

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.

Изображение выглядит как текст

Автоматически созданное описание

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).

Изображение выглядит как текст

Автоматически созданное описание

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 2 – Результаты gobuster

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 3 - Страница 10.10.11.104/js

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 4 - Страница 10.10.11.104/css

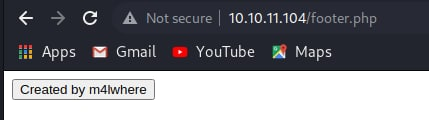


Рисунок 5 - Страница 10.10.11.104/footer.php

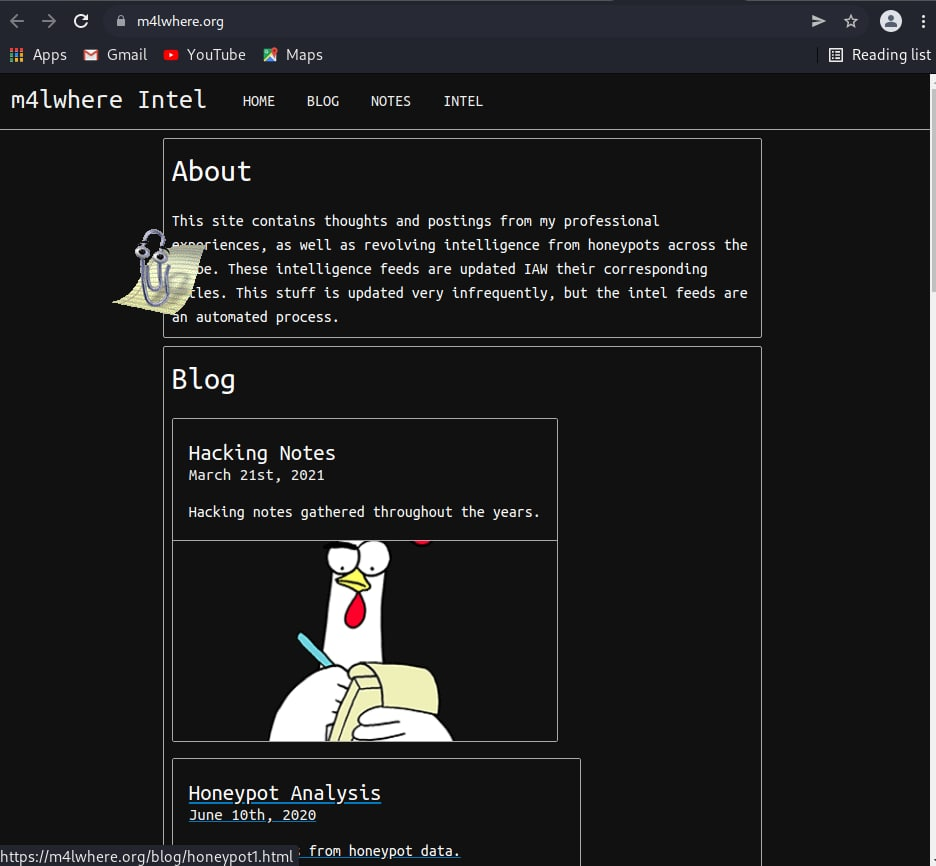


Рисунок 6 – Результат перехода по кнопке «created by m4lwhere»

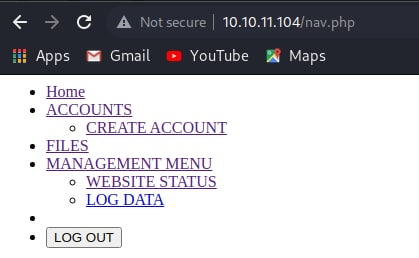


Рисунок 7 – Найденное меню

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).

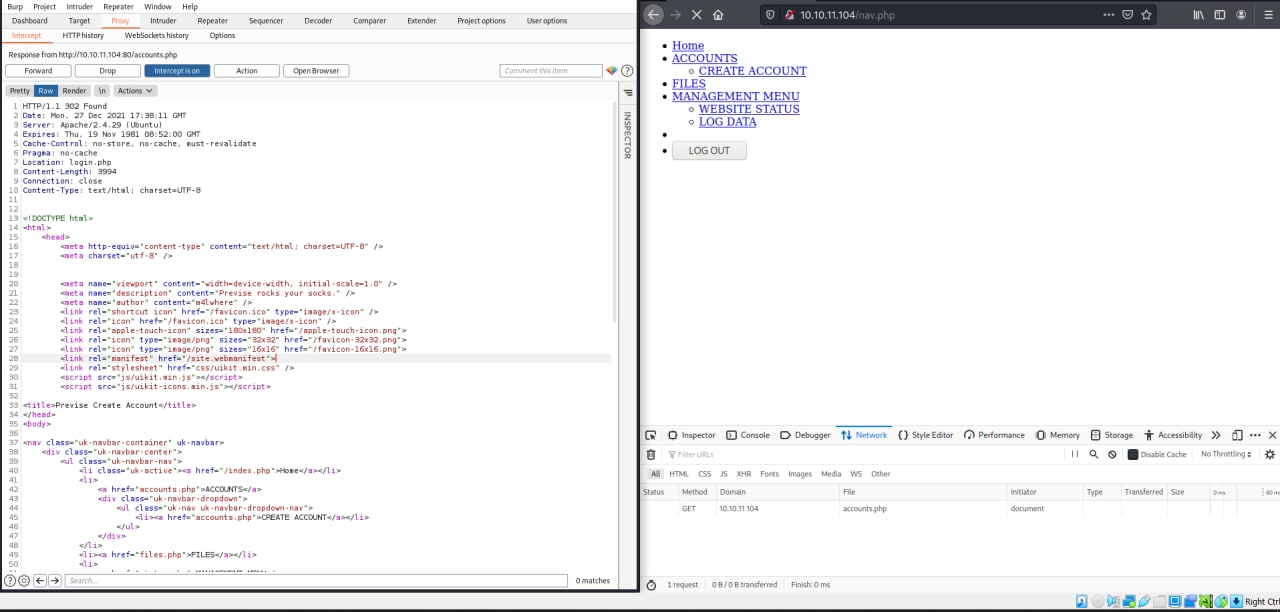


Рисунок 8 – Перехват страницы



Рисунок 9 – Заменяем http-код на 200

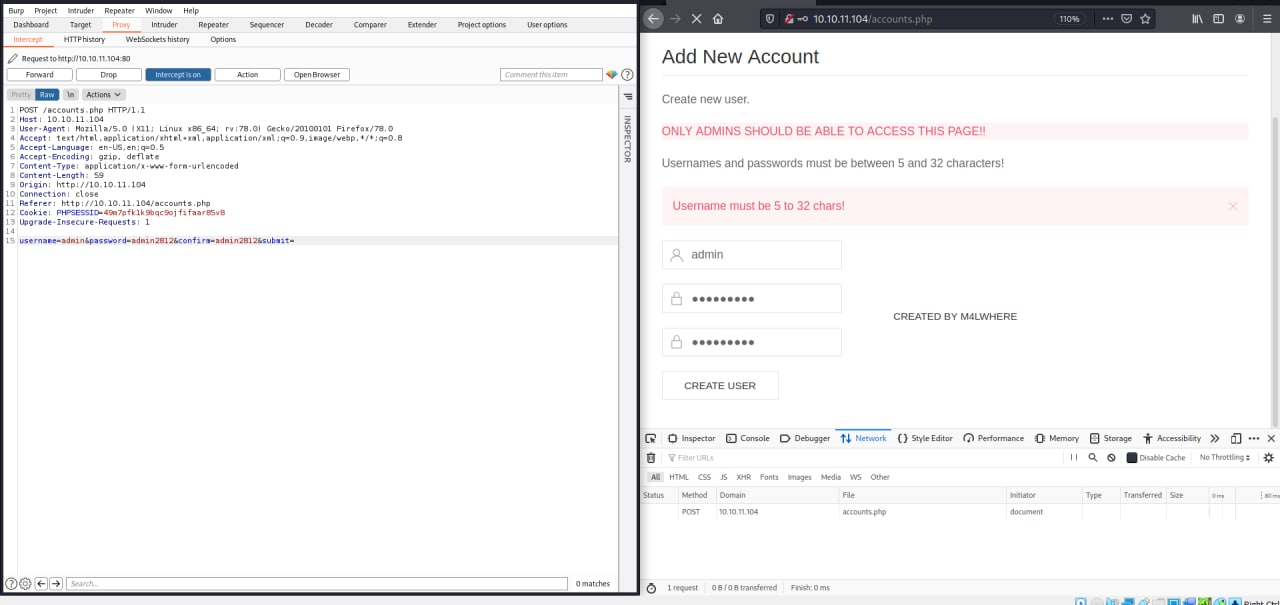


Рисунок 10 – Создание аккаунта

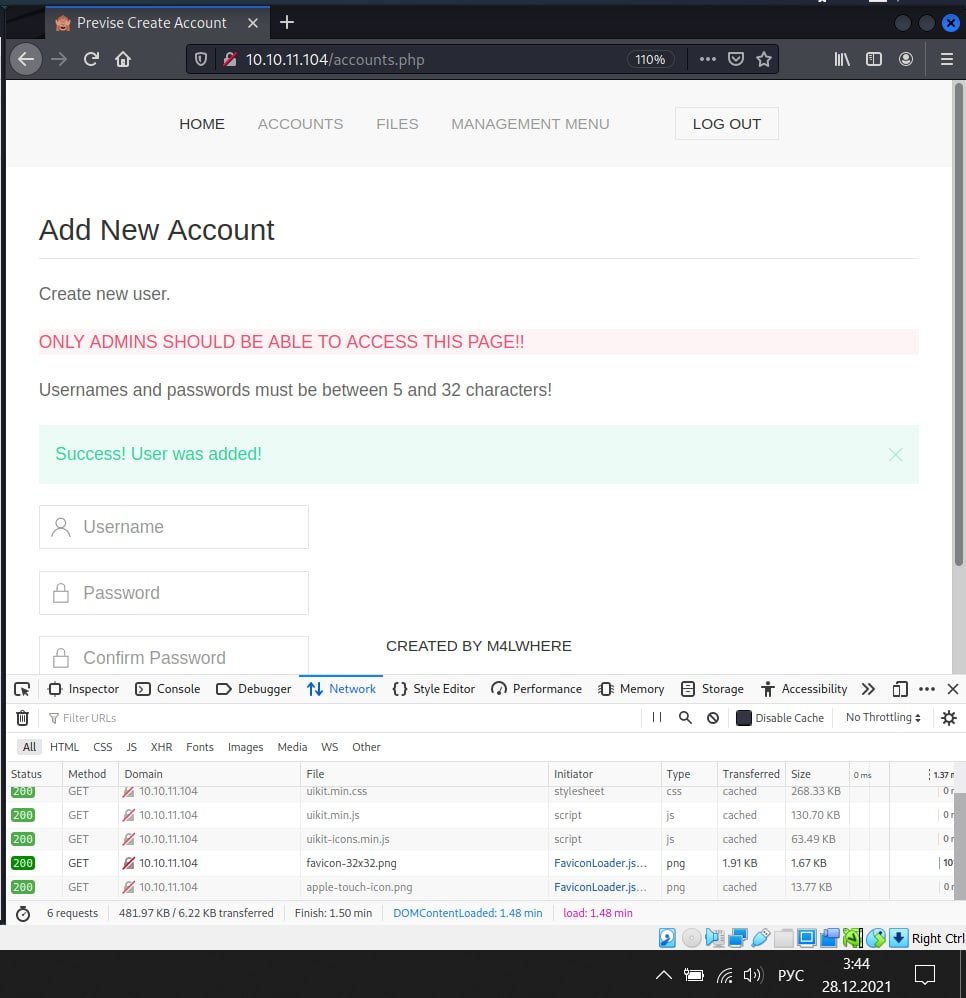


Рисунок 11 – Уведомление о успешном создании аккаунта

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

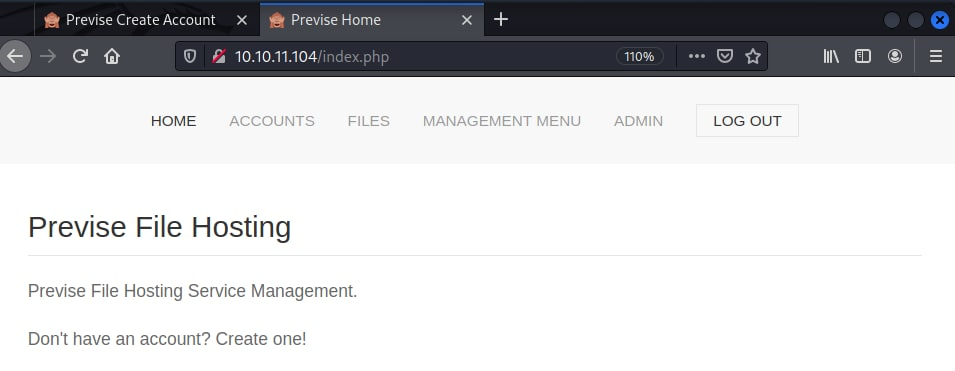


Рисунок 12 – Меню после авторизации

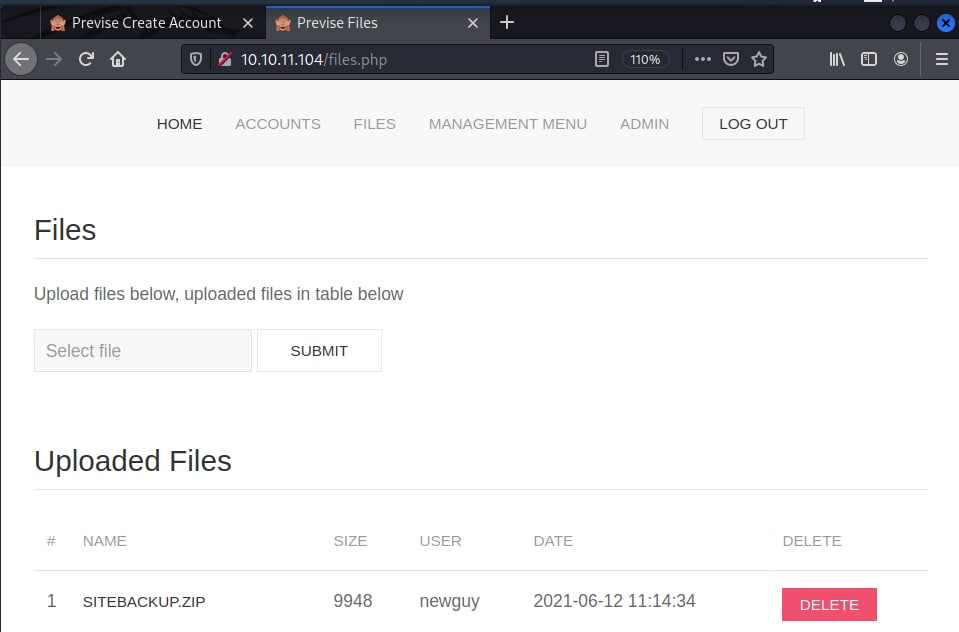


Рисунок 13 – Найден архив

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

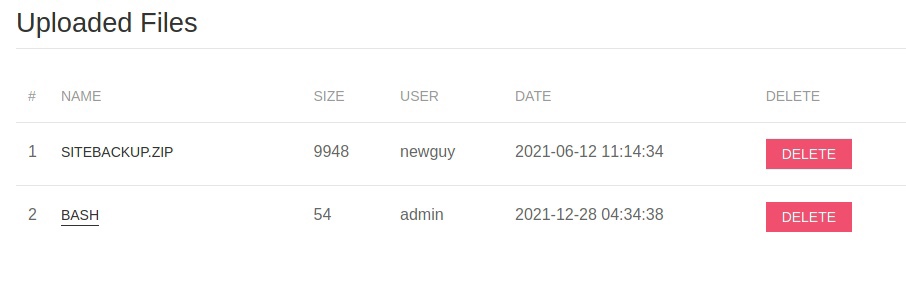


Рисунок 14 – Доступ к архиву и еще одному файлу

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 15 – Содержимое второго файла

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

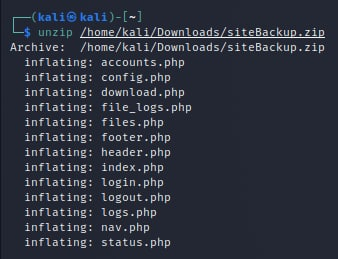


Рисунок 16 – Распаковка архива

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 17 – Страница подключения к БД

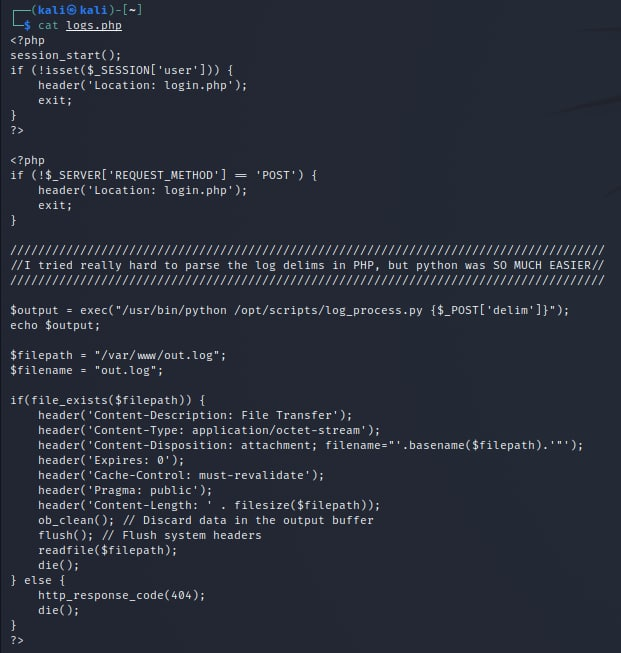


Рисунок 18 – Найденная функция exec в исходном коде

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).

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 19 – Первоначальный перехват burp

Изображение выглядит как текст

Автоматически созданное описаниеРисунок 20 – Подмена значения на иньекцию

Изображение выглядит как текст

Автоматически созданное описание

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).

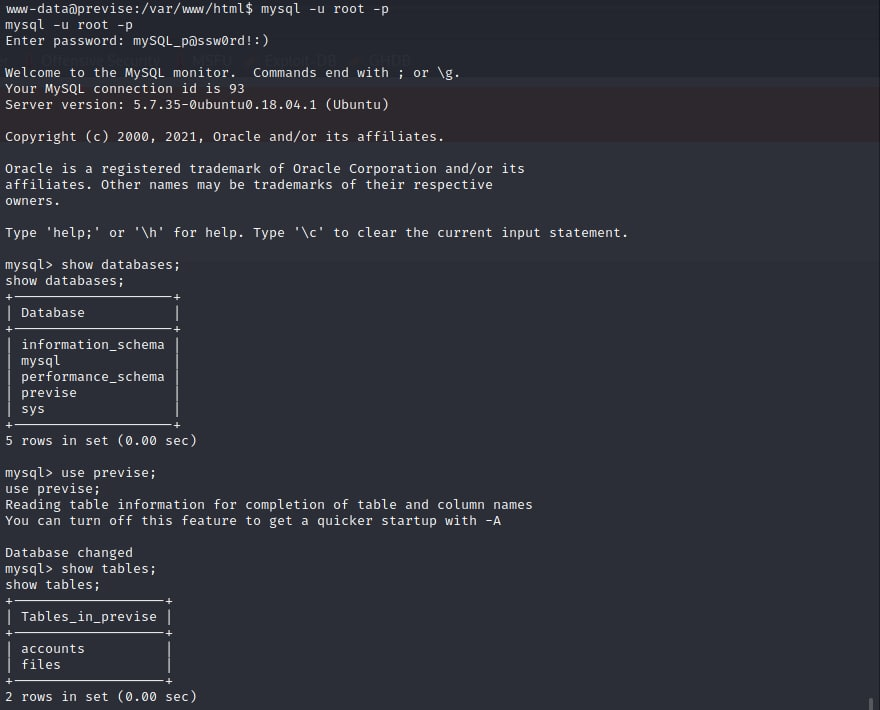


Рисунок 22 – работа с БД

Изображение выглядит как текст, снимок экрана, монитор, экран

Автоматически созданное описание

Рисунок 23 – Полученная база пользователей

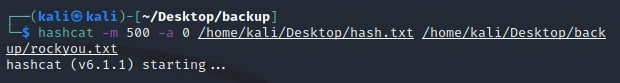


Рисунок 24 – Запуск восстановления пароля

Изображение выглядит как текст, табличка

Автоматически созданное описание

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).

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 26 – Получение флага

Итоговые значения:

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

