Cliquez ici pour entrer du texte.

Tests d'intrusion -

Création :	xx/yy/2019
Référence :	X1904-00542
Classification :	C3 - Confidentiel Client
Version :	1.0
Liste destinataires	
Auteurs :	
Responsable du document :	
Destinataire :	

1 Propriétés du document

1.1 Intervenants

Auditeur(s)	
Auditeur1	Consultant sécurité Mail : Tel : Mob :
Auditeur 2	Consultant sécurité Mail : Tel : Mob :

Responsable d’audit	
RESP_NAME	Responsable d'audit Tel : Mob :

1.2 Gestion des changements de version

Version	Nom	Commentaires
0.1		Création et rédaction
1.0		Relecture et validation

Ce tableau gère les modifications apportées au document au-delà de sa version initiale.

2 Table des matières

3 Introduction

3.1 Objectifs de la mission

L'audit de sécurité effectué au profit de Society avait pour objectif d'identifier et de mettre en évidence les vulnérabilités présentes sur le périmètre cible suivant :

Environnement	Nome	Role	Comptes
ENV Principale	Serveur1	Console Principal	user003 user004 user005 user006
	Serveur 2	Domaine Manager	
	Serveur3	Server Base de données	
	Serveur 4	Scalabity servers 4	
	Serveur 5	Scalabity servers 5	

Il s'agissait :

- De tester la résistance de l'ensemble des éléments exposés sur Internet dans le cadre de tentatives d'intrusion maitrisées et sans impacts sur les systèmes ciblés ;
- De simuler les possibilités de malveillance par un utilisateur malintentionné ;
- D'identifier les scénarios d'attaque depuis l'extérieur et leurs impacts sur le SI (Système d'Information) de la société ;
- De proposer un plan de remédiation des risques principaux permettant d'améliorer le niveau de sécurité global du SI.

3.2 Interlocuteurs principaux

Pour Society :

- TRUC Monsieur — Chef de projet

Pour Prestataire securite :

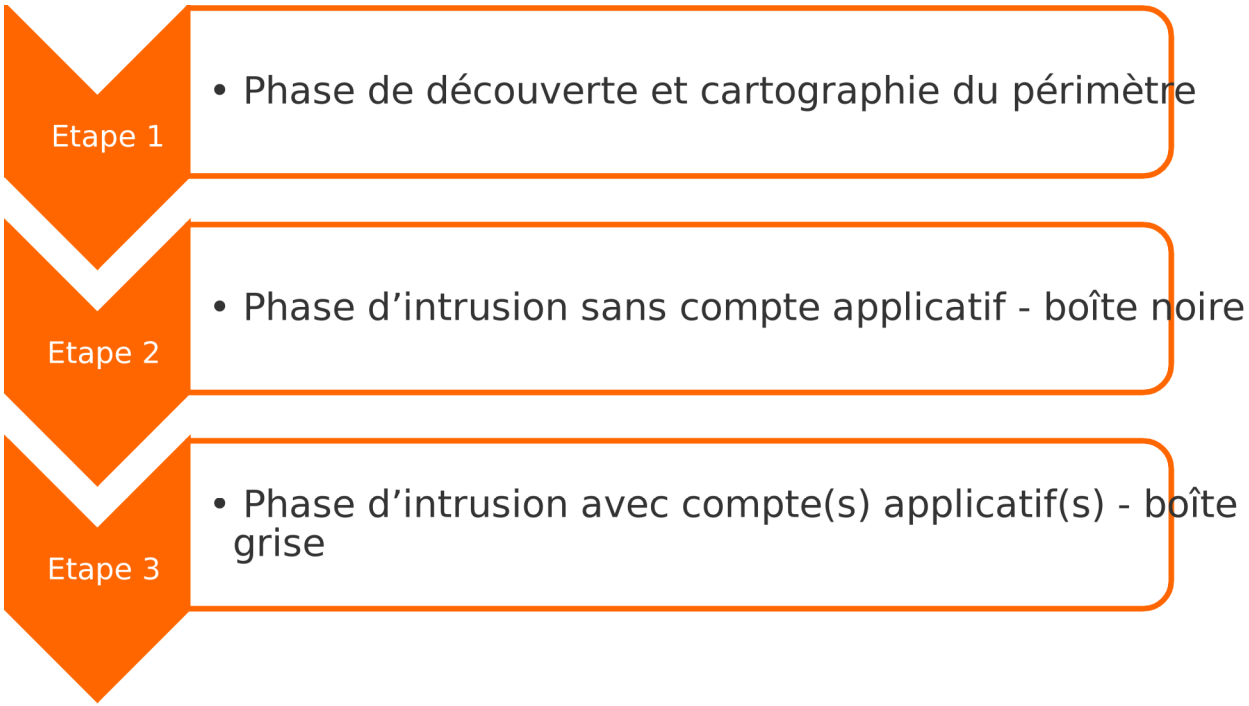
- *Auditeur 1* — *Responsable d'audit et Consultant sécurité*
- Auditeur2 — *Consultant sécurité*

3.3 Organisation de la mission

Les tests externes se sont déroulés du xxxxx au xxxxx 2019, depuis les locaux de Society.
La phase de rédaction s'est déroulée le xx mois 2019. Une autorisation d'audit écrite nous a été remise par M. Resp de la Society.

Méthodologie TIE

La démarche des tests d'intrusion externes s'articule autour de 3 étapes :



- Phase de découverte : Menée sans connaissance préalable du Système d'Information, elle a pour objectif d'obtenir un maximum d'informations sensibles sur les services accessibles et les équipements d'infrastructure associés, en cartographiant la plate-forme grâce à différentes techniques. Durant cette phase, des recherches sont menées sur les forums ou autres sites spécialisés afin de récupérer des informations techniques ou des traces de compromission en rapport avec le périmètre audité ;
- **Phase d'intrusion boite noire** : Cette partie permet d'identifier les vulnérabilités existantes et de mesurer les risques potentiels de prise de contrôle ou de récupération d'informations sensibles (données clients, données bancaires…) sans être authentifié sur l'application ;
- **Phase d'intrusion boite grise** : Le test d'intrusion est approfondi en testant les fonctionnalités réservées aux utilisateurs authentifiés ainsi que l'étanchéité entre les différents utilisateurs.

3.4 Limites de **l'audit**

Durant notre audit, aucun xxx n'était réellement connecté à notre environnement :

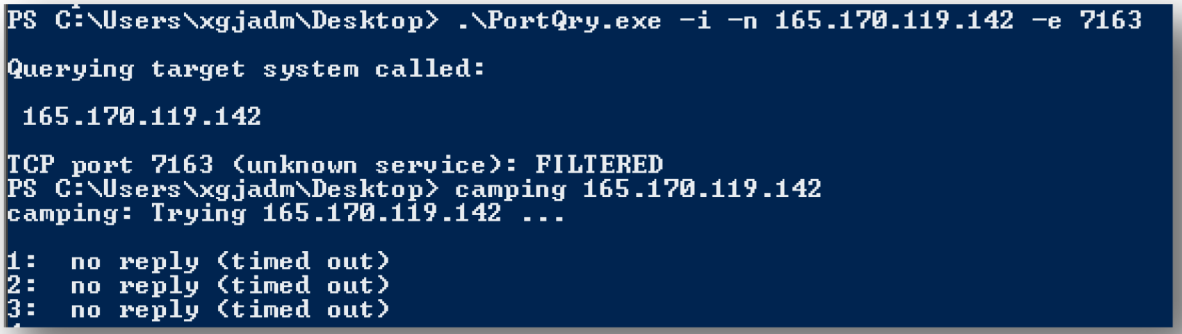
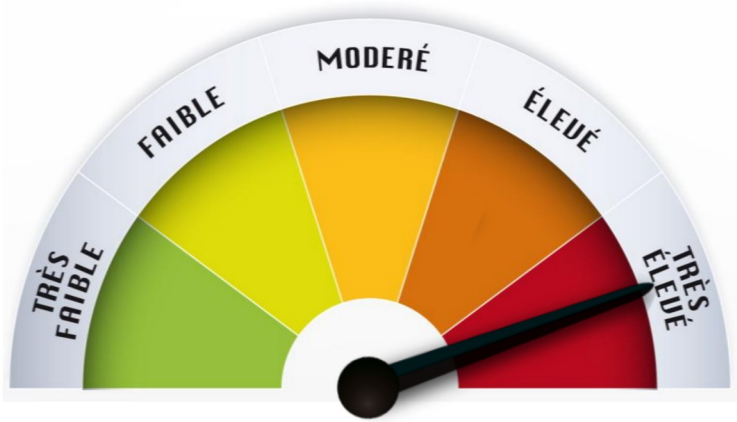


Figure 1 - xxx ne pouvant être joint

Ainsi, il n'a pas été possible de connaitre l'exposition réseau du SI_vuln depuis l'interne.

4 Tableau de bord

Risque



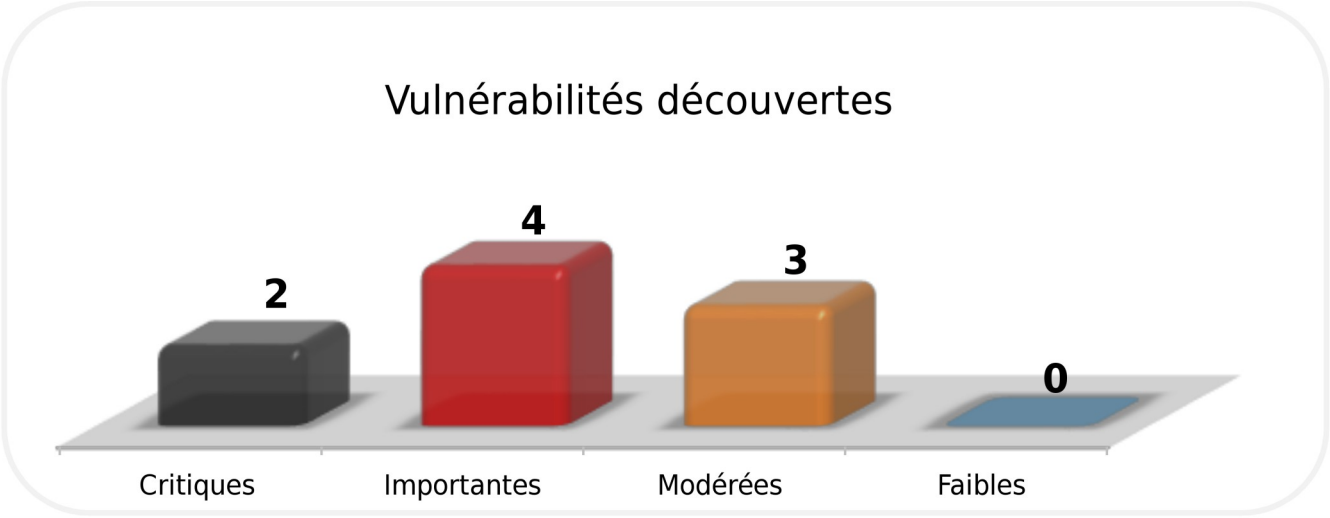
Impacts

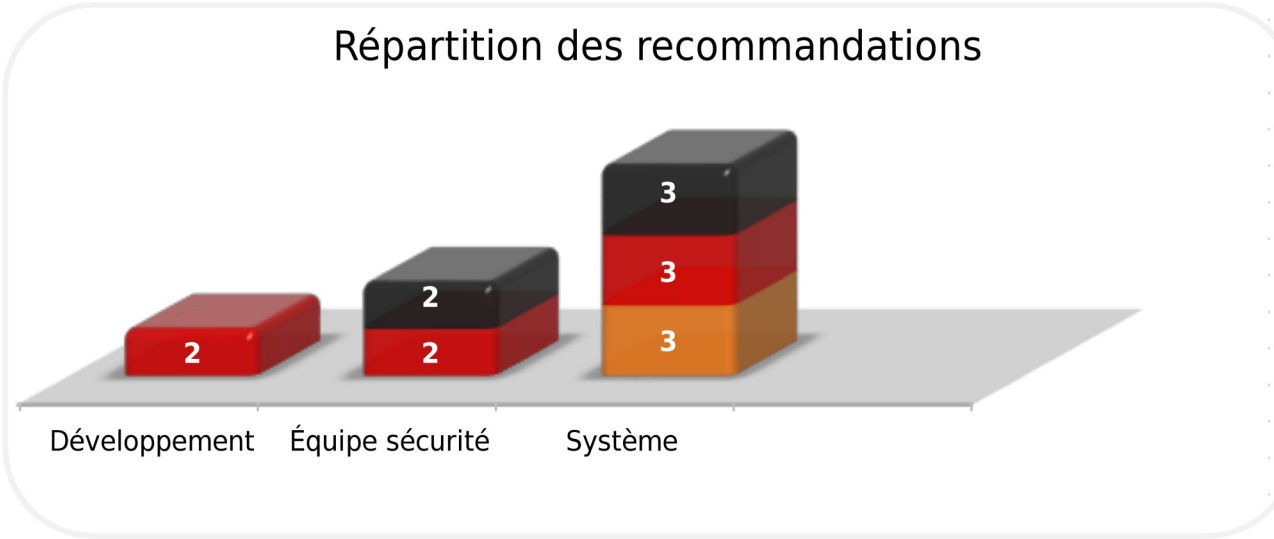
Impacts techniques

Disponibilité	3
Intégrité	4
Confidentialité	4
Preuve	3

Impacts métiers

Image de marque	3
Financier	2
Violation de la vie privée	2
Non-conformité	2


Vulnérabilités découvertes
2
4
3
0
Critiques
Importantes
Modérées
Faibles


Répartition des recommandations
2
2
2
3
3
3
Développement
Équipe sécurité
Système

5 Synthèse

5.1 Conclusion

Le **test d'intrusion depuis l'in**terne mené sur l'APPLI a révélé un niveau de risque global très élevé[4].

Durant l'audit, xxxxx a mis en avant 9 vulnérabilités. Parmi celles-ci, 2 présentent un risque critique, 4 présentent un risque majeur, et 3 des risques plus faibles.

L'audit mené sur la plateforme APPLI, permettant la télédistribution de logiciels sur les géré par Society a permis de remonter quelques points positifs.

Tout d'abord, une authentification forte par jeton matériel RSA est configurée pour plusieurs utilisateurs lorsqu'ils souhaitent se connecter aux serveurs frontaux, sur lesquels est installé le

De plus, des restrictions logicielles ont été mises en place sur ce même serveur afin qu'un utilisateur ne puisse pas exécuter les quelques programmes non autorisés.

Par ailleurs, les flux réseaux sont chiffrés lors des communications entre les serveurs, empêchant ainsi la transmission de données sensibles en clair sur le réseau ou la possibilité d'écouter voire modifier le trafic légitime.

Cependant, certaines vulnérabilités représentent un risque pour l'infrastructure hébergeant ces applications. Bien que cela soit du ressort du contrôle d'accès propre à chaque ,
une possibilité de compromission totale du domaine a pu être menée, mettant à genou toutes les mesures de sécurité mises en place sur APPLI1.

Cela a pu aboutir grâce à la possibilité d'élever les privilèges de l'utilisateur sur le serveur frontal en utilisant des permissions trop laxistes sur certains dossiers de l'application ou un problème de configuration de l'intégration de l'application sur le système d'exploitation.

Il est également important de stipuler que l'authentification forte par jeton matériel RSA n'est pas applicable pour tous les comptes du domaine. Ainsi, l'usurpation d'identité de plusieurs comptes du domaine ou même d'un compte Windows local permet de contourner
cette mesure de sécurité.

---

[1] ***Échelle :*** *Très faible, faible, modéré, élevé, très élevé*

Les différentes vulnérabilités détaillées tout au long du rapport sont récapitulées et priorisées au sein d'un **plan d'action** disponible à la fin de cette section de synthèse. Nous vous recommandons de le suivre au plus vite pour parfaire le niveau de sécurité.

5.2 Points positifs

Points positifs	Commentaires
Authentification forte	Un token hardware RSA est en place lors de la connexion à la console
Chiffrement des communications	La communication entre le client et le serveur est chiffrée. Le protocole de chiffrement utilisé est robuste et il assure un bon niveau de sécurité.
Antivirus	Un antivirus récent et à jour est installé sur les systèmes du périmètre. Ceci est une bonne mesure de sécurité.
Restriction réseau	Tous les utilisateurs du domaine ne peuvent se connecter au serveur via le protocole RDP

5.3 Points à améliorer

Points à améliorer	Commentaires
Mots de passe faible	Des mots de passe faibles ont été relevés. Ces mots de passe sont aisément devinables par un attaquant, lui octroyant ainsi un accès authentifié aux systèmes.
Droits sur les dossiers de l'application	Certains dossiers disposent de permissions trop laxistes
Restrictions logicielles	Il est possible de rebondir sur le serveur Windows hébergeant l'application faute à des restrictions logicielles trop laxistes

5.4 Tableaux de synthèse

5.4.1 Vulnérabilités identifiées

Voici la synthèse des vulnérabilités découvertes durant l'audit :

Réf.	Risque	Libellé	Résumé de la vulnérabilité	Périmètre concerné	Impacts	Exploitation
TI-1	Critique	Mots de passe faibles ou par défaut	Des mots de passe faibles ou par défaut été identifiés. Ils permettent la compromission de comptes fortemen privilégiés et ainsi la compromissiond l'environnement APPLI1	Domaine Windows	Critique	Quasi certaine
TI-2	Critique	Réutilisation de mots de passe locaux	Le mot de passe de l'administrateur lo Windows est réutilisé entre plusieurs systèmes de l'environnement.	Ensemble des serveurs de l'environnement APPLI1	Critique	Probable
TI-3	Critique	Restrictions logicielles insuffisantes	Il est possible de s'échapper de la pris mise en place par l'environnement e d'exécuter des commandes directement le serveur.	SERVEUR3	Critique	Probable
TI-4	Majeur	Permissions des dossiers de l'application	Les permissions relatives à certains dos de l'application ne sont pas assez restrictives.	Application truc	Critique	Possible

TI-5	Majeur	Injection de code arbitrai via DLL	Les services de l'application DSM charg certaines bibliothèques partagées de manière non sécurisée, permettant à utilisateur malveillant de faire exécuter propre code en créant sa bibliothèqu partagées.	Application 2	Critique	Possible
TI-6	Majeur	Contournement de l'authentification forte pa token RSA	L'authentification forte par token RSA p être contournée.	Environnement APPLI1	Majeur	Probable
TI-7	Majeur	Comptes utilisés pour exécuter des services Windows	Des comptes administrateurs sont utili pour exécuter des services Windows n nécessitant pas ce type de privilèges.	Machin Explorer	Majeur	Probable
TI-8	Modéré	Variable d'environnemer PATH non sécurisée	La variable d'environnement PATH cont un dossier qui est inscriptible par un utilisateur avec des privilèges faibles.	Machines utilisant l solution de x	Majeur	Possible
TI-9	Modéré	Présence de mots de pass en cache	Les serveurs Windows stockent les empreintes des mots de passe des 1(derniers utilisateurs AD connectés.	Machin Explorer	Majeur	Possible

5.4.2 **Plan d’action**

Voici le plan d’action priorisé permettant d’augmenter rapidement le niveau de sécurité :

Réf.	Libellé	Recommandation	Périmètre concerné	Responsable	Priorité	Difficulté correction
TI-1	Mots de passe faibles ou par défaut	Modifier les mots de passe des compte indiqués ci-après.	Domaine Windows	Système	Court terme	Triviale
TI-2	Réutilisation de mots de passe locaux	Ne jamais utiliser le même mot de pas plusieurs fois, surtout pour des compt critiques.	Ensemble des serveurs de l’environnement APPLI1	Système	Court terme	Moyenne
TI-4	Permissions des dossiers de l’application	Corriger les permissions des dossiers identifiés lors de l'audit.	Application Dxx	Système	Court terme	Moyenne
TI-5	Injection de code arbitrai via DLL	Les développements doivent être revu pour s'assurer que les DLL soient charg de manière sécurisées.	Application Dxx	Développement	Court terme	Moyenne
TI-6	Contournement de l’authentification forte pa token RSA	Tous les comptes doivent être configur pour utiliser le token RSA.	Environnement APPLI1	Équipe sécurité	Court terme	Moyenne
TI-7	Comptes utilisés pour exécuter des services Windows	Les privilèges du compte de service doi être réduits.	Dxx	Système	Court terme	Moyenne

TI-7	Comptes utilisés pour exécuter des services Windows	Vérifier s'il est possible d'utiliser un cor Windows local pour exécuter les service	DSM	Système	Court terme	Moyenne
TI-6	Contournement de l'authentification forte pa token RSA	Revoir le processus d'authentification s l'application Dxx pour forcer l'utilisateur du token RSA lors de la connexion	Environnement	Développement	Court terme	Complexe
TI-8	Variable d'environnemer PATH non sécurisée	Il convient de ne pas insérer de valeurs cette variable avant l'entrée C:\Windows\System32, mais plutôt à la de la valeur originale.	Machines utilisant la solution de	Système	Court terme	Triviale
TI-3	Restrictions logicielles insuffisantes	Empêcher l'utilisation de Powershell a profils 'Viewer'	SERVEUR3	Système	Moyen terme	Moyenne
TI-1	Mots de passe faibles ou par défaut	Une politique de complexité des mots passe doit être mise en place	Domaine Windows	Équipe sécurité	Moyen terme	Complexe
TI-4	Permissions des dossiers de l'application	Mise en place d'une procédure de revue de suivi des permissions.	Application Dxx	Équipe sécurité	Moyen terme	Très complexe
TI-9	Présence de mots de pass en cache	Désactiver le cache Windows sur les serveurs	Dxx	Système	Moyen terme	Triviale

TI-2	Réutilisation de mots de passe locaux	Mise en place d'une solution de généra aléatoire des mots de passe d'administration, par exemple via la sol LAPS de Microsoft.	Ensemble des serveurs de l'environnement APPLI1	Système	Long terme	Complexe
TI-1	Mots de passe faibles ou par défaut	Des audits de mots de passe doivent ê réalisés régulièrement sur les systèm sensibles et les utilisateurs devraient é sensibilisés	Domaine Windows	Équipe sécurité	Long terme	Très complexe

5.4.3 Constat du contre audit

Réf.	Libellé	Risque Initial	Risque actuel	Etat
SYS-1	Manque de mises à jour	Critique	Insignifiant	Corrigé
SEC-1	Comptes et mots de passe faibles	Critique	Critique	Non corrigé
SYS-2	Restrictions logicielles insuffisantes	Critique	Critique	Non corrigé
SEC-2	Réutilisation de mots de passe entre environnements	Critique		Non testé
SYS-3	Réutilisation de mots de passe locaux	Critique	Critique	Non corrigé
SYS-4	Exploitation de l'architecture	Critique		Non testé
SEC-3	Contournement de l’authentification fort token RSA	Majeur	Majeur	Non corrigé
SYS-5	Comptes utilisés pour exécuter des serv Windows	Majeur	Majeur	Non corrigé
SYS-6	Mots de passe en clair dans les fichiers mots de passe par défaut	Majeur	Insignifiant	Corrigé
DEV-1	Présence de mots de passe en cache	Modéré	Modéré	Non corrigé
DEV-2	DLL Hijacking	Modéré	Modéré	Non corrigé

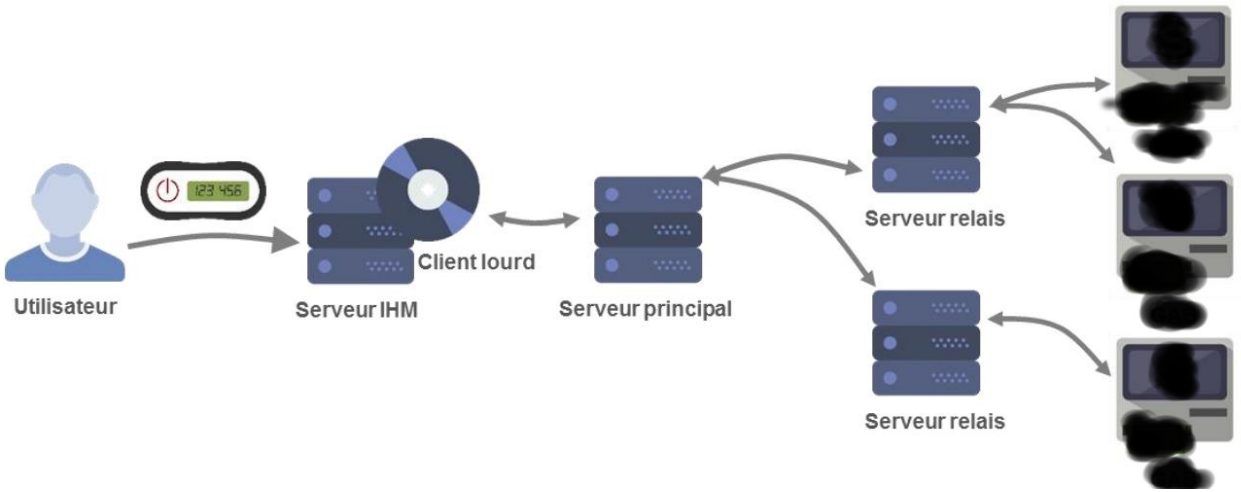
6 Description Technique

6.1 Présentation simplifiée de la plateforme APPLI1

APPLIXest une plateforme permettant de télédistribuer des packages sur les machines ainsi que de présenter un inventaire des logiciels présents sur les machins. Cette plateforme permet également de réaliser de la télécollecte de traces.

APPLIX est un progiciel (produit Y de Computer Associates - CA).

Le schéma ci-dessous présente un schéma simplifié de la plate-forme :



La plateforme est ainsi composée d'un serveur IHM, de 3 serveurs principaux et de 5 serveurs relais.

Ces serveurs sont intégrés au domaine Windows .

L'authentification sur le serveur IHM est réalisée par une authentification Windows (compte Active Directory) ainsi qu'avec un token RSA afin d'assurer une authentification forte.

Les communications sont réalisées au travers du protocole propriétaire : CSAMPmux.exe sur le port 7163.

Au total, sur le SI il y a 6 plateformes distinctes. Il y en a une pour chaque filiales (xxx /YYY / ZZZ) qui elle-même disposent de chacune de deux domaines HXXX et HYYY.

Phase de découverte

La phase de découverte a pour objectif d'obtenir un maximum d'informations sur les réseaux et les machines ciblées, tout d'abord à partir des informationspubliques disponibles, puis en cartographiant le réseau grâce à différentes techniques, telles que la détection des services actifs, les commandes de type « traceroute » et l'utilisation de champs spécifiques (Timestamp, IPID, Sequence Number), renvoyés par les systèmes distants.

La cartographie est une étape importante d'une attaque. Elle apporte la connaissance du réseau attaqué. Un réseau qui fournit de nombreuses informations sur sa constitution facilite la tâche du pirate. L'objectif final de cette phase est d'obtenir une typologie estimée du réseau cible décrivant les

équipements réseau, les machines utilisées, les types de systèmes d'exploitation, leurs adresses IP, les services disponibles depuis Internet (applications et versions).

Pour cela, nous nous basons sur diverses sources publiques telles que :

- Les bases Whois pour obtenir des informations sur les adresses IP ;
- Les forums et les sites de partage
- Les moteurs de recherche
- Les métadonnées au sein des documents

Les outils utilisés dans cette phase sont :

- Scanners de ports ;
- Outils de détection de système d'exploitation ;
- Outils analysant les métadonnées au sein des documents ;
- Outils effectuant des recherches avancées sur les moteurs de recherche.

Plusieurs actions sont possibles pour effectuer une cartographie :

- L'interrogation des DNS (serveurs de noms de domaines) ;
- Les requêtes ICMP (Ping et Traceroute) ;
- La détection des services actifs ;
- Les requêtes TCP et UDP à variation de TTL sur les ports non filtrés ;
- La détection des versions de système d'exploitation ;
- Identification des applicatifs (recherche de bannières, identification par signatures) ;

6.1.1 Non-conformités

La réalisation des étapes décrites précédemment n'a pas permis de mettre en avant d'élément non conforme avec l'état de l'art.

6.1.2 Services actifs

Les services suivants ont été détectés :

Hôte	Protocole	Port	Service	Bannière
250.200.200.200	tcp	53	domain	
	tcp	443	https	
	tcp	1720	h323q931	
	tcp	3389	rdp	

6.2 Présentation des vulnérabilités

À partir des informations recueillies à l’étape précédente, nous pouvons tester les vulnérabilités des différents services accessibles au niveau réseau, système d’exploitation et application. Pour chacune des vulnérabilités découvertes, nous décrirons son fonctionnement, ses conséquences et les moyens de s’en protéger. Ce chapitre décrit les tests effectués sur le périmètre de la mission.

6.2.1 Mots de passe faibles ou par défaut

Critique				
Titre	Mots de passe faibles ou par défaut			TI- 1
Périmètre	Domaine Windows xxx, yyy Explorer			
Description	Des mots de passe faibles ou par défaut ont été identifiés. Ils permettent la compromission de comptes fortement privilégiés et ainsi la compromission de l'environnement APPLIX.			
Probabilité	Menace		Vulnérabilité	Probabilité d'exploitation
	Condition	Utilisateur anonyme	Catégorie OWASP (web)	A2 - Violation de Gestion d'authentification et de Session	Quasi certaine
	Facilité technique d'exploitation		Facilité de découverte	
Impact	Impact technique		Impact métier	Impact global
	Disponibilité		Image de marque	Critique
	Intégrité		Financier	
	Confidentialité		Violation de vie privée	
	Preuve		Non-conformité	

Long terme	Responsable	Difficulté
Des audits de mots de passe doivent être réalisés régulièr sur les systèmes sensibles et les utilisateurs devraient être sensibilisés	Équipe sécurité	●●●●

[C3 - Confidentiel Client]

Description

L'utilisation de mots de passe forts est l'une des briques de base dans la sécurisation d'un système d'information. Cependant cette étape est souvent oubliée, ainsi il est fréquent de trouver des comptes avec des mots de passe triviaux, sans mot de passe ou avec des mots de passe par défaut.

Un mot de passe fort est un mot de passe qui est difficile à retrouver, même à l'aide d'outils automatisés.

La force d'un mot de passe dépend de sa longueur et du nombre de possibilités existantes pour chaque caractère le composant. En effet, un mot de passe constitué de minuscules, de majuscules, de caractères spéciaux et de chiffres est techniquement plus difficile à découvrir qu'un mot de passe constitué uniquement de minuscules.

État constaté

Plusieurs mots de passe faibles ont été identifiés sur des comptes fortement privilégiés de la plate-forme.

Nom de compte	Robustesse du mot de passe	Impact
Dom_user	Mot de passe trivial	Administrateur sur les serveurs de la plate-forme APPLI1 (et sur de nombreux autres serveurs) Ne nécessite pas de token RSA.
Dom\adm_user	Mot de passe trivial	Administrateur sur les serveurs de la plate-forme APPLI1 (et sur

de l'ensemble de l'infrastructure de APPLI1 (ainsi qu'à d'autres plateformes qui n'étaient pas dans notre périmètre).

La capture ci-dessous illustre la connexion sur un des serveurs de la plate-forme APPLI1 avec le compte « _user » qui dispose des droits d'administration :

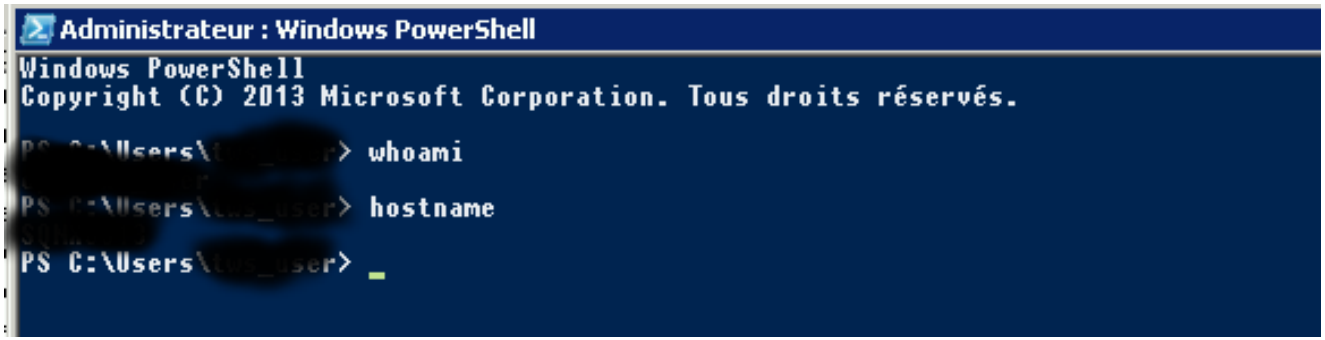


Figure 2 Accès à un compte à forts privilèges, protégé par un mot de passe faible

Recommandations

Les actions suivantes sont recommandées :

- À court terme, le mot de passe des comptes identifiés lors de l'audit doivent être modifiés. Un mot de passe robuste doit être mis en place. De plus, nous vous conseillons de durcir les mots de passe utilisés pour protéger les clés privées ;
- À plus moyen terme, et si ce n'est pas déjà le cas, une politique de complexité des mots de passe doit être mise en place, tant sur le plan technique qu'organisationnel ;
- Enfin, à plus long terme, nous vous recommandons de sensibiliser les utilisateurs et d'effectuer des audits de mots de passe sur les comptes AD afin d'avertir les potentiels utilisateurs possédant un mot de passe trop simple.

Reference (s)

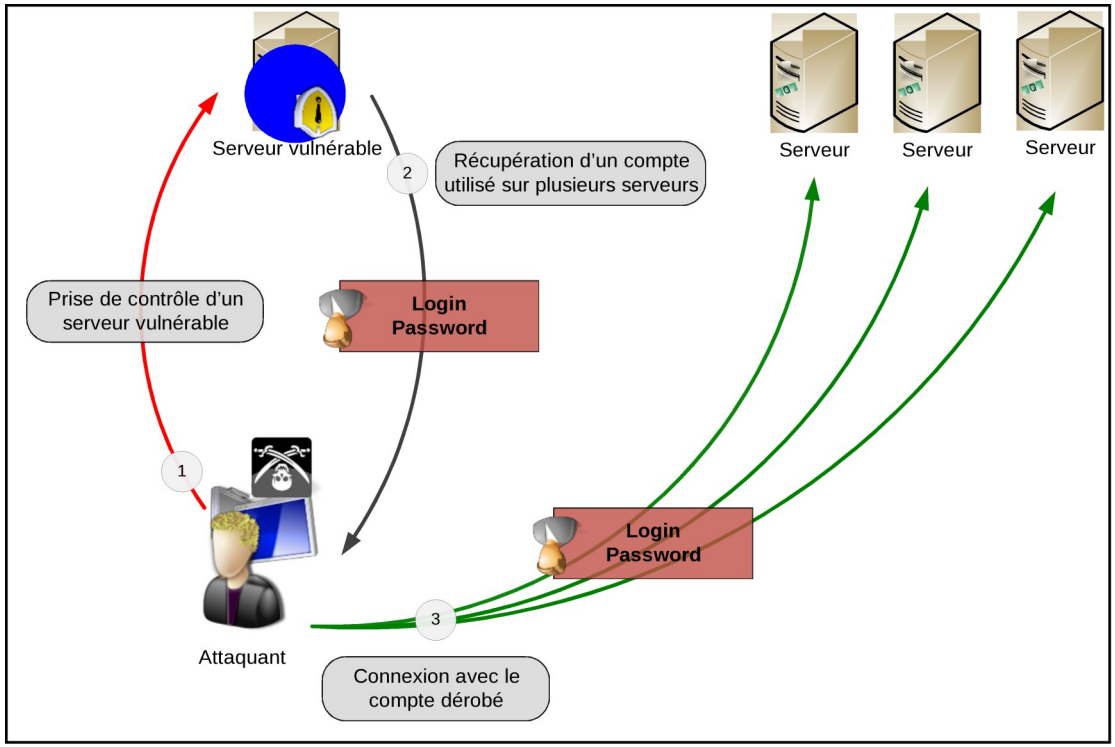
https://www.owasp.org/index.php/Testing_for_Weak_password_policy_(OTG-AUTHN-007)

6.2.2 Réutilisation de mots de passe locaux

Critique				
Titre	Réutilisation de mots de passe locaux			TI- 2
Périmètre	Ensemble des serveurs de l'environnement APPLI1			
Description	Le mot de passe de l'administrateur local Windows est réutilisé entre plusieurs systèmes de l'environnement.			
Probabilité	Menace		Vulnérabilité	Probabilité d'exploitation
	Condition	Utilisateur authentifié		Probable
	Facilité technique d'exploitation		Facilité de découverte	
Impact	Impact technique		Impact métier	Impact global
	Disponibilité		Image de marque	Critique
	Intégrité		Financier	
	Confidentialité		Violation de vie privée	
	Preuve		Non-conformité	
Recommandations				

DESCRIPTION

Un compte disposant des privilèges administrateur local détient tous les droits sur le système d'exploitation. Ce dernier peut accéder à des fonctionnalités sensibles du système d'exploitation dans le but de lire et modifier des informations critiques sur ce dernier. La réutilisation de mots de passe est un réel danger lors de la compromission d'une machine.



Attaque par réutilisation de mots de passe

En effet, si plusieurs machines utilisent des comptes partageant le même mot de passe, il est alors facile pour un attaquant de compromettre l'ensemble de ces machines.

De plus, l'attaquant n'a pas besoin de casser le condensat et de découvrir le mot de passe en clair, la simple utilisation du condensat à la place du mot de passe permet de rebondir sur d'autres machines :il s'agit de la fonctionnalité« Pass-The-Hash »inhérenteaux systèmes Microsoft Windows.

Risques

Un attaquant ayant réussi à récupérer le condensat de l'administrateur local pourra se connecter avec les plus hauts privilèges sur toutes les machines utilisant le même mot de passe et ainsi :

- Accéder à l'ensemble des données stockées sur la machine distante ;
- Exécuter des commandes ;
- Installer des backdoors ou chevaux de Troie ;
- Etc.

L'attaquant n'a pas besoin de disposer du mot de passe en clair. L'accès à la base des comptes (via les droits Administrateur) suffisent à obtenir les empreintes des mots de passe, pouvant ensuite être réutilisés pour s'authentifier sur d'autres systèmes quel que soit la complexité du mot de passe utilisé.

Recommandations

Modifier les mots de passes locaux de sorte à ce qu'ils soient uniques sur chaque poste/serveur du périmètre, dans le but de se protéger du risque de rebond sur l'ensemble des postes/serveurs à partir de la compromission d'une seule machine.

Un outil tel que LAPS (Local Administrator Password Solution - https://support.microsoft.com/fr-fr/kb/3062591) peut être utilisé pour la gestion des comptes d'administration locale.

En 2015, Microsoft a publié l'outil LAPS (Local Administrator Password Solution). Cet outil gratuit permet à une entreprise de définir automatiquement des mots de passe de compte administrateur locaux aléatoires et spécifiques sur des postes de travail et des serveurs membres d'un domaine.
Ces mots de passe sont stockés dans un attribut confidentiel sur le compte machine du domaine et peuvent être récupérés par les administrateurs système si besoin.

7 Annexe

7.1 Qualification d'une vulnérabilité

Chaque vulnérabilité identifiée est qualifiée par nos équipes. La qualification est enrichie de plusieurs critères. Nous vous indiquons ici la correspondance de chacun de ces critères.

NOTE DEDIEE AUX TESTS D'INTRUSION APPLICATIFS

Les métriques présentées reprennent les principes fondateurs de la méthodologie OWASP pour la pondération des risques. Pour plus d'informations, il est possible de se référer à cette adresse : https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology.

7.1.1 Niveau de risque général

Le niveau de risque est calculé en fonction de la probabilité et de l'impact.

En fonction du niveau de risque calculé, cinq catégories sont définies par criticité croissante :

Indicateur	Niveau de risque
	Risque insignifiant. Information indiquée car contraire à l'état de l'art
	Risque mineur
	Risque modéré
	Risque majeur
	Risque critique

7.1.2 Périmètre

Le périmètre définit la zone d'exploitabilité de la vulnérabilité remontée. Il peut correspondre à une instance précise du périmètre de l'audit (ex. : une URL, une adresse IP), ou à un ensemble de composants (ex. : Serveurs Windows, Front Office…

7.1.4 Probabilité – Menace

Champ		Détails
Condition	Utilisateur anonyme	L’exploitation est possible sans nécessiter de compte utilisateur
	Utilisateur authentifié	L’exploitation nécessite un compte utilisateur
	Utilisateur interne	L’exploitation nécessite un accès interne au SI et potentiellement un compte utilisateur.
	Compte de service	L’exploitation nécessite un compte de service
	Développeur	L’exploitation nécessite des connaissances liées au projet (typiquement un développeur ayant participé au projet ou ayant accès au code source).
	Administrateur	L’exploitation nécessite un compte d’administration (technique ou fonctionnelle).
Facilité technique d’exploitation		Vulnérabilité théorique, non exploitable en l’état au moment de l’audit
		Compétences techniques avancées requises pour l’exploitation (création de code d’exploitation) ou nécessitant un investissement important (serveurs de calcul par exemple)
		Compétences techniques avancées requises pour l’exploitation (maîtrise des principaux outils et des techniques d’attaques).
		Compétences réseaux, systèmes, ou de développement requises pour l’exploitation.

7.1.5 Probabilité – Vulnérabilité

Champ	Détails	
Catégorie OWASP	Correspond à la principale catégorie définie dans le Top Ten de l'OWASP à laquelle est rattachée la vulnérabilité. Note : Les vulnérabilités ne sont pas toutes corrélables avec les éléments de ce référentiel (ex. : faille logique).	
Facilité de découverte		Impossible ou pratiquement impossible
		Difficile
		Modérée
		Facile
		Outils automatiques disponibles permettant de découvrir la vulnérabilité

7.1.6 Probabilité – **Probabilité d'exploitation**

La probabilité d'exploitation est une pondération assignée par l'auditeur et est fonction de la vulnérabilité, sa facilité d'exploitation, sa prévalence, et son accessibilité sur le périmètre audité.

Pondération	Description
Invraisemblable	Probabilité d'exploitation quasi nulle
Improbable	Probabilité d'exploitation improbable
Possible	Probabilité d'exploitation possible
Probable	Probabilité d'exploitation probable

7.1.7 Impact – Impact technique

Les impacts techniques sont divisés en 4 catégories :

- La Disponibilité désigne l'atteinte au niveau de service de l'application
- L'Intégrité concerne la modification des données manipulées par l'application
- La Confidentialité entre en jeu lorsque des informations techniques et ou sensibles sont divulguées
- La Preuve (ou Traçabilité) est la capacité à assurer un suivi de l'attaquant, et notamment la capacité à l'identifier précisément

Champ		Détails
Disponibilité		Aucune atteinte
		Faible perturbation (ex. : léger ralentissement)
		Perturbation modérée
		Perturbation importante
		Indisponibilité totale (ex. : arrêt du serveur)
Intégrité		Aucune atteinte aux données manipulées par l'application
		Données non importantes ou relatives à un utilisateur altérables
		Part modérée de données modifiables, ou nombre limité d'utilisateurs affectés par les modifications
		Une partie importante des données peut être altérée par l'exploitation
		Toutes les données peuvent être altérées de manière

		Toutes les données peuvent être récupérées
Preuve / Traçabilité		Non impacté
		Attaquant potentiellement traçable
		Attaquant partiellement traçable
		Perte importante de suivi de l'attaquant
		Perte complète de suivi de l'attaquant

7.1.8 Impact – Impact métier

Les impacts métiers sont divisés en 4 catégories :

- L'image de marque correspond à l'atteinte à la réputation de l'entreprise
- L'impact financier estime le préjudice pécuniaire subi
- La violation de la vie privée est faite lorsque des données personnelles des utilisateurs sont rendues à des personnes non autorisées
- La mise en non-conformité est la mise en défaut de l'entreprise suite à une vulnérabilité liée par rapport à :
  - Un standard (PCI-DSS ou RGSv2 par exemple)
  - Une politique de sécurité interne (PSSI par exemple)
  - Une obligation légale (CNIL / RGPD par exemple)
  - (ex. : données personnelles divulguées alors qu'un contrat oblige l'entreprise à les protéger)

Champ	Détails
	Aucun impact

	💲 💲 💲 💲	Inférieur au coût de correction de la vulnérabilité
	💲 💲 💲 💲	Impact mineur sur les profits annuels
	💲 💲 💲 💲	Impact majeur sur les profits annuels
	💲 💲 💲 💲	Faillite
Violation de la vie privée	🪪 🪪 🪪 🪪	Aucun impact
	🪪 🪪 🪪 🪪	Un individu impacté
	🪪 🪪 🪪 🪪	Des dizaines ou centaines d’individus impactés
	🪪 🪪 🪪 🪪	Des milliers d’individus sont impactés
	🪪 🪪 🪪 🪪	Les individus impactés se comptent par millions
Mise en non-conformité	📋 📋 📋 📋	Aucun impact
	📋 📋 📋 📋	Violation mineure
	📋 📋 📋 📋	Violation modérée
	📋 📋 📋 📋	Violation importante
	📋 📋 📋 📋	Violation très importante

7.1.9 Impact – Impact global

L'impact global fait la synthèse des différentes métriques d'impact utilisées, et de l'expérience de l'auditeur et notamment de sa compréhension du métier et du rôle fonctionnel du périmètre audité.

Pondération	Description
Négligeable	Impact global nul ou négligeable
Mineur	Impact global faible
Modéré	Impact global modéré
Majeur	Impact global important
Critique	Impact global extrêmement important

7.1.10 Recommandations

La difficulté de correction identifie la complexité de mise en place d'une parade. La correction de la vulnérabilité nécessite :

Pondération	Détails
●○○○	Peu de compétences,de moyens et de temps requis (changement d'un paramètre de configuration, changement de mot de passe, etc.).
●●○○	Des compétences et des moyens raisonnables ou un peu de temps (application d'un correctif, modification de la configuration, etc.).
●●●○	Beaucoup de compétences, de moyens ou de temps (développement, correction de l'architecture, réorganisation des procédures, etc.).
●●●●	Énormément de compétences, de moyens et de temps (refonte de l'architecture, ré-implémentation complète, demande d'un correctif à l'éditeur etc.).

NOTE

Plusieurs corrections peuvent être proposées, et ce, avec une priorité variable. L'intérêt est ici de permettre un meilleur lissage de la correction dans le temps. Par exemple, si une vulnérabilité Cross Site Scripting (XSS) est identifiée sur une application web équipée d'un pare-feu applicatif (WAF), la recommandation pourra s'axer autours des points suivants :

- Moyen terme : Nettoyer les entrées utilisateur destinées à l'affichage
- Court terme : Ajouter une règle de blocage de la charge malveillante dans le pare-feu applicatif (WAF)

7.2 Champs du tableau de vulnérabilités

Ce tableau recense les différentes vulnérabilités trouvées pendant l'audit

Réf.	Risque	Libellé	Résumé de la vulnérabilité	Périmètre concerné	Impacts	Exploitati
TIE4	Majeur	Cross-Site Scripting (XSS)	Les entrées utilisateurs pe des caractères HTML/Jav dangereux rendant possib de code côté client.	www.application.com	Majeur	Complexe

Voici la signification exacte de chaque colonne :

Libellé	Signification
Réf.	Référence de la vulnérabilité utilisée dans le rapport
Risque	Risque global associé à la vulnérabilité
Libellé	Intitulé de la vulnérabilité
Résumé de la vulnérabilité	Présentation succincte de la vulnérabilité
Périmètre concerné	Liste des serveurs / applications concernés par la vulnérabilité
Impacts	Conséquences techniques et métier en cas de non-correction
Exploitation	Facilité de découverte de la vulnérabilité et niveau d'expertise Nécessaire à son exploitation

7.3 Champs du plan d’actions

Le plan d’action recense les différentes recommandations évoquées précédemment afin de corriger les vulnérabilités identifiées.

Réf.	Libellé	Recommandation	Périmètre concerné	Responsable	Priorité	Difficulté correction
TIE4	Cross Site Scripting (XSS)	Effectuer une vérification des entré et sorties utilisateurs	www.application.com	Développement	Haute	Complexe

Voici la signification exacte de chaque colonne :

Libellé	Signification
Réf.	Référence de la vulnérabilité
Libellé	Intitulé de la vulnérabilité
Recommandation	Synthèse de la recommandation
Périmètre concerné	Liste des serveurs ou applications concernés par la recommandation
Priorité	Urgence de correction de la vulnérabilité (critère détaillé plus haut)
Difficulté de correction	Difficulté de correction (critère détaillé plus haut)