

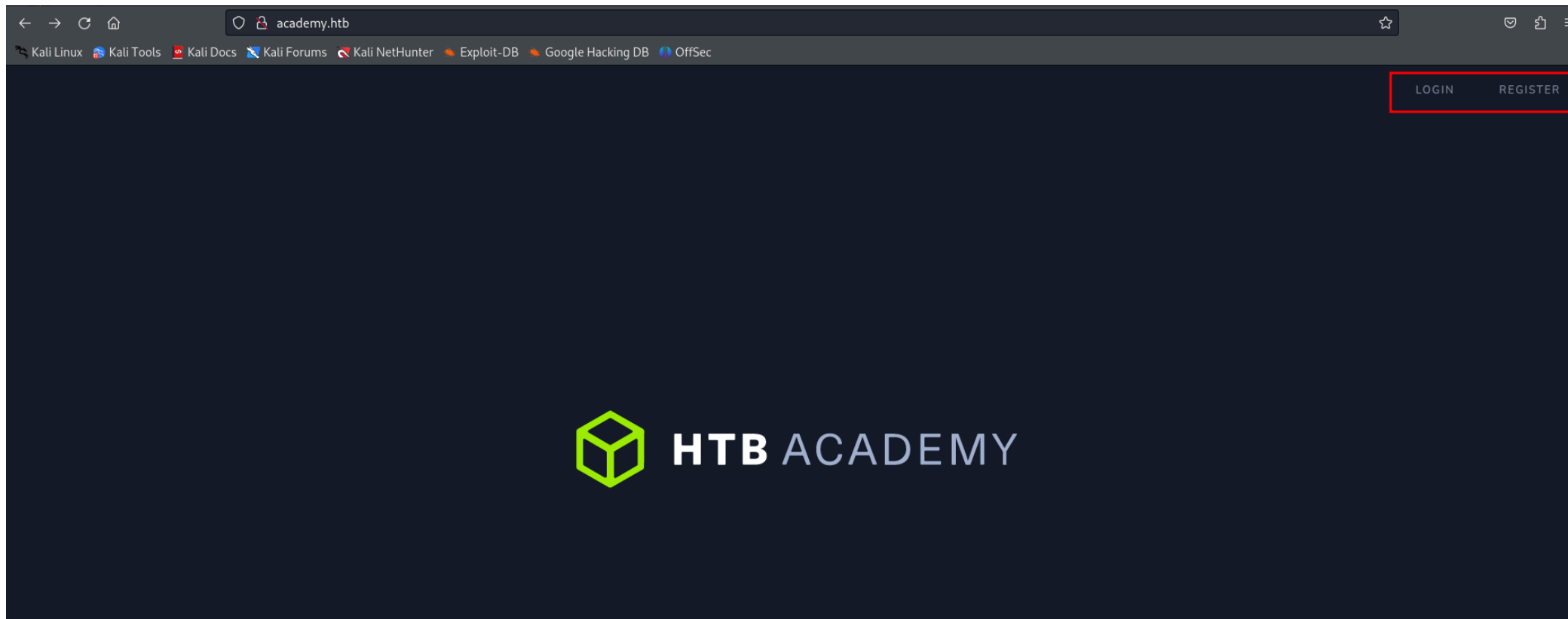
Academy

academy.htb

Nmap Scans


```
``` sudo nmap -p- --min-rate=10000 academy.htb

PORT STATE SERVICE 22/tcp open ssh 80/tcp open http 33060/tcp open mysqlx
```
```



← → ↻ 🏠 academy.htb/login.php

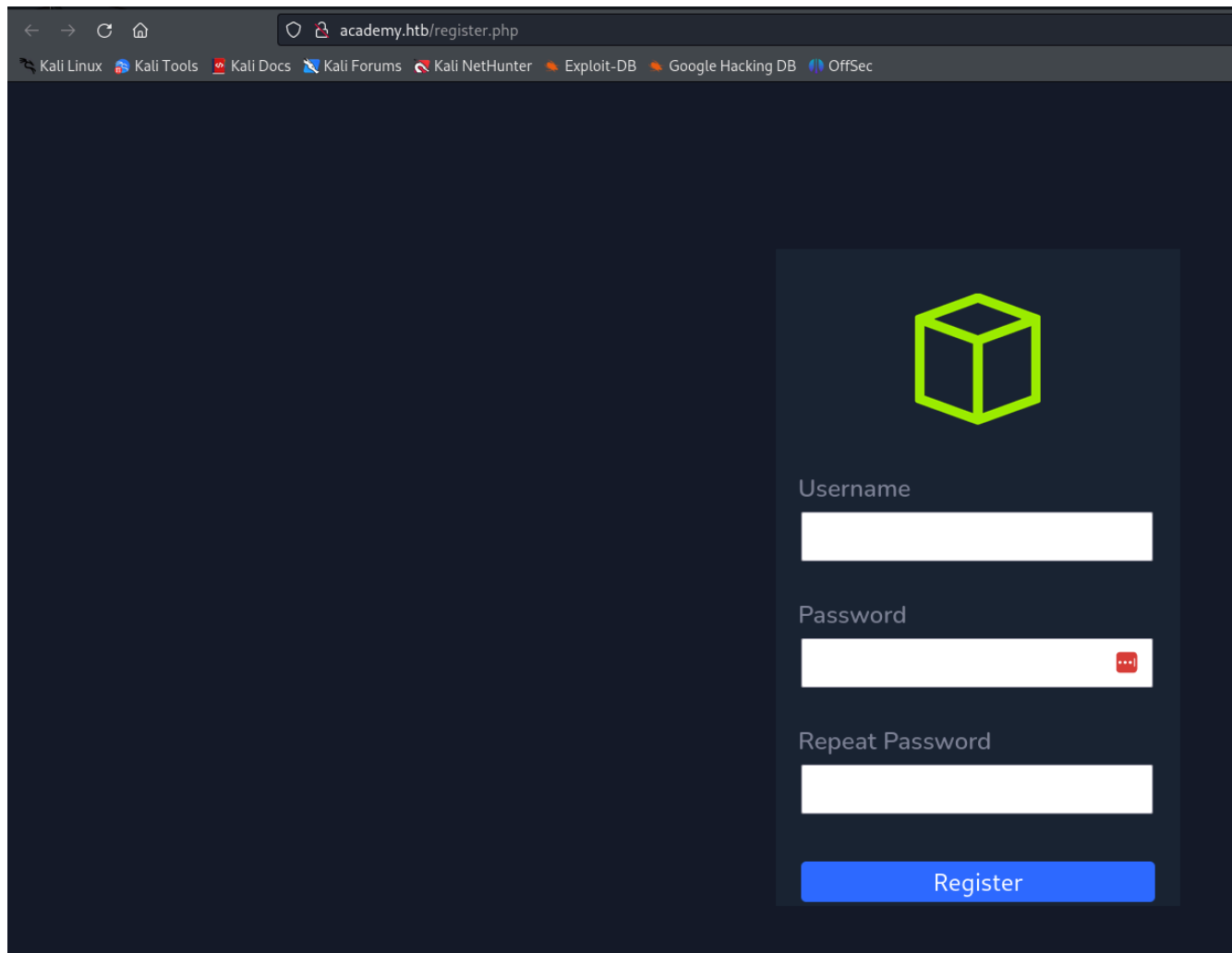
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec



Username

Password


Login



The screenshot shows a web browser window with the address bar displaying `academy.htb/register.php`. The browser's tab bar includes links to Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, and OffSec. The main content area features a registration form with a green cube icon at the top. The form consists of three input fields: Username, Password, and Repeat Password, followed by a blue Register button.

academy.htb/register.php

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec



Username

Password

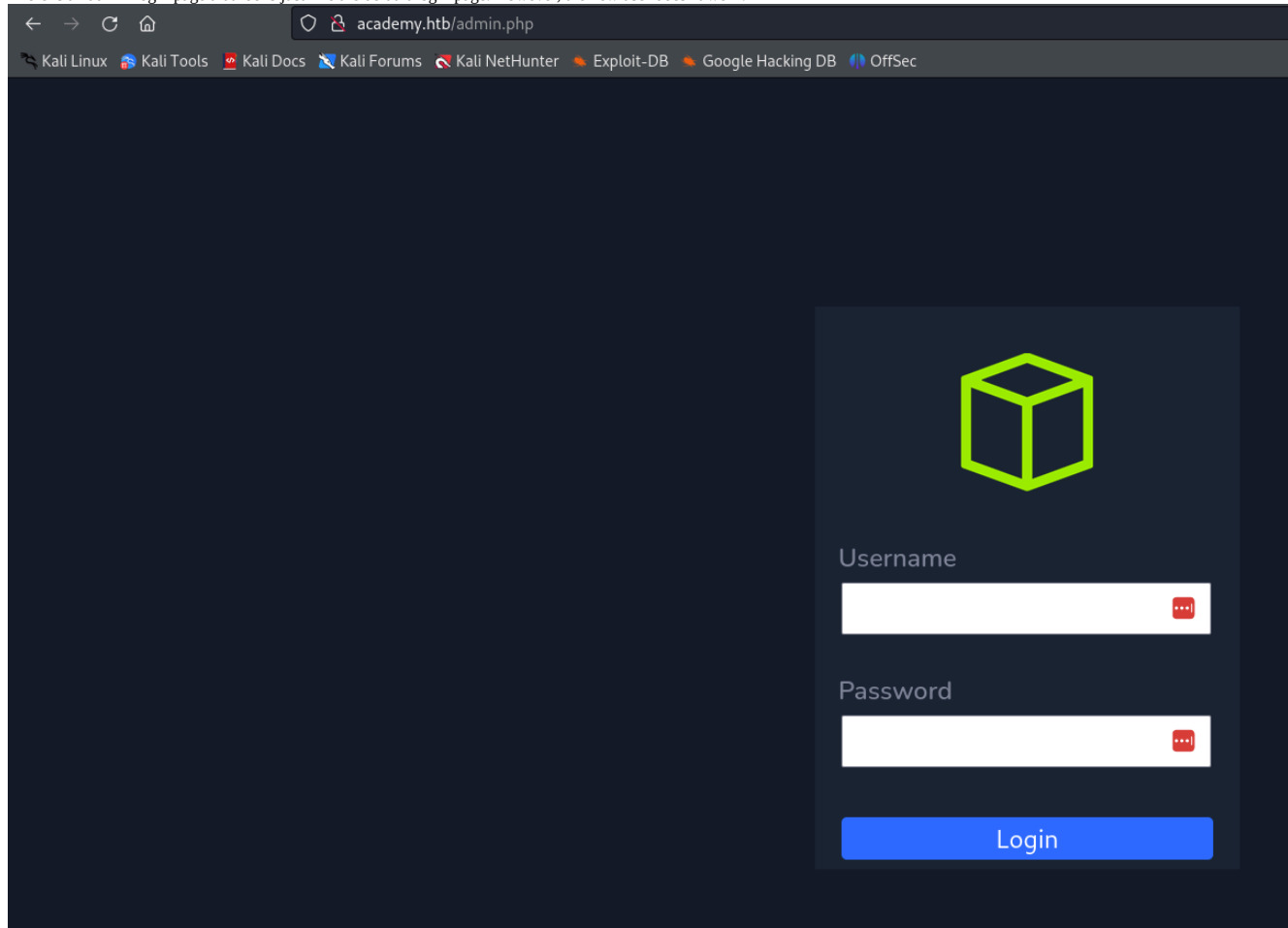
Repeat Password

Register

I created a random user

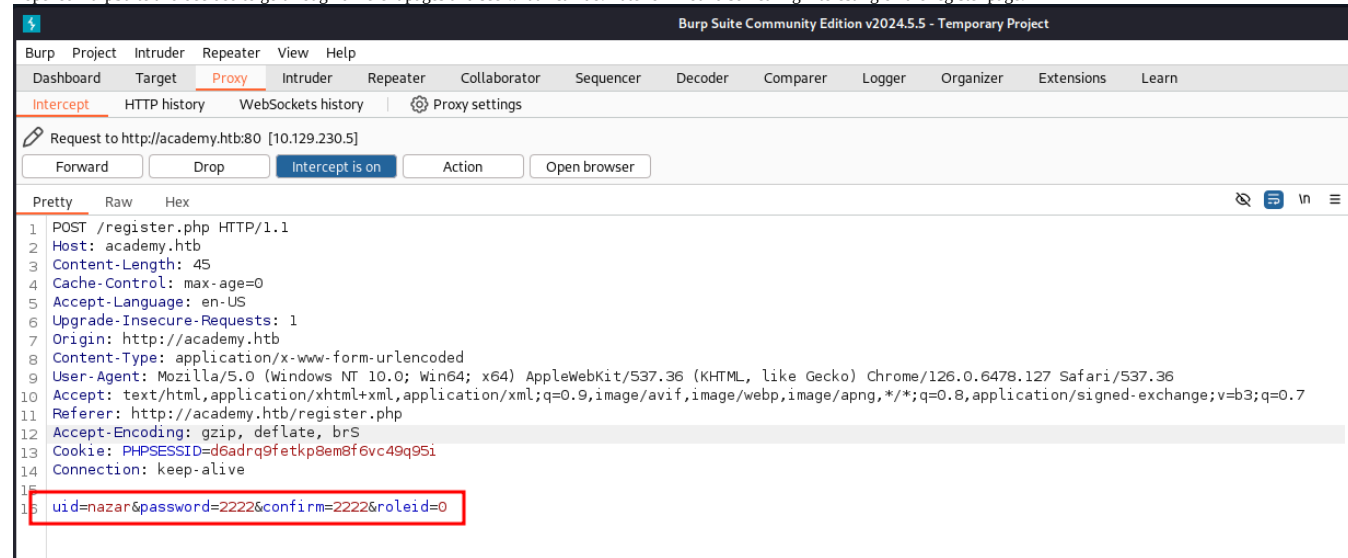


There is an admin login page that looks just like the default login page. However, the new user doesn't work.



BurpSuite

I opened BurpSuite and decided to go through different pages and see what I can do. Later on I found something interesting on the register page.



Admin Role

I set roleid to 1 than went to the admin.php and got in.

← → ↻ ⚠ Not secure 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 |

Subdomain

That's where I found a subdomain.

← → ↺ 🏠

🔒 dev-staging-01.academy.htb

☆

🔍 📄 📁

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

UnexpectedValueException

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

G 📄 📁 COPY

Application frames (1) All frames (11)

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:113

2 Illuminate\Foundation\Exceptions\Handler report

.../app/Exceptions/Handler.php:39

/var/www/html/htb-academy-dev-01/app/Exceptions/Handler.php

```
29.  /**
30.   * Report or log an exception.
31.   * This is a great spot to send exceptions to Sentry, Bugsnag, etc.
32.   *
33.   * @param \Exception $exception
34.   * @return void
35.   */
36.  public function report(Exception $exception)
37.  {
38.      parent::report($exception);
39.  }
40.
41.
42.  /**
43.   * Render an exception into an HTTP response.
44.   *
45.   * @param \Illuminate\Http\Request $request
46.   * @param \Exception $exception
47.   * @return \Illuminate\Http\Response
48.   */
49.  public function render($request, Exception $exception)
50.  {
51.      return parent::render($request, $exception);
52.  }
53.  }
```

No comments for this stack frame.

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 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0

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_CONNECTION

keep-alive

It looks like a page where we can see all the logs. Discovering a little bit more I realized that it was the laravel framework. Then I found an exploit CVE-2018-15133 and used it to get a shell.

User Flag

Reading this file: /var/www/html/academy/.env I found a password for user cry011t3 and sshed into it. Interesting that the user is part of group adm.

Root

In order to, not to spend too much time I used the hint and found that I had to read the audit logs. Using a tool called: aureport and the next command: aureport --tty I found a password to user mrb3n

Then, using sudo -l I found that the user can execute composer as a root. Then I found how to exploit it to get root. https://gtfobins.github.io/gtfobins/composer/#sudo