Une image contenant cadenas, verrouiller

Le contenu généré par l’IA peut être incorrect.

|  |
| --- |
| TryHackMe  Capture the Flag  Room : Brains (easy) |
| TryHackMe | Cyber Security TrainingUne image contenant oiseau, Graphique, conception  Description générée automatiquement |
| Réalisé par : CHARPEIL Romain |

## RED Team

## Scanning

Pour ce CTF là, j’ai recherché comment effectuer un scan disons ‘réaliste’ :

Nmap -sS -p- -sV –version-light -O –osscan-limit @ip

-sS : SYN scan (demi-connexion, plus discret qu'un TCP connect -sT)

-p- : Scanne tous les ports (1-65535) au lieu des 1000 par défaut

-sV --version-light : Détecte les versions des services mais en mode léger

-O --osscan-limit : Essaie d’identifier l’OS mais uniquement si les conditions sont bonnes

Une image contenant texte, capture d’écran, Police

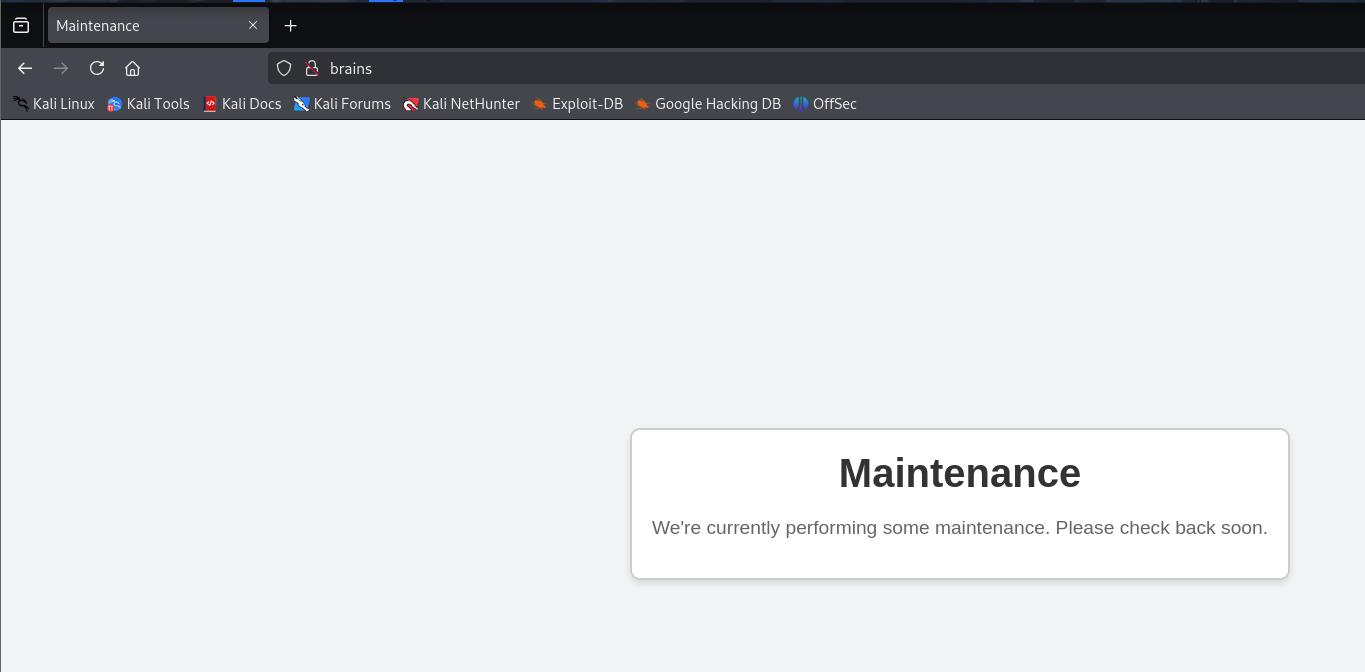
Le contenu généré par l’IA peut être incorrect.

Port http 80 et 50000 Apache Tomcat ouverts.

Une image contenant texte, clipart, graphisme, dessin humoristique

Le contenu généré par l’IA peut être incorrect.

La page du serveur http :



Une image contenant texte, capture d’écran, logiciel, Page web

Le contenu généré par l’IA peut être incorrect.Une image contenant texte, capture d’écran, menu

Le contenu généré par l’IA peut être incorrect.

On va directement gobuster :

Gobuster dir -e -u <http://brains> -w /usr/share/wordlists/dirb/bin.txt

Une image contenant texte, Police, capture d’écran

Le contenu généré par l’IA peut être incorrect.

On sait que Tomcat est au port 50000, donc dans l’URL :

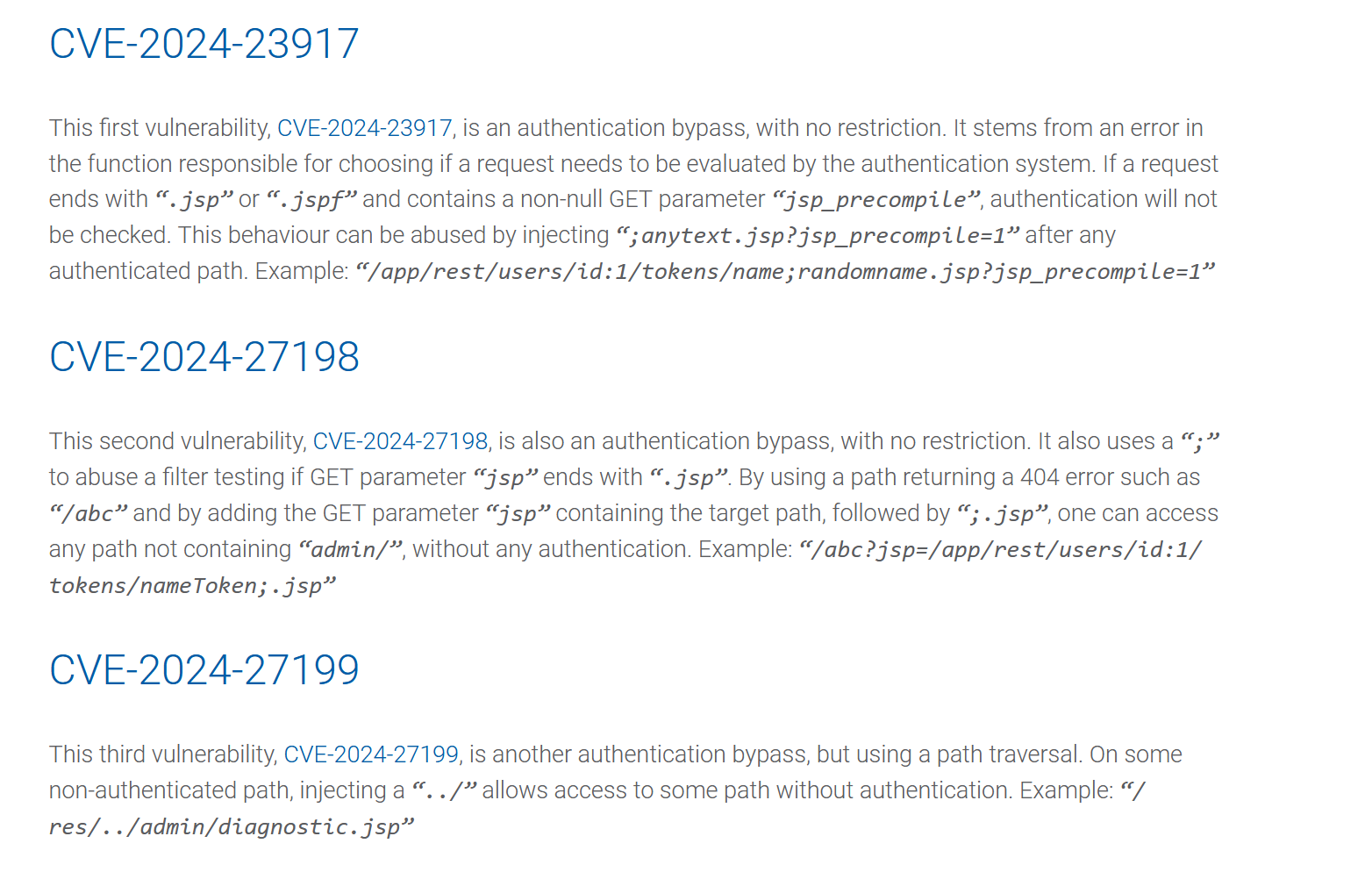
Une image contenant texte, capture d’écran, logiciel, Logiciel multimédia

Le contenu généré par l’IA peut être incorrect.

On avait une version notée :



Sur internet, si on regarde, il y a :



## Exploitation

Des exploits qui permettent de Bypass l’authentification ;

L’exploit était disponible sur Metasploit, celui permettait de faire du Remote Code Exécution

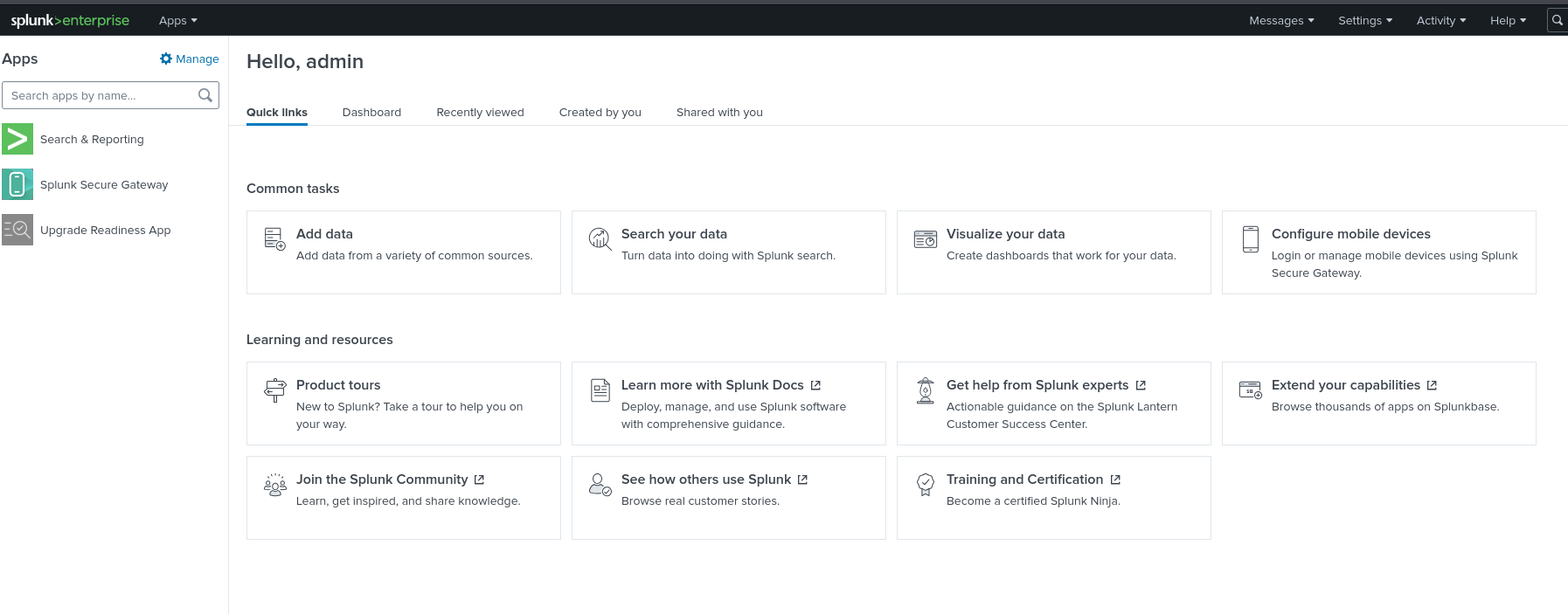
Une image contenant texte, capture d’écran, Police

Le contenu généré par l’IA peut être incorrect.

Une image contenant texte, capture d’écran, Police

Le contenu généré par l’IA peut être incorrect.

## BLUE Team



Nous sommes sur une instance Splunk, il faut faire de l’investigation :

What is the name of the backdoor user which was created on the server after exploitation?

Eviluser



Haut du formulaire

Bas du formulaire

What is the name of the malicious-looking package installed on the server?

Datacollector



Haut du formulaire

Bas du formulaire

What is the name of the plugin installed on the server after successful exploitation?

AyzzbuXY.zip

