craquage de mot de passe pour s'assurer au maximum de son efficacité et sa résistance aux attaques contre les mots de passes.

3. Gestion des accès

1.1 Accès physique au système

La sécurité des accès physiques au système est une étape primordiale pour protéger la configuration physique d'un serveur Linux..

La sécurité des accès physiques au système repose en premier lieu sur l'emplacement et l'environnement physique où est installé le serveur. Cela permet d'empêcher l'accès non autorisé ainsi que les dommages de tout genre pouvant affecter le serveur..
Les mesures suivantes permettent de contrôler les accès au système :

BIOS : C'est le premier programme qui s'exécute au démarrage du système, il permet le contrôle des éléments matériels. Il convient de sécuriser l'accès au BIOS par un mot de passe afin d'empêcher toute modification de ses paramètres (par exemple : changer la configuration du BIOS de manière à démarrer à partir d'un CD-ROM ou une clé USB).

Note : Les méthodes utilisées pour sécuriser le Bios par mot de passe varient selon les fabricants des serveurs. Il est conseillé de consulter le manuel du serveur pour obtenir les instructions appropriées.

GRUB : Il est recommandé de protéger la configuration du chargeur de démarrage par un mot de passe pour empêcher toute tentative de connexion avec le mode single ou bien le changement des paramètres pendant le démarrage. Pour ce faire, ajouter une directive de mot de passe dans le fichier de configuration du GRUB :

Tout d'abord il faut générer un hachage MD5 du mot de passe (Les commandes doivent être adaptées à la distribution de linux et à la version du GRUB utilisées). Par exemple sous Ubuntu/Debian taper les commandes :

```
#grub
> md5crypt
```

Puis éditer le fichier de configuration du GRUB et ajouter la ligne suivante en dessous de la ligne timeout :

```
Password – md5 passwd_hashé
```

- Sous RHEL/ Fedora : /boot/grub/grub.conf.
- Sous Ubuntu /Debian : /boot/grub/menu.lst (à partir de la version 9.10 les modifications doivent être faites au niveau du fichier /etc/default/grub).

Note : Bien que GRUB accepte également les mots de passe en texte clair, il est recommandé d'utiliser un hachage md5 ou sha-512 pour une meilleure sécurité.

Authentification pour le single mode : Il est recommandé d'activer l'authentification pour le single mode, pour cela éditer le fichier ***/etc/inittab*** et ajouter la ligne suivante :

```
su :S :wait :/sbin/sulogin
```

Fermeture des sessions du Shell inactif : Il est recommandé de fermer les sessions Shell au bout d'un certain temps d'inactivité. Par exemple certains Shells Linux offrent la possibilité de définir la variable d'environnement TMOUT qui permet de déconnecter automatiquement les utilisateurs après une période d'in- activité. Afin d'éviter la modification de cette variable par les utilisateurs, il est d'usage de la définir dans le fichier **/etc/profile** et de lui appliquer la restriction **"ro"..**

```
if [ "EUID" = "0"]//["USER" = "root" ] ; then
TMOUT=900
else TMOUT=3600
fi
readonly TMOUT
export TMOUT
```

Verrouiller l'accès à la console : Vlock (Virtual console lock program) est un programme qui permet de verrouiller le terminal et de demander un mot de

passe pour être débloqué. Le paquet Vlock est présent dans les dépôts des principales distributions GNU/Linux. Pour l'installer utiliser la commande :

```
Sous RHEL/ Fedora : yum install vlock
Sous debian/ubuntu : apt-get install vlock
```

Pour verrouiller la session courante, utiliser la commande :

```
vlock -c
```

L'effet de la combinaison CTR-ALT-DEL : Dans la plupart des distributions linux l'utilisation de la combinaison ctrl-alt-del conduit au redémarrage du système. Il convient de désactiver l'effet de cette option surtout pour les serveurs de production. Pour ce faire, décommenter la ligne contenant ctrl-alt-del dans le fichier **/etc/inittab** comme suit :

```
Trap CTRL-ALT-DELETE
ca : :ctrlaltdel :/sbin/shutdown -t3 -r now
```

Pour les versions les plus récentes de linux, cette configuration doit être faite au niveau du fichier **/etc/init/control-alt-delete.conf.**

Blocage des Supports USB : Il est recommandé de désactiver le support USB au niveau du serveur sauf en cas de besoin. Pour cela, il est possible de modifier les paramètres du GRUB en ajoutant **'nousb'** dans le fichier de configuration du GRUB et en redémarrant le système par la suite :

- Sous RHEL/Fedora : ***/boot/grub/grub.conf***
- Sous ubuntu /Debian : ***/boot/grub/grub.cfg***

Pour sécuriser l'accès physique au système il convient de :

R 20	Placer le serveur dans une salle dédiée (salle serveur, salle machine, etc.
R 21	Définir un mot de passe pour le Bios.

R 22	Définir un mot de passe pour le chargeur de démarrage GRUB.
R 23	Activer l'authentification pour le single mode.
R 24	Verrouiller le Shell après un certain temps d'inactivité.
R 25	Désactiver l'effet de la combinaison CTR-ALT-DEL.
R 26	Bloquer le support du Storage USB.

1.2. Droits d'accès aux fichiers

Les droits d'accès aux fichiers constituent un élément essentiel du système linux. En effet, ils permettent de définir des droits différents (lecture, écriture, exécution) sur un même fichier selon la catégorie d'utilisateurs (propriétaire, groupe, autres). Ci-après des restrictions d'autorisation importantes qui doivent être vé rifiées régulièrement.

Les fichiers /etc/passwd, /etc/shadow, /etc/group, /etc/gshadow : Ce sont les fichiers de configuration qui contiennent les informations concernant les utilisateurs et les mots de passe. Normalement linux attribue les droits suivants par défaut pour ces fichiers :

- rw-r–r– pour /etc/passwd et /etc/group
- r——— pour /etc/shadow et /etc/gshadow

Vu l'importance de ces fichiers, il convient de faire une vérification des droits de ceux-ci. Si les paramètres par défaut sont altérés, une investigation doit être menée pour préciser la source de ce changement et rétablir les droits susmentionnés en effectuant les commandes suivantes :

```
# cd /etc
# chown root :root passwd shadow group gshadow # chmod
644 passwd group
# chmod 400 shadow gshadow
```

Le droit de **Sticky bit :** Le droit Sticky Bit (appelé aussi bit collant) est alloué à la catégorie "autres" d'un répertoire. Il permet d'interdire à tout utilisateur (sauf le root) de supprimer un fichier dont il n'est pas le propriétaire, quelque soient les droits du répertoire. Pour mettre en place cette option, il faut tout d'abord lister les répertoires ayant le droit d'écriture mais pas le Sticky bit. Ensuite, identifier les répertoires concernés et y ajouter le Sticky bit par la commande :

```
# find / -type d \( -perm -0002 -a ! -perm -1000 \) -print
# chmod +t /rep
```

Où rep représente le répertoire auquel vous désirez ajouter le Sticky bit.

Les fichiers avec droit d'écriture : Il convient de limiter les droits d'écriture sur les fichiers au stricte nécessaire. Tout d'abord il faut lister tous les fichiers ayant le droit d'écriture, puis enlever ce droit pour ceux dont le besoin n'est pas justifié :

```
# find / -type f -perm -0002 –print
# chmod o-w fichier
```

Les fichiers ayant le SUID et le GUID : Le droit SUID permet d'allouer temporairement à un utilisateur les droits du propriétaire du fichier, durant son exécution. De même, le droit GUID est similaire au droit SUID sauf qu'il donne à un utilisateur les droits du groupe auquel appartient le propriétaire du fichier et non pas les droits du propriétaire.
Il est fortement recommandé d'enlever ces droits sauf en cas de besoin majeur. Pour cela il faut identifier les fichiers ayant le SUID et le GUID, puis appliquer la commande suivante sur les fichiers trouvés :

```
# find / \( -perm -4000 -o -perm -2000 \) -type f -print
# chmod -s fichier
```

La valeur UMASK : Le masque de protection de fichier permet de définir les droits par défaut de tout fichier créé. Il convient de fixer la valeur de « UMASK » à 027. Ce qui signifie que tout fichier crée aura comme droits : ***rwxr-x—***

R 27	Vérifier les permissions sur les fichiers /etc/passwd, /etc/shadow, /etc/group et /etc/gshadow.
R 28	Limiter les droits d'écriture sur les fichiers au strict minimum.
R 29	Identifier les fichiers ayant le SUID et le GUID, enlever ces droits si le besoin n'est pas justifié.
R 30	Fixer la valeur de UMASK à 027 pour protéger les fichiers.
R 31	Trouver et supprimer les fichiers sans propriétaires.

1.3. Accès à distance

L'administration des serveurs nécessite généralement une connexion à distance. Pour sécuriser les échanges entre la machine cliente et le serveur, il est recommandé d'utiliser le protocole SSH (Secure Shell) qui permet d'établir des connexions chiffrées. Afin d'augmenter le niveau de sécurité de l'utilisation de SSH, Il convient de configurer les paramètres ci-dessous au niveau du fichier **/etc/ssh/sshd_config :**

Utiliser la version 2 du protocole SSH : Il existe deux versions différentes du protocole SSH (la version 1 et la version 2). Il est recommandé d'utiliser la version 2 du protocole puisque la 1ère version expose le serveur à une vulnérabilité qui permet à un attaquant d'insérer des données dans le flux de communication. Pour paramétrer l'utilisation de la deuxième version de SSH, ajouter au fichier :

```
Protocol 2
```

Limiter les utilisateurs qui peuvent utiliser l'accès au serveur via SSH : Pour cela, ajouter la ligne suivante :

```
AllowUsers USER1 USER2
```

Limiter l'accès par adresse IP : Il est recommandé de limiter l'accès SSH à des adresses IP spécifiques (par exemple, contrôler au niveau du Iptables) :

```
-A INPUT -p tcp -m tcp –dport 22 –source IPADDRESS -j ACCEPT
```

Désactiver l'authentification en tant que root :
Il convient de ne pas autoriser la connexion distante via SSH pour le compte root. Il est recommandé de se connecter tout d'abords par SSH en tant que simple utilisateur, puis utiliser la commande **su** pour se connecter en tant que root. Pour désactiver l'authentification en tant que root ajouter cette ligne au fichier de configuration ***/etc/ssh/sshd_config***

```
PermitRootLogin no
```

Authentification par clé RSA : Il convient aussi d'implémenter une authentification à base des clés publiques (RSA).

R 32	Utiliser une version récente de SSH pour les accès distants au serveur, afin d'assurer un échange de données sécurisé.
R 33	Paramétrer SSH pour augmenter son niveau de sécurité.
R 34	Surveiller les connexions en vérifiant régulièrement le fichier ***/var/-log/auth.log.***

Note : Il est important de redémarrer le service SSH après ces modifications.

1.1. Mise en place d'un système de filtrage : Iptables

Pour contrôler les privilèges d'accès et limiter l'utilisation des ressources du réseau, il est important de mettre en place un mécanisme de filtrage. En effet, l'utilisation des filtres permet de contrôler le trafic entrant et le trafic sortant.

Le noyau Linux offre le module Netfilter qui intercepte et manipule les paquets IP avant et après le routage. Il est possible de le configurer via la commande iptables. La première étape lors de l'utilisation d'iptables est de démarrer le service iptables par la commande :

```
service iptables start
```

Pour que iptables soit lancé par défaut dès que le système est démarré, Il faut changer le statut du niveau d'exécution sur le service à l'aide de chkconfig :

```
chkconfig –level 345 iptables on
```

Une configuration optimale du pare-feu se base généralement sur une règle de refus par défaut. En effet, il est recommandé de bloquer tous les paquets entrants et sortants sur une passerelle réseau et de n'autoriser que les paquets spécifiques selon les cas.

Pour réinitialiser la configuration de Iptables si elle existe, utiliser la commande:

```
# iptables -F
# iptables -X
```

Pour bloquer tout trafic entrant ou sortant de la machine, utiliser les commandes suivantes :

```
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP
```

Pour autoriser le trafic entrant d'une connexion déjà établie, taper la commande :

```
# iptables -A INPUT -m state –state ESTABLISHED, RELATED
-j ACCEPT
```

Pour interdire aux paquets externes d'utiliser l'adresse locale taper les commandes suivantes :

```
#iptables -A INPUT -i eth0 -s $LOOP -j DROP
#iptables -A FORWARD -i eth0 -s $LOOP -j DROP
#iptables -A INPUT -i eth0 -d $LOOP -j DROP
#iptables -A FORWARD -i eth0 -d $LOOP -j DROP
```

Exemple : pour autoriser les requêtes DNS, taper la commande :

```
#iptables -A OUTPUT -p udp -o eth0 –dport 53 –sport 1024 :65535
-j ACCEPT
```

Pour créer une chaîne pour journaliser tout le trafic rejeté :

```
# iptables -N LOGnDROP
# iptables -A LOGnDROP -j LOG –log-prefix
'DROP_LOG : '
# iptables -A LOGnDROP -j DROP
```

R 35	Appliquer une défense en profondeur en implémentant un pare-feu local : – Une configuration correcte de pare-feu se base sur une règle de refus par défaut ; – Les connexions entrantes ne doivent pas être autorisées que pour des services locaux par des machines autorisées ; – Les connexions sortantes ne doivent pas être autorisées que pour les services utilisés par le système (DNS, web, email, etc.) ; – Interdire la règle forward pour toutes les connexions (si le par feu ne protège pas d'autres systèmes) ; – Utiliser de préférence des actions telles que DROP plutôt que RE- JECT (qui envoie à l'émetteur un message indiquant que le port n'est pas ouvert) ; – Journaliser le trafic rejeté.

1.2. Contrôle des services réseaux : TCPwrapper

TCPwrapper permet de contrôler l'accès aux démons des services par hosts. Ceci est fait grâce aux deux fichiers de configuration à savoir :
/etc/hosts.deny (contient une liste des hôtes dont l'accès est interdit) ;
/etc/hosts.allow (contient une liste des hôtes dont l'accès est permit).
Le principe recommandé lors d'un filtrage et de tout rejeter et n'accepter que

ce qui est utile. Donc ajouter au fichier **/etc/hosts.deny :**

```
ALL : ALL
```

Ensuite autoriser seul le trafic utile dans le fichier **/etc/hosts.allow**
Par exemple, pour limiter le nombre d'hôtes ayant accès au service portmap puisqu'il n'est doté d'aucune forme d'authentification interne. Il faut ajouter les adresses IP des machines souhaitées dans le fichier : **/etc/hosts.allow**

```
Portmap : 10.0.0.0/255.255.255.0
```

Cette ligne indique que seul le réseau 10.0.0.0/24 est autorisé à utiliser le portmap.

TCPwrapper permet aussi d'envoyer des bannières de connexion, prévenir des attaques provenant d'hôtes particuliers et améliorer la fonctionnalité de journalisation.

R 36	Contrôler l'accès aux services réseaux par l'utilisation de TCPwrapper.

Note : Il convient d'utiliser les règles de pare-feu « Iptables » avec les « TCP-wrapper » pour créer une redondance dans les contrôles d'accès aux services.

4. Sauvegarde et restauration

Un système sécurisé doit absolument garantir un accès sûr aux données. Les différents incidents qui pourraient compromettre celles-ci ne sont pas prédictibles, et malheureusement malgré une politique très bien pensée et appliquée, ils ne peuvent pas être évités. C'est pourquoi une bonne politique de sauvegarde est nécessaire.

Les sauvegardes peuvent être simples (une simple copie, ou un archivage de base), ou évoluées (suivant un modèle client/serveur et/ou par l'utilisation d'outils de sauvegarde automatiques). Il existe différents outils de sauvegarde et le système Linux offre un ensemble de commandes. L'administrateur des systèmes peut choisir la méthode de sauvegarde la plus adaptée à son

contexte applicatif. Par exemple :

La commande **tar :** permet de sauvegarder des fichiers et des arbres d'un utilisateur ou d'une application. Pour sauvegarder une liste de répertoires dans une archive **tar** unique, il suffit de lancer la commande **tar** suivie par la commande **gzip** pour compresser :

```
tar -cvf archive-name.tar dir1 dir2 dir3....
gzip -9 archive-name.tar
```

La commande dump permet de faire des sauvegardes incrémentales des systèmes de fichiers Ext2 et Ext3. Par exemple pour sauvegarder le système de fichiers /boot, utiliser la commande :

```
dump 0zf backup.boot /boot
```

La commande dd permet de réaliser des copies physiques, elle peut parfois être utilisée pour sauvegarder des disques et des systèmes de fichiers. Cependant l'utilisation de cette commande s'avère très dangereuse, donc il est recommandé d'éviter la sauvegarde par l'utilitaire dd.

Si les sauvegardes sont faites localement (comme le montrent les exemples ci-dessus), l'accès aux fichiers de sauvegardes doit être restreint.

R 37	Effectuer une sauvegarde de bas niveau à l'installation du système, avant sa mise en production, pour pouvoir rétablir le serveur dans sonétat initial en cas de problème majeur.
R 38	Refaire cette sauvegarde à chaque fois que le système est mis à jour.
R 39	S'assurer que le logiciel de sauvegarde utilisé exige une authentification entre le client et le serveur de sauvegarde.

R 40	Chiffrer les données sauvegardées selon leurs degrés de sensibilité.
R 41	Prévoir une durée minimale entre les opérations de sauvegarde afin de revenir vers un système propre si un incident intervient.
R 42	Surveiller régulièrement le bon déroulement des sauvegardes.
R 43	Vérifier les sauvegardes en restaurant régulièrement des éléments sauvegardés pour s'assurer du bon fonctionnement du mécanisme de restauration et éviter de se retrouver avec des sauvegardes inutilisables.
R 44	Vérifier que toutes les opérations de sauvegardes sont journalisées.
R 45	Restreindre l'accès aux fichiers de sauvegarde aux seules personnes autorisées.
R 46	Placer les sauvegardes dans un lieu sûr distinct du site source.

5. Chiffrement

Toutes les données transmises sur un réseau doivent être chiffrées, Il est fortement recommandé de ne rien faire transiter en clair, de manière à ce qu'aucune communication ne soit interceptée ou altérée. Donc la mise en œuvre systématique de solutions utilisant l'authentification et le chiffrement afin de protéger les données sensibles que ce soit celles transitant sur le réseau ou celles stockées sur le disque dur est primordiale. Par exemple il convient d'utiliser :

- SSH au lieu de TELNET, FTP, RSH ;
- IMAPS au lieu d'IMAP ;
- HTTPS au lieu de HTTP ;
- etc.

De même, il convient d'utiliser **GNU Privacy Guard (GPG ou GnuPG)** ou équivalent pour transmettre des messages signés et chiffrés afin de garantir l'authenticité et la confidentialité des données transmises.

R 47	Utiliser un moyen de chiffrement approprié pour sécuriser les données sensibles transférées via le réseau (données d'authentification, emails, pièces jointes, documents sensibles, etc.).

6. Supervision et audit

1.1. Journalisation

Lorsque le système Linux démarre, fonctionne et effectue tout type d'action, ses actions et celles de la plupart de ses services sont tracées dans des fichiers di- vers. Deux démons sont spécialisés dans la réception des messages à écrire dans ces fichiers :

- ***klogd*** : kernel log daemon, chargé de la gestion des informations émises par le noyau.
- ***syslogd*** : system log daemon, chargé de la gestion des informations émisespar tous types de services et éventuellement le noyau.

Il est recommandé de configurer **syslogd** afin de journaliser toutes les activités du système. En effet il faut définir les services, les niveaux et les destinations au niveau du fichier **/etc/syslogd.conf.** Par exemple pour envoyer tous les événements système à un serveur de logs il faut ajouter la ligne suivante :

```
*.* @adresse_IP_serveur_log
```

Les logs systèmes sont situés dans le fichier /var/log. il est recommandé à l'administrateur de consulter ce qui suit :

- **/var/log/messages** : Ce fichier regroupe les messages des différents démons et services du système ;
- **/var/log/secure** : Ce fichier garde des traces sur les connexions

de façon dé- taillées (adresse IP, service, port . . .). C'est également ici que le démon sshd stocke les tentatives de connexion ;

– **/var/log/auth.log** : Ce fichier enregistre tous les logins qui se connectent au système, ainsi que le mécanisme de connexion utilisé.

Il convient par la suite de mettre en place des outils d'analyse de journaux d'évènements, tels que :

- LogWatch ;
- Swatch, outil d'analyse des logs en Perl ;
- LogCheck, outil d'analyse basé sur le système Cron.
- Etc.

R 48	Définir et mettre en place une politique de journalisation d'événements.
R 49	Activer la journalisation du système et des services.
R 50	Rediriger les logs vers un serveur de logs dédié.
R 51	Centraliser les logs.
R 52	Archiver les logs.
R 53	Analyser les logs.
R 54	Restreindre l'accès aux fichiers de logs aux seules personnes autorisées.
R 55	Définir des rôles précis au niveau de l'outil de consultation des logs.
R 56	Afin de pouvoir confronter les journaux de plusieurs systèmes, il est nécessaire que leurs horloges soient synchronisées (NTP).

1.2. Vérification de l'intégrité du système

La vérification de l'intégrité du système linux permet de s'assurer de l'intégrité des répertoires et des fichiers importants du système en identifiant tous changements apportés à ces derniers. En effet, en cas de compromission, certains fichiers sont modifiés par l'attaquant pour masquer sa présence et installer une ou plusieurs portes dérobées (backdoors) sur le système.

Le principe de la vérification de l'intégrité du système consiste à prendre l'empreinte des fichiers pour créer une base de données de référence avec la signature de chacun des fichiers à surveiller. Cette signature est constituée de nombreux indicateurs garantissant l'unicité du fichier auquel elle se rapporte (propriétaire, date de création, date de dernière modification, taille, calcul d'empreinte, etc.). Cette empreinte sera ensuite régulièrement comparée à l'empreinte courante et l'administrateur sera avisé, en général par un courrier électronique, en cas de modification de l'intégrité d'un fichier.

De nombreux outils permettant la vérification de l'intégrité des fichiers peuvent être utilisés, notamment : Open source Tripwire, Advanced Intrusion Detection Environment (AIDE) et Another File Integrity Checker (AFICK), etc.

R 57	Utiliser des outils appropriés pour s'assurer de l'intégrité des fichiers du système.

Il est recommandé de protéger la base de données des empreintes par mot de passe pour éviter qu'un attaquant compromettant la machine puisse aussi compromettre trivialement la base.

1.3. Audit

L'audit périodique de la sécurité de l'OS est un moyen essentiel pour identifier les vulnérabilités et veiller à ce que les mesures de sécurité existantes soient efficaces. Il existe différents outils commerciaux et open source que l'administrateur peut utiliser afin d'évaluer le niveau de sécurité de son système.

Lynis par exemple est un outil open source qui permet de réaliser un audit simple d'un serveur linux, en effet, il génère un rapport de sécurité récapitulatif

et synthétique de l'état du serveur et ce, en analysant l'ensemble du système : le chargeur de démarrage (bootloader), les services, le kernel, la mémoire, les processus, les utilisateurs, les groupes et l'authentification, les shells, le système de fichiers, le stockage, la configuration réseau, etc.

L'administrateur pourra consulter le rapport complet, qui se trouve dans : ***/var/log/lynis.log***.

R 58	Effectuer régulièrement des audits du système afin d'analyser : – La configuration du serveur ; – Les performances du serveur ; – L'évolution du matériel ; – L'évolution des logiciels ; – Les mises à jour.

ASIN
AGENCE DES SYSTÈMES D'INFORMATION ET DU NUMÉRIQUE
RÉPUBLIQUE DU BÉNIN

Rejoignez nous sur nos différents cannaux !

@asinbenin