CTF : DG'Hack

Julien ROYON CHALENDARD

CTF :
Walter's Blog

Catégorie :
Web

12 - 27 Novembre 2020

Sommaire

1 Description

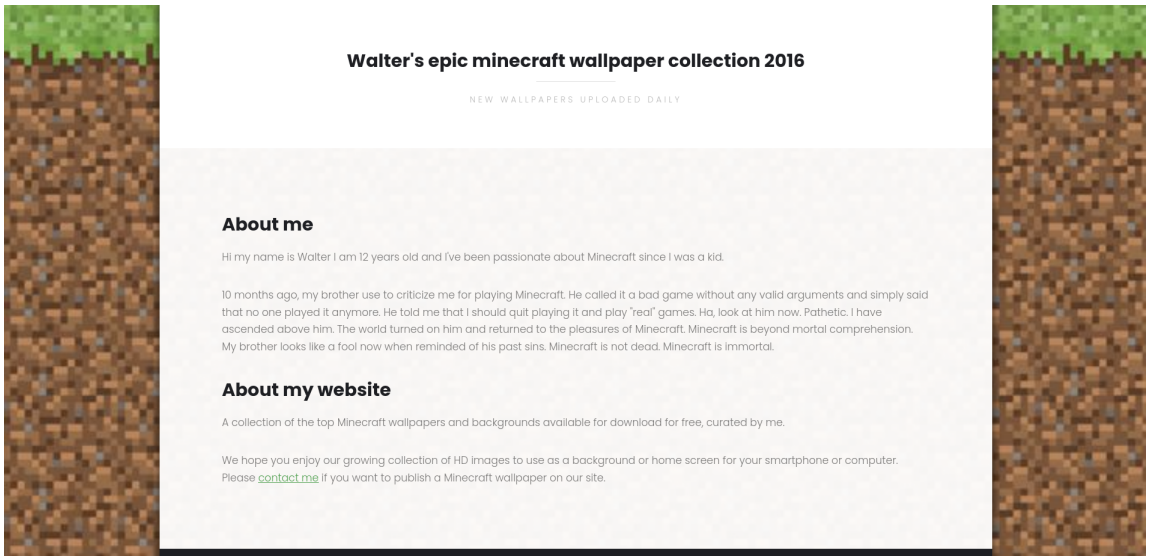
Un ancien stagiaire avait développé ce site web il y a plusieurs années. Malheureusement, ce projet a mal été documenté et nous ne retrouvons plus les accès pour l'administrer...

Votre tuteur vous autorise à tout essayer pour récupérer les accès à ce service, soyez inventif !

Le flag est situé dans le fichier /flag.txt

2 Enumération

Nous parcourons l'application web, il s'agit de wallpapers sur le jeu Minecraft

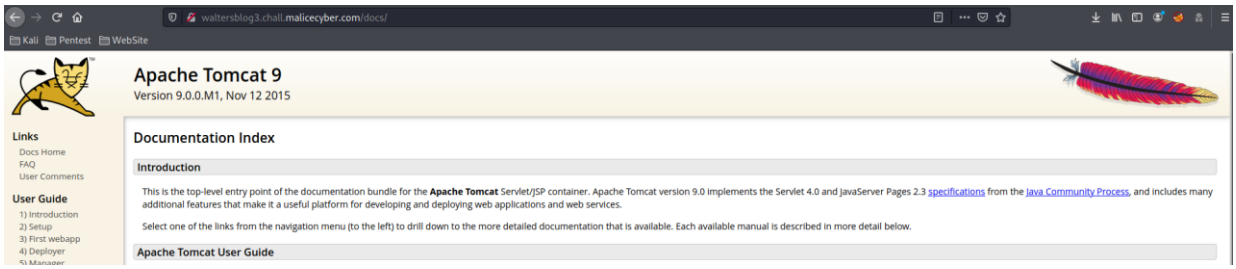


Pour commencer notre énumération, nous commencer par lancer Gobuster qui va nous permettre de rechercher des fichiers ou des répertoires dans l'application web.

```
kali@kali:~/DG'hAck/Walter_Blog$ gobuster dir -u http://waltersblog3.chall.malicecyber.com/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x txt,html,php
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://waltersblog3.chall.malicecyber.com/
[+] Threads:        10
[+] Wordlist:       /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Extensions:     txt,html,php
[+] Timeout:        10s
===============================================================
2020/11/12 23:52:41 Starting gobuster
===============================================================
/images (Status: 302)
/index.html (Status: 200)
/contact.html (Status: 200)
/docs (Status: 302)
/assets (Status: 302)
/examples (Status: 302)
[ERROR] 2020/11/12 23:52:58 [!] Get http://waltersblog3.chall.malicecyber.com/00.php: net/http: request canceled (Client.Timeout exceeded while awaiting headers)
[ERROR] 2020/11/12 23:53:02 [!] Get http://waltersblog3.chall.malicecyber.com/blue.txt: net/http: request canceled (Client.Timeout exceeded while awaiting headers)
[ERROR] 2020/11/12 23:53:12 [!] Get http://waltersblog3.chall.malicecyber.com/power.txt: net/http: request canceled (Client.Timeout exceeded while awaiting headers)
/manager (Status: 302)
[ERROR] 2020/11/12 23:53:40 [!] Get http://waltersblog3.chall.malicecyber.com/l2: net/http: request canceled (Client.Timeout exceeded while awaiting headers)
Progress: 6311 / 220561 (2.86%)
```

Nous remarquons plusieurs éléments intéressant qui sont «docs», «examples» et «manager». Avec un peu de pratique, nous remarquons qu'il s'agit d'un service Tomcat sur le serveur.

Pour s'en assurer et avoir la version du service, nous allons voir «docs».



Nous voyons qu'il s'agit bien d'un Tomcat dans sa version 9.0.0

Suite à cela, nous décidons d'utiliser «searchsploit» pour voir s'il existe des vulnérabilités concernant Apache Tomcat 9.

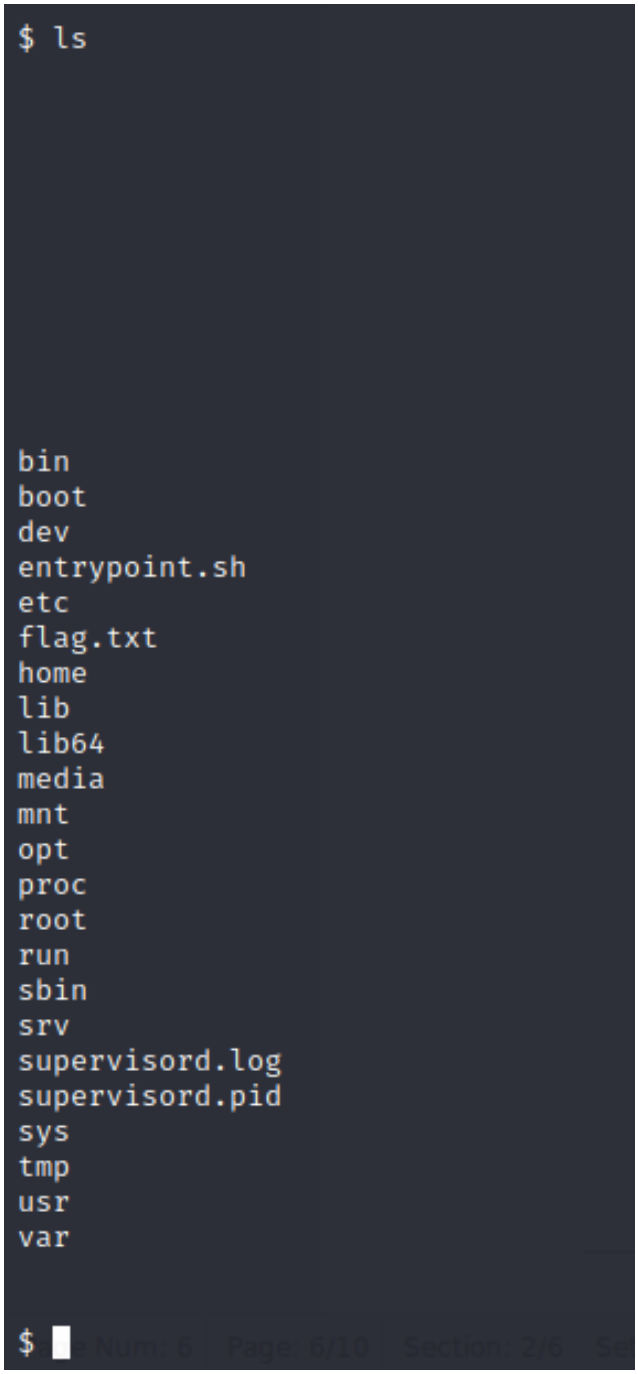
Il y a « Apache Tomcat ¡ 9.0.1 (Beta) / ¡ 8.5.23 / ¡ 8.0.47 / ¡ 7.0.8 - JSP Upload Bypass / Remote Code Execution (1)» qui pourrait correspondre à notre version de Tomcat.

3 Exploitation

En regardant le programme Python donné, il s'agit de la CVE 2017 - 12617 qui permet d'upload un fichier JSP sur le serveur et de l'exécuter.

On exécute le programme en ajoutant en argument l'application web ainsi que l'argument permet de faire spawn un shell.

Nous sommes connecté sur le serveur, nous pouvons regarder le fichier flag.txt



Le fichier flag.txt se situe à la racine du serveur.

Nous avons récupéré le flag.