JEDHA DEMODAY

EVIL CORP

Christian Xiang

Sommaire

Date début pentest : 30/01/2023

Date fin pentest : 02/02/2023

Introduction

Dans cette présentation, je vais vous présenter 3 vulnérabilités courantes qui peuvent compromettre la sécurité d'un système informatique.

L'adresse IP est le 172.31.35.242 .

La première vulnérabilité concerne l'injection de commande bash dans un site web.

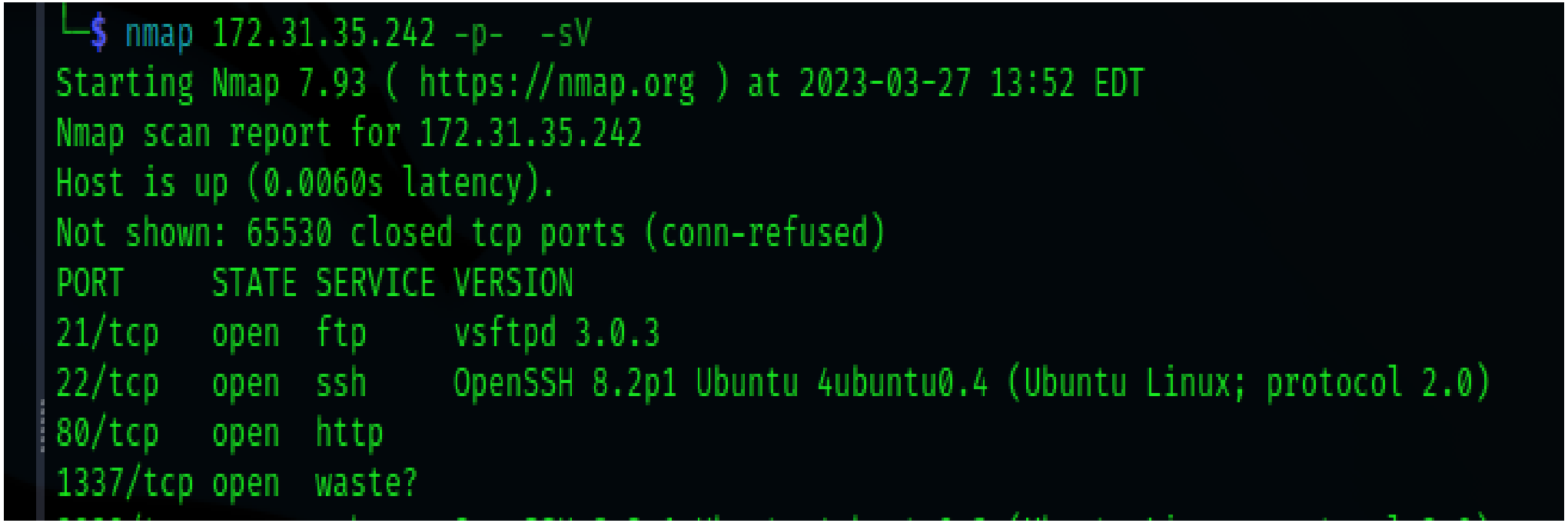
La deuxième concerne une attaque par force brute sur un utilisateur SSH.

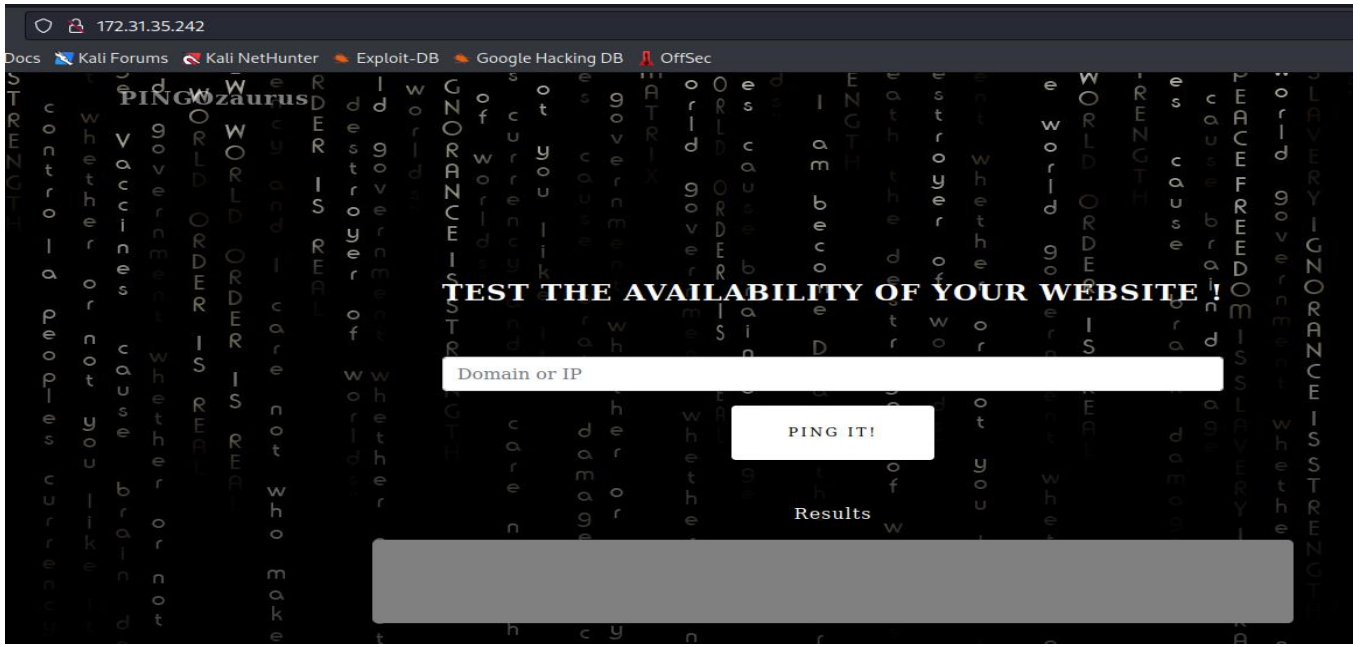
La troisième concerne l'injection SQL sur un site web

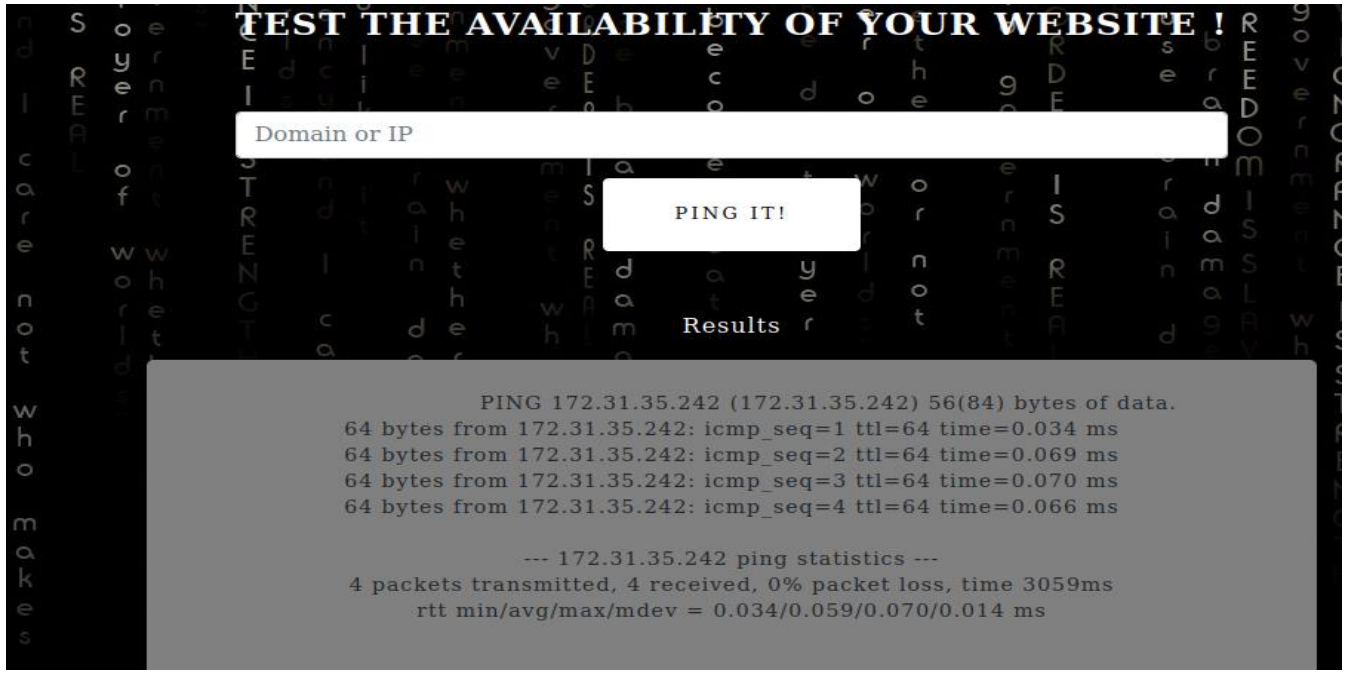
Nous allons examiner les méthodes pour détecter et corriger ces vulnérabilités.

Vulnérabilité 1

Avant de commencer , nous allons effectuer un scan Nmap sur l'adresse IP 172.31.35.242.

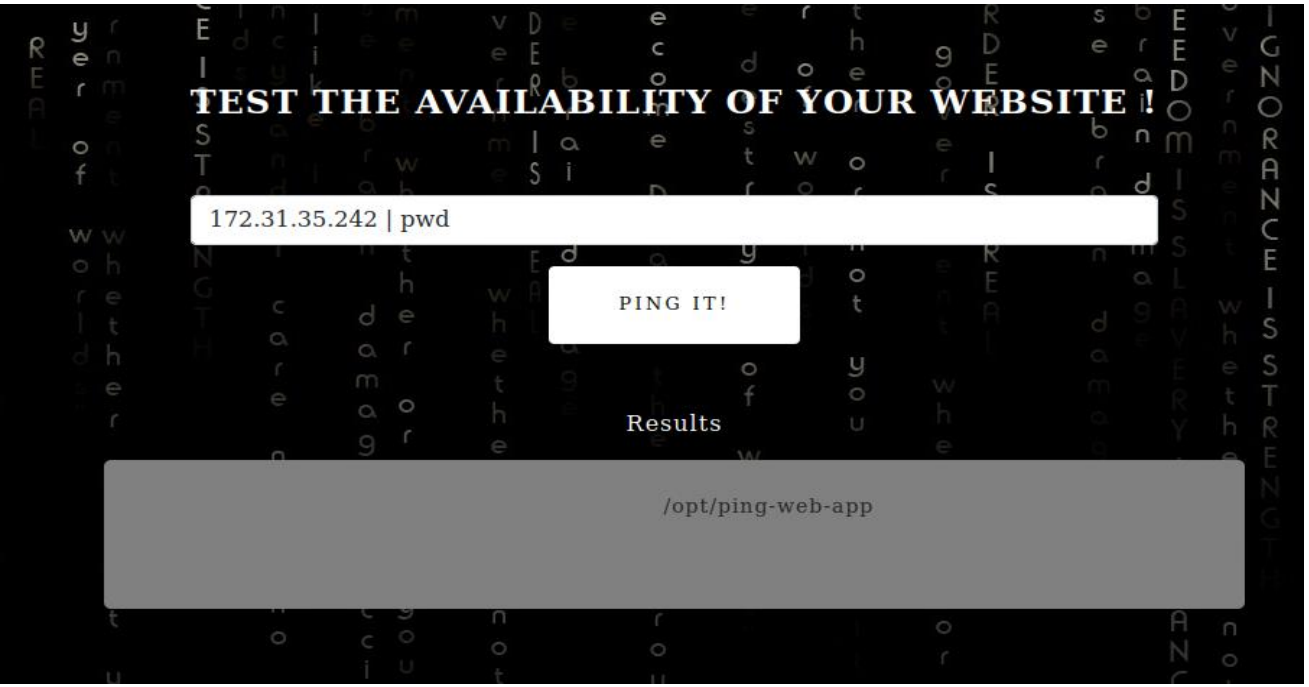






Après les résultat nmap on constate qu'il y a un port 80 http sur l'adresse IP 172.31.35.242
On ouvre firefox et on visite la page web.

Ce site web http envoie des pings et affiche comme résultat les ping envoyé à l'adresse IP qu'on rentre comme input.



J'ai eu l'idée de lancer des commande bash avec un pipe et j'obtiens le user www.data.

Pour parvenir à cela j'ai voulu tester avec la commande pwd pour afficher dans quel répertoire je me trouve actuellement.

Avec la commande whoami , qui veut dire " qui suis-je " me permet d'afficher l'utilisateur.

Cette vulnérabilité est lié à **l'OWASP A03:2021 Injection.**

Vulnérabilité 2:

```
alice@jedhabootcamp:/home$ ls
alice   bob   john
```

```
┌──(kali㉿kali)-[~]
└─$ hydra -l john -P /home/kali/Desktop/rockyou.txt ssh://172.31.35.242
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret serv
ns, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-03-18 12:05:24
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the
4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previo
d, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344398 login tries (l:1/p:14344398), ~896525 tr
[DATA] attacking ssh://172.31.35.242:22/
[STATUS] 136.00 tries/min, 136 tries in 00:01h, 14344263 to do in 1757:53h, 15 active
[STATUS] 105.33 tries/min, 316 tries in 00:03h, 14344083 to do in 2269:39h, 15 active
[STATUS] 98.71 tries/min, 691 tries in 00:07h, 14343708 to do in 2421:46h, 15 active

[22][ssh] host: 172.31.35.242   login: john   password: peterpan
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 1 final worker threads did not complete until end.
[ERROR] 1 target did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-03-18 12:16:33
```

Depuis le serveur ssh avec l'utilisateur alice on peut identifier l'utilisateur john dans le répertoire /home.

Je décide de faire une attaque brute force avec hydra.

Hydra –l john –P /home/kali/Desktop/rockyou.txt ssh://172.31.35.242

Hydra : outil bruteforce
-l : nom utilisateur
-P : chemin du dictionnaire
Ssh://172.31.35.242 : protocole et IP cible.

Cela me permet d'envoyer plusieurs mots dans le password de l'utilisateur john à partir du dictionnaire rockyou.txt

J'obtiens comme résultat peterpan.

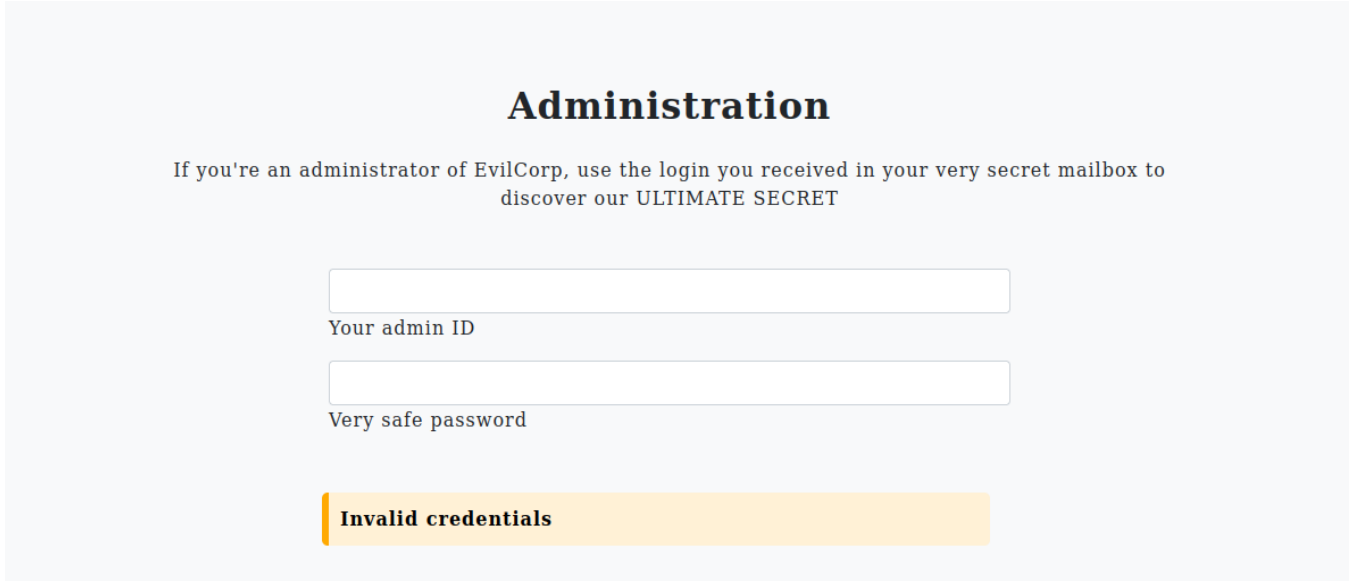
Je fais une connexion ssh
john@172.31.35.242
Et j'utilise le mot de passe peterpan

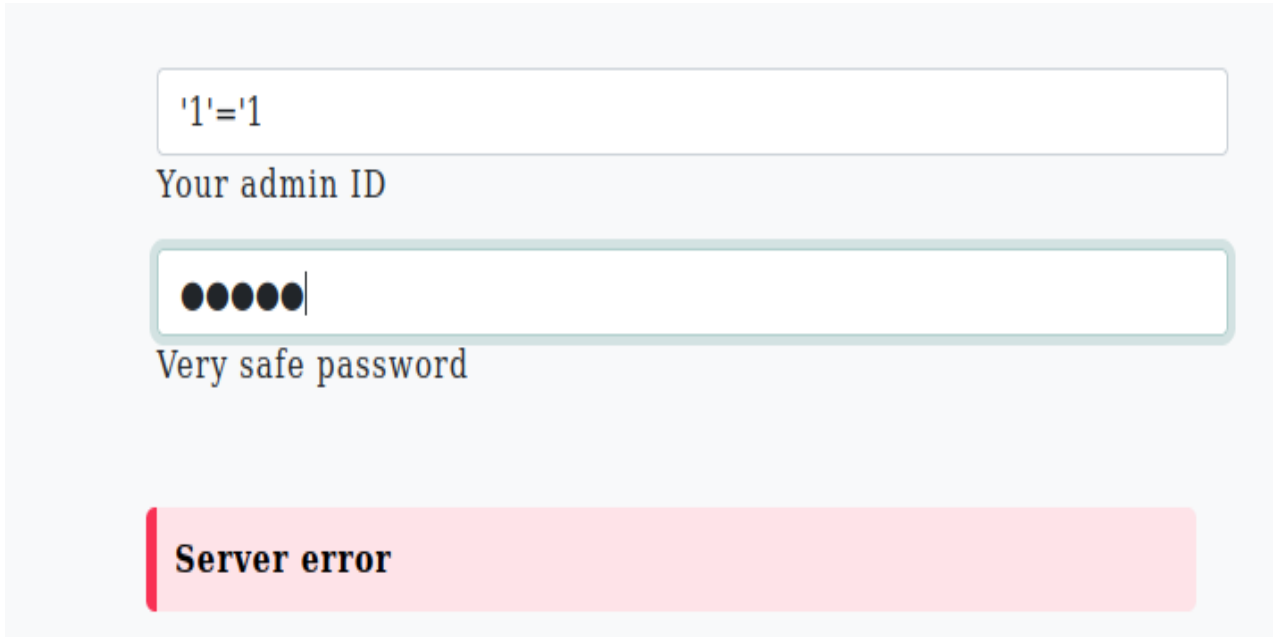
La connexion a bien été autorisé.

Vulnérabilité 4 :

Avec les résultat obtenu nmap , on s'aperçoit que le port 1337 est un site web.

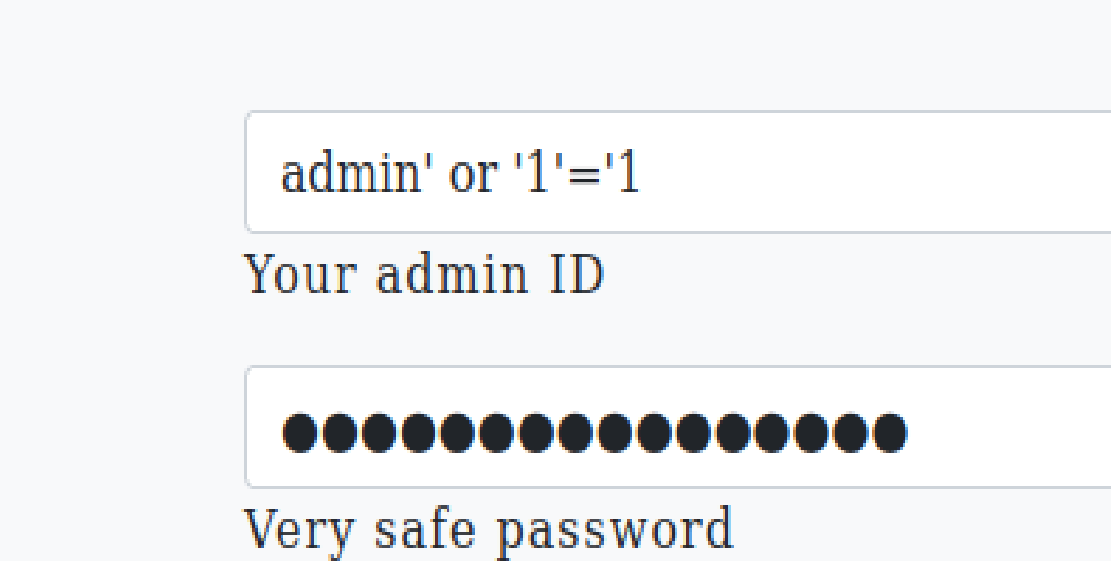
Il y a une page d'accueil et également un onglet Administration.





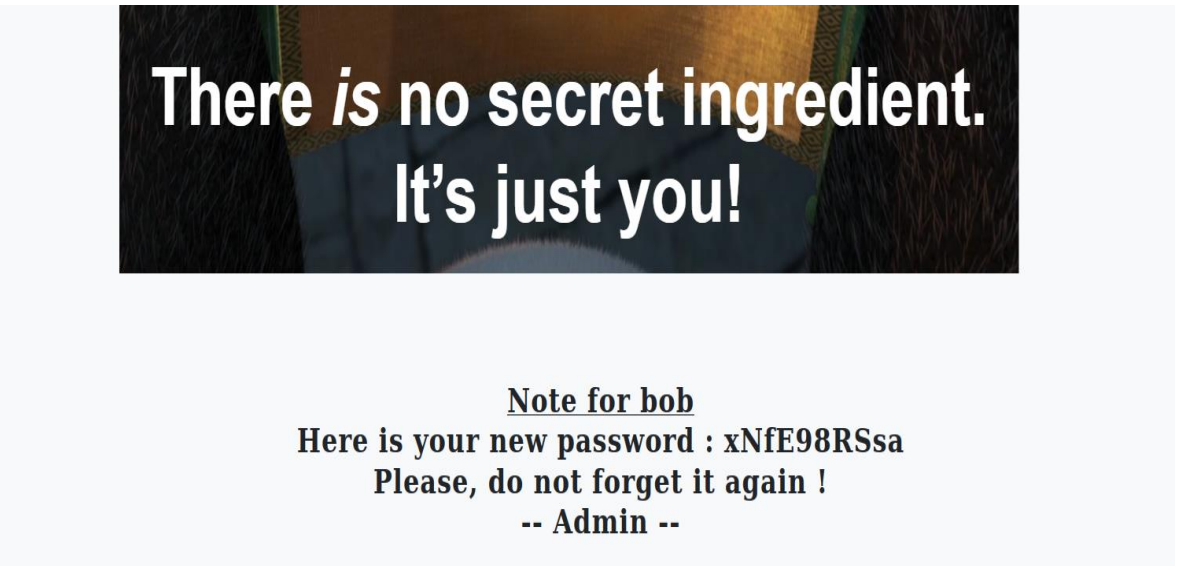
Depuis l'onglet Administration on peut voir qu'il y a un formulaire d'authentification , J'ai tapé une commande au hasard et le site me renvoie comme réponse Invalid Credentials qui dit " Authentifiant invalide " ce qui est une réponse tout à fait normal

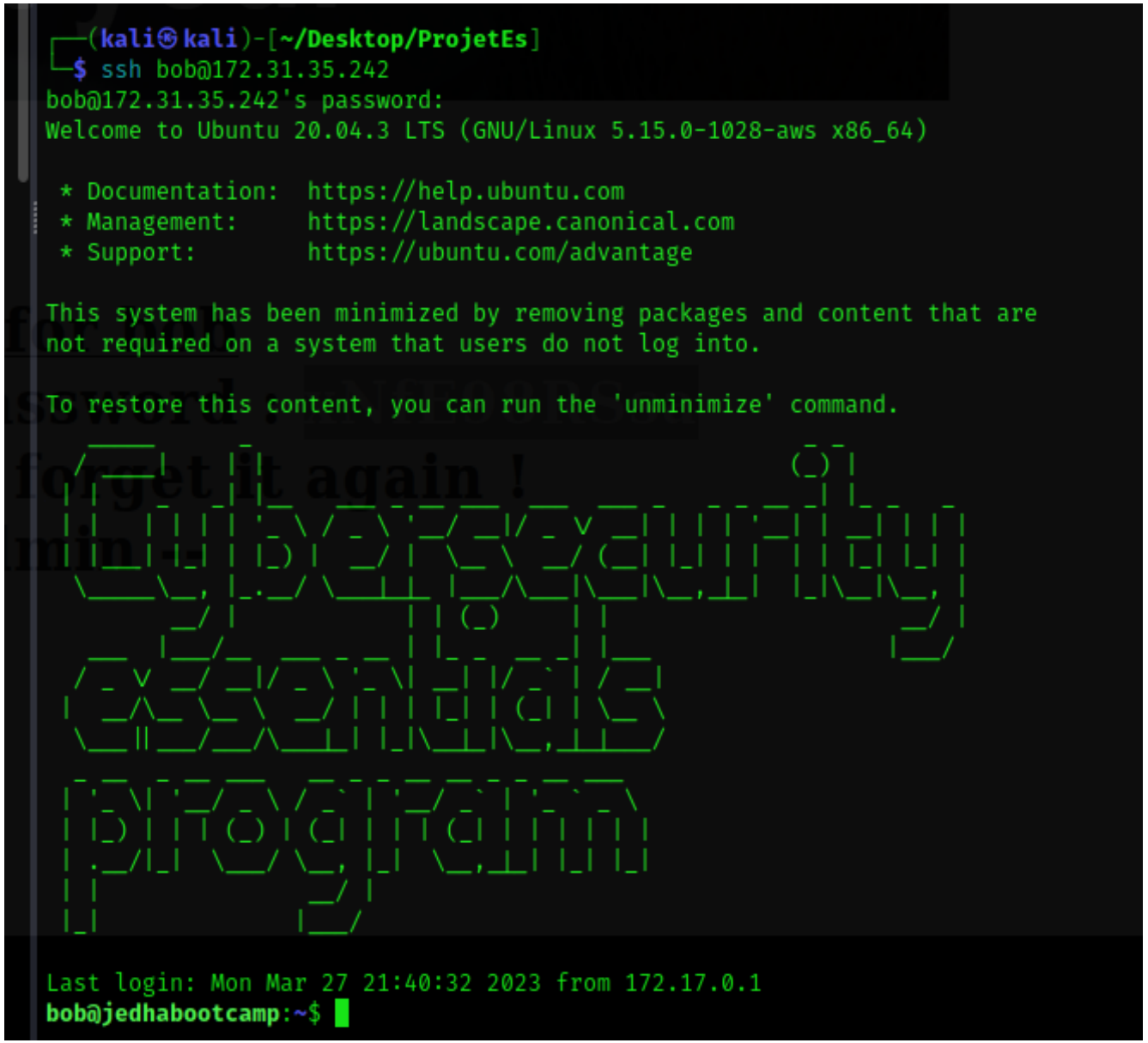
Cependant avec une injection SQL il me renvoie Server error , ce qui me donne comme idée que le site est vulnérable au injection SQL.



Je tente l'injection admin' or '1' = '1

Avec cette injection j'ai réussi à Bypass le système d'authentification ce qui est lié à la vulnérabilité de **l'OWASP A03 2021 Injection.**





Commande de connexion :
ssh bob@172.31.35.242

On obtiens bien une connexion autorisé avec le mot de passe : xNfE98RSsa

Correction des vulnérabilités :

Vulnérabilité 1 : La vulnérabilité 1 n'as pas de contrôle d'un formulaire WEB , il faut mettre en place un WAF (Web Application Firewall) qui est un pare-feu applicatif pour les applications web. Il surveille et filtre le trafic HTTP entre un navigateur web et l'application web pour empêcher les attaques de type injection.

Vulnérabilité 2 : La vulnérabilité 2 est que l'utilisateur john à un mot de passe trop faible trop facile a cracker , pour le rendre beaucoup plus difficile a cracker il faut utiliser un mot de passe plus complexe , mettre en place une politique de mot de passe qui demande 8 caractère & 1 spécial caractère & 1 chiffre minimum.

Vulnérabilité 4 : La vulnérabilité 4 est que le site est vulnérable au injection SQL , il est recommandé de mettre en place des contrôles d'entrées pour éviter que des requêtes malveillantes ne soient exécutées, d'utiliser des requêtes préparées pour éviter les injections SQL et de mettre à jour régulièrement les bibliothèques et les composants du site pour prévenir les vulnérabilités connues cad mettre en place un WAF aussi.