

Федеральное государственное автономное образовательное учреждение высшего
образования

«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

Факультет информационных технологий
Кафедра «Информационная безопасность»

Направление подготовки/ специальность: 10.03.01 Информационная безопасность

ОТЧЕТ

по проектной практике

Студент: Ильин Кирилл Александрович Группа: 241-353

Место прохождения практики: Московский Политех, кафедра «Информационная
безопасность»

Отчет принят с оценкой _____ Дата _____

Руководитель практики: Гневшев Александр Юрьевич

Москва 2025

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ.....	2
Общая информация о проекте	3
Название проекта.....	3
Цели и задачи проекта.....	3
Описание задания по проектной практике.....	4
Описание достигнутых результатов по проектной практике	5
ЗАКЛЮЧЕНИЕ	17
СПИСОК ЛИТЕРАТУРЫ.....	17
ПРИЛОЖЕНИЯ	17

ЗАДАНИЕ ПО ПРОЕКТНОЙ ПРАКТИКЕ

Проектная практика включала базовую и вариативную части, общей трудоёмкостью 72 академических часа. Работа выполнялась в составе команды из двух человек: Ильин К.А. (241-353) и Кондраков В.И. (241-371).

Для контроля версий использовалась система Git, документация оформлялась с применением языка разметки Markdown, а для создания статического веб-сайта применялись HTML и CSS. Репозитории размещались на платформе [GitHub](#).

Проект состоял из двух частей: обязательной (базовой) для всех студентов и вариативной, задание на которую было выдано ответственным за практику представителем выпускающей кафедры.

1. Базовая часть задания

1. Настройка Git и репозитория:

Создать групповой репозиторий на [GitHub](#) на основе предоставленного [шаблона](#).

Освоить базовые команды Git: клонирование, коммит, пуш и создание веток.

Регулярно фиксировать изменения с осмысленными сообщениями к коммитам.

Примерное время: 5 часов.

2. Написание документов в Markdown:

Все материалы проекта (описание, журнал прогресса и др.) оформить в формате Markdown.

Изучить синтаксис Markdown и подготовить необходимые документы.

Примерное время: 5 часов.

3. Создание статического веб-сайта:

Для создания сайта необходимо использовать только HTML и CSS.

Создать новый сайт об основном проекте по дисциплине «Проектная деятельность» (INVADE). Оформление и наполнение сайта должны быть уникальны.

Сайт должен включать:

Домашнюю страницу с аннотацией проекта.

Страницу «О проекте» с описанием проекта.

Страницу «Участники» с описанием личного вклада каждого участника группы в проект по «Проектной деятельности».

Страницу «Журнал» с минимум тремя постами (новостями, блоками) о прогрессе работы.

Страницу «Ресурсы» со ссылками на полезные материалы.

Оформить страницы сайта графическими материалами (фотографиями, схемами, диаграммами, иллюстрациями)

Примерное время: изучение и настройка — 14 часов, дизайн и наполнение — 8 часов.

2. Вариативная часть задания:

В качестве вариативной части нашей группе было дано следующее задание:

Тема задания:

"Настроить систему логирования и базового анализа событий безопасности веб-сервера."

Задачи задания:

Установить и настроить веб-сервер (Apache/Nginx).

Включить и настроить ведение логов доступа и ошибок.

Обработать логи: фильтрация атак, brute-force, SQL-инъекции, DoS-атаки (и другие на усмотрение студентов).

Оформить шаблон отчета ИБ-инцидента (карточки инцидента) на основе логов.

Примечание: рекомендуется проводить все манипуляции в изолированном сегменте.

Примерное время: 32-40 часов

ДОСТИГНУТЫЕ РЕЗУЛЬТАТЫ ПО ПРОЕКТНОЙ ПРАКТИКЕ

Изучен язык разметки HTML для формирования базовой структуры веб-сайта
(Затраченное время: 22 часа)

Настроен групповой репозиторий на платформе GitHub, выполнено добавление и отслеживание изменений проекта с использованием системы контроля версий Git;(Затраченное время: 5 часов)

Установлен и сконфигурирован веб-сервер Apache в изолированной среде (локальный сегмент), обеспечена доступность по адресу 127.0.0.1; (Затраченное время: 8 часов)

Активированы и проверены механизмы логирования событий на веб-сервере, включая ведение файлов access.log и error.log; (Затраченное время: 3 часа)

Проведены и зафиксированы три практических теста по моделированию атак:

Brute-force атака на форму входа с использованием инструмента Hydra, приведшая к успешному подбору пароля;

SQL-инъекция с применением утилиты sqlmap, позволившая извлечь данные из уязвимой базы SQLite;

DoS-атака типа Slowloris, направленная на исчерпание доступных соединений веб-сервера, результатом которой стало достижение лимита MaxRequestWorkers и нарушение доступности;

(Затраченное время: 14 часов)

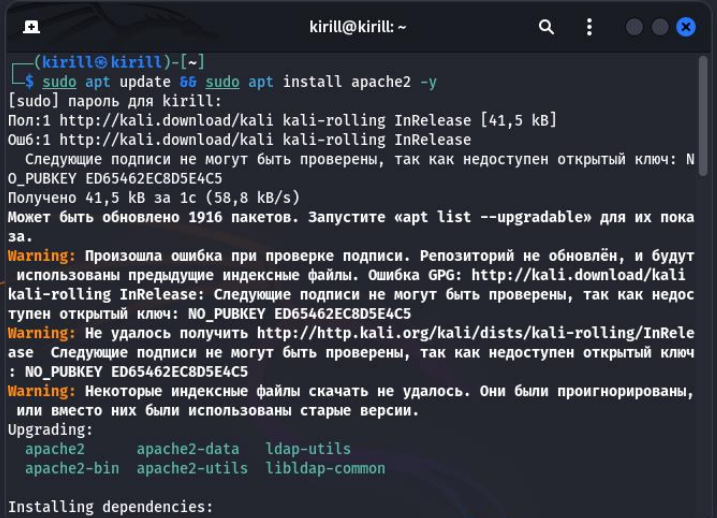
В результате работы получен практический опыт в **использовании HTML, настройки репозитория, по развёртыванию веб-сервера, организации логирования, реализации тестовых атак**. Все действия проводились в рамках изолированной среды и сопровождалось регистрацией действий для последующего документирования.

Также я исполнял обязанности тимлида нашей команды и осуществлял проверку всех файлов, подготовленных сокомандником.

(Анализ требований к работе занял 3 часа, редактирование текста на сайте — 4

часа, создание и наполнение GitHub-репозитория, а также его проверка — 9 часов, участие во всех организационных онлайн-собраниях — 8 часов).

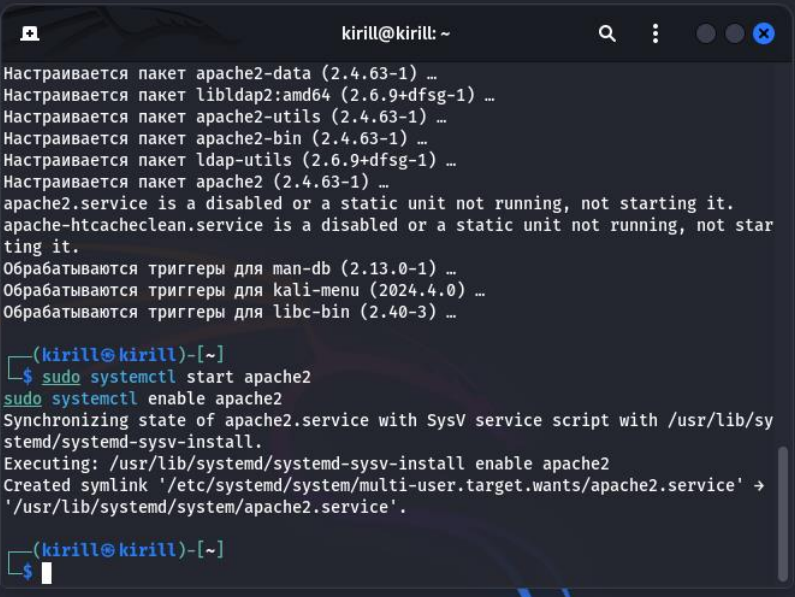
Вариативная часть:



```
(kirill@kirill)-[~]  
$ sudo apt update && sudo apt install apache2 -y  
[sudo] пароль для kirill:  
Пол:1 http://kali.download/kali kali-rolling InRelease [41,5 kB]  
Ошб:1 http://kali.download/kali kali-rolling InRelease  
Следующие подписи не могут быть проверены, так как недоступен открытый ключ: NO_PUBKEY ED65462EC8D5E4C5  
Получено 41,5 kB за 1с (58,8 kB/s)  
Может быть обновлено 1916 пакетов. Запустите «apt list --upgradable» для их пока  
за.  
Warning: Произошла ошибка при проверке подписи. Репозиторий не обновлён, и будут  
использованы предыдущие индексные файлы. Ошибка GPG: http://kali.download/kali  
kali-rolling InRelease: Следующие подписи не могут быть проверены, так как недос  
тупен открытый ключ: NO_PUBKEY ED65462EC8D5E4C5  
Warning: Не удалось получить http://http.kali.org/kali/dists/kali-rolling/InRele  
ase Следующие подписи не могут быть проверены, так как недоступен открытый ключ  
: NO_PUBKEY ED65462EC8D5E4C5  
Warning: Некоторые индексные файлы скачать не удалось. Они были проигнорированы,  
или вместо них были использованы старые версии.  
Upgrading:  
  apache2      apache2-data  ldap-utils  
  apache2-bin  apache2-utils libldap-common  
  
Installing dependencies:
```

KALI

Рисунок 1. Установка Apache



```
Настраивается пакет apache2-data (2.4.63-1) ...  
Настраивается пакет libldap2:amd64 (2.6.9+dfsg-1) ...  
Настраивается пакет apache2-utils (2.4.63-1) ...  
Настраивается пакет apache2-bin (2.4.63-1) ...  
Настраивается пакет ldap-utils (2.6.9+dfsg-1) ...  
Настраивается пакет apache2 (2.4.63-1) ...  
apache2.service is a disabled or a static unit not running, not starting it.  
apache-htcacheclean.service is a disabled or a static unit not running, not star  
ting it.  
Обрабатываются триггеры для man-db (2.13.0-1) ...  
Обрабатываются триггеры для kali-menu (2024.4.0) ...  
Обрабатываются триггеры для libc-bin (2.40-3) ...  
  
(kirill@kirill)-[~]  
$ sudo systemctl start apache2  
sudo systemctl enable apache2  
Synchronizing state of apache2.service with SysV service script with /usr/lib/sy  
stemd/systemd-sysv-install.  
Executing: /usr/lib/systemd/systemd-sysv-install enable apache2  
Created symlink '/etc/systemd/system/multi-user.target.wants/apache2.service' →  
'/usr/lib/systemd/system/apache2.service'.  
  
(kirill@kirill)-[~]  
$
```

KALI

Рисунок 2. Проверка работоспособности

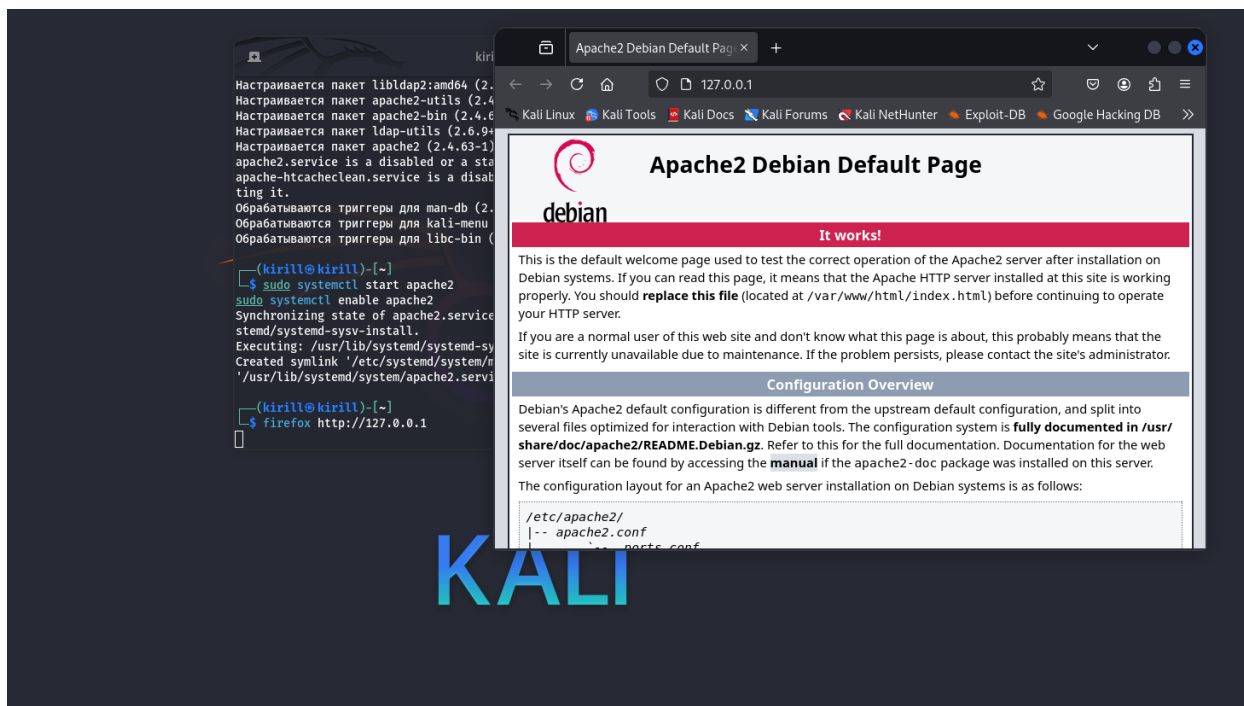


Рисунок 3. Проверяем локальную доступность



Рисунок 4. Настройка логирования, запрос страницы

```
kirill@kirill: ~  
</div>  
  
</div>  
</div>  
<div class="validator">  
</div>  
</body>  
</html>  
  
(kirill@kirill)-[~]  
$ sudo tail -n 5 /var/log/apache2/access.log  
127.0.0.1 - - [14/May/2025:05:53:53 +0300] "GET / HTTP/1.1" 200 3383 "-" "Mozilla/5.0 (X  
11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0"  
127.0.0.1 - - [14/May/2025:05:53:56 +0300] "GET /icons/openlogo-75.png HTTP/1.1" 200 604  
0 "http://127.0.0.1/" "Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/  
128.0"  
127.0.0.1 - - [14/May/2025:05:53:56 +0300] "GET /favicon.ico HTTP/1.1" 404 487 "http://1  
27.0.0.1/" "Mozilla/5.0 (X11; Linux x86 64; rv:128.0) Gecko/20100101 Firefox/128.0"  
127.0.0.1 - - [14/May/2025:05:56:38 +0300] "GET / HTTP/1.1" 200 10958 "-" "curl/8.11.0"  
  
(kirill@kirill)-[~]  
$
```

KALI

Рисунок 5. Анализ логов

```
kirill@kirill: ~  
zsh: suspended less /var/log/apache2/access.log  
(kirill@kirill)-[~]  
$ sudo nano /etc/apache2/apache2.conf  
(kirill@kirill)-[~]  
$ sudo apt install whois net-tools nmap sqlmap hydra slowloris -y  
Уже установлен пакет whois самой новой версии (5.5.23).  
whois помечен как установленный вручную.  
Уже установлен пакет net-tools самой новой версии (2.10-1.1).  
net-tools помечен как установленный вручную.  
Уже установлен пакет hydra самой новой версии (9.5-3).  
hydra помечен как установленный вручную.  
Upgrading:  
ndiff nmap nmap-common sqlmap zenmap  
Installing:  
slowloris  
Summary:  
Upgrading: 5, Installing: 1, Removing: 0, Not Upgrading: 1905  
Download size: 14,2 MB  
Space needed: 544 kB / 1 146 MB available  
Пол:2 http://http.kali.org/kali kali-rolling/non-free amd64 ndiff all 7.95+dfsg-1kali1 [
```

KALI

Рисунок 6. Установка инструментов для тестирования

Brute-force атака

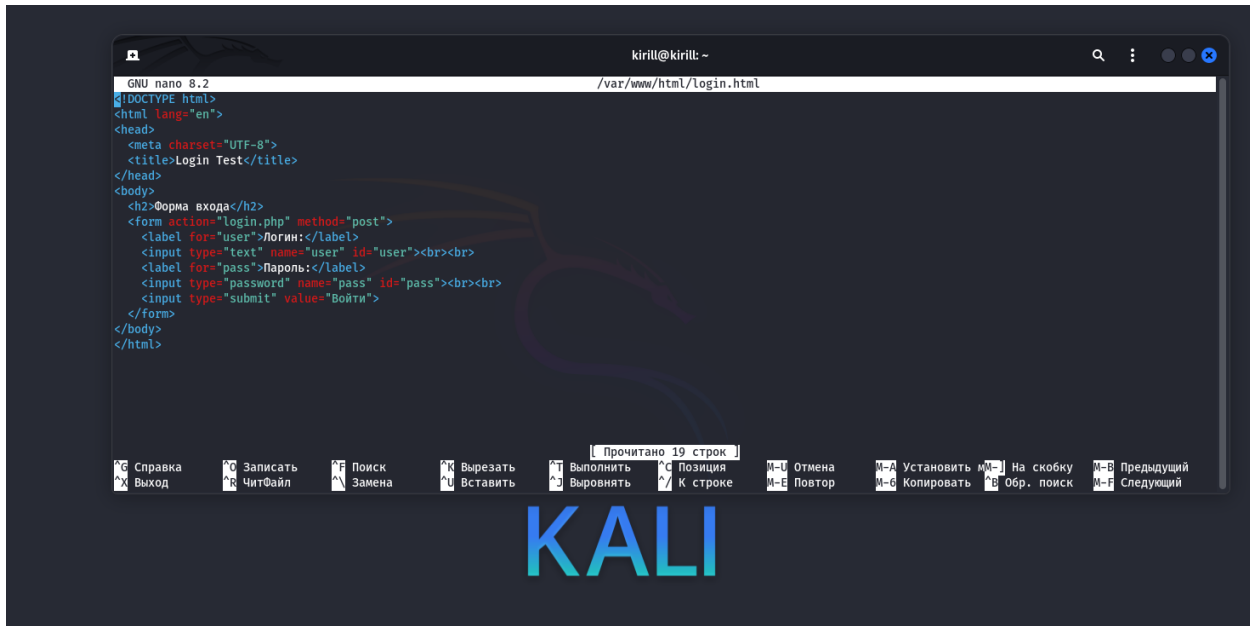


Рисунок 7. Создаём простую форму входа на сайт

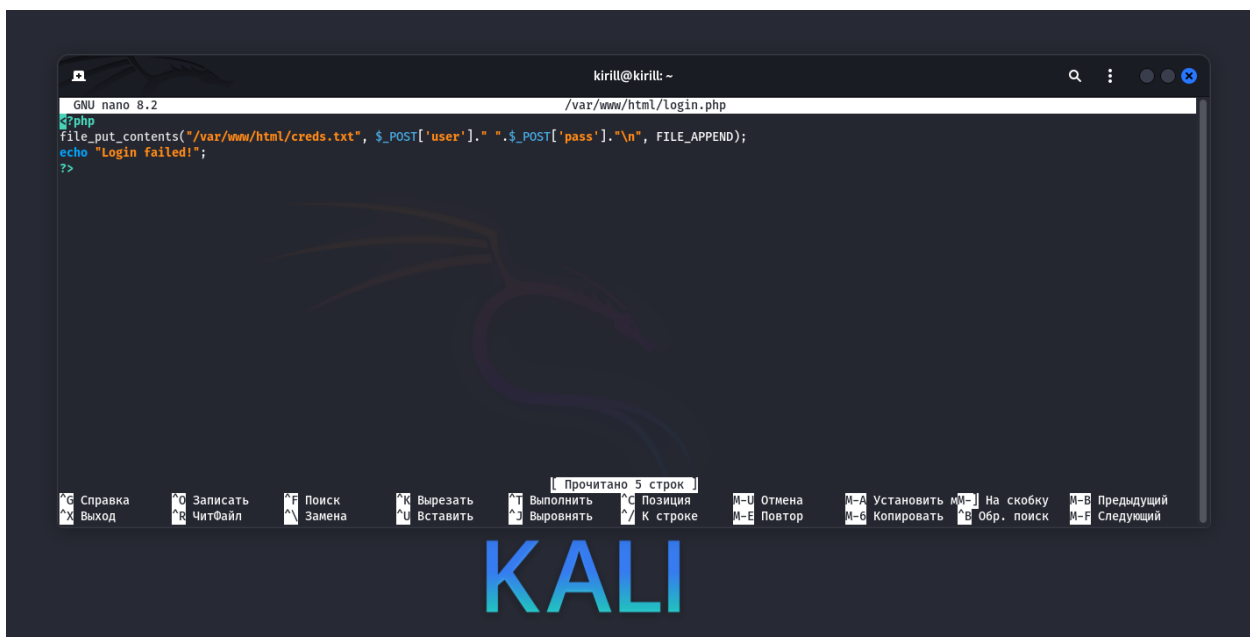


Рисунок 8. Создаём простую форму входа на сайт

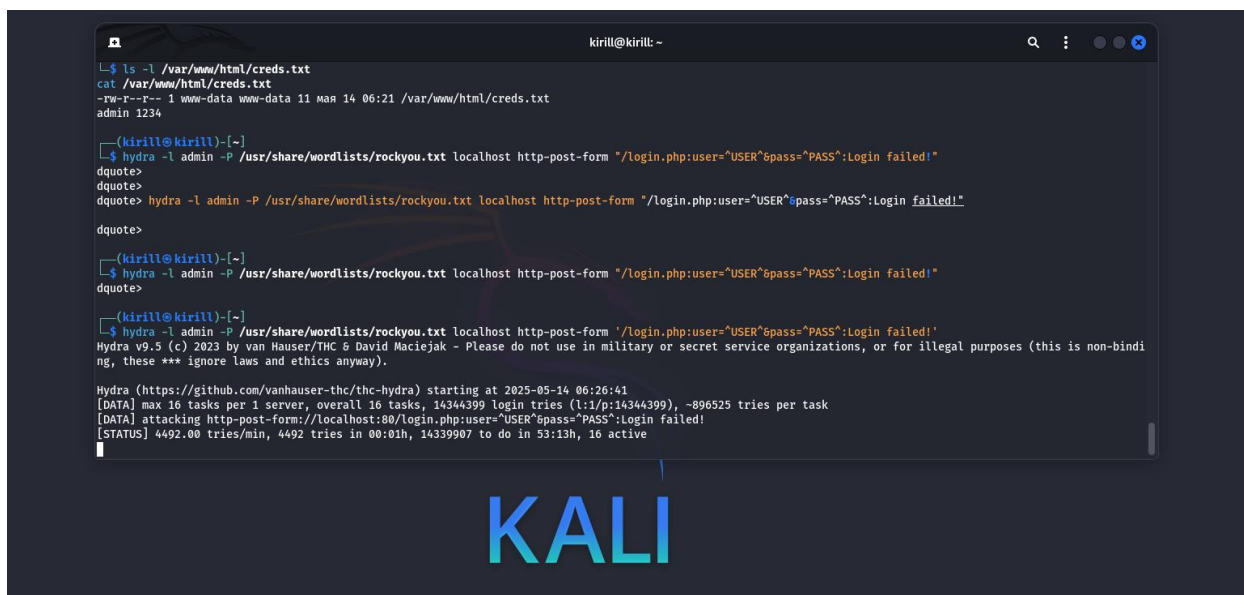


Рисунок 9. Запуск атаки

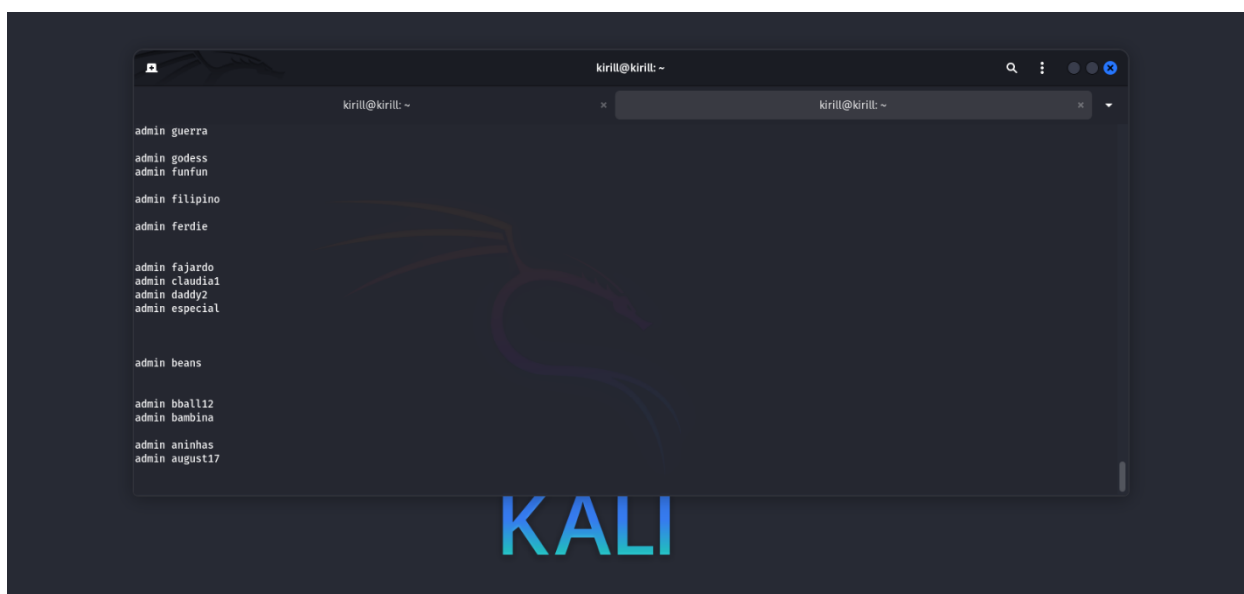


Рисунок 10. Как выглядит работа

SQL-инъекция

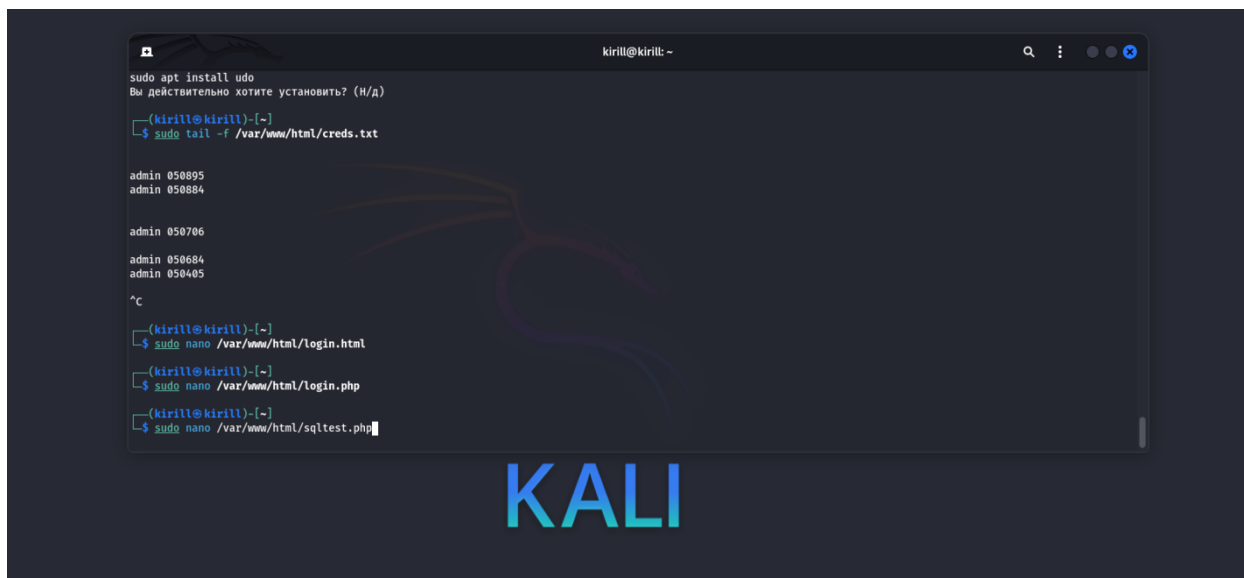


Рисунок 11. Создаём уязвимый скрипт

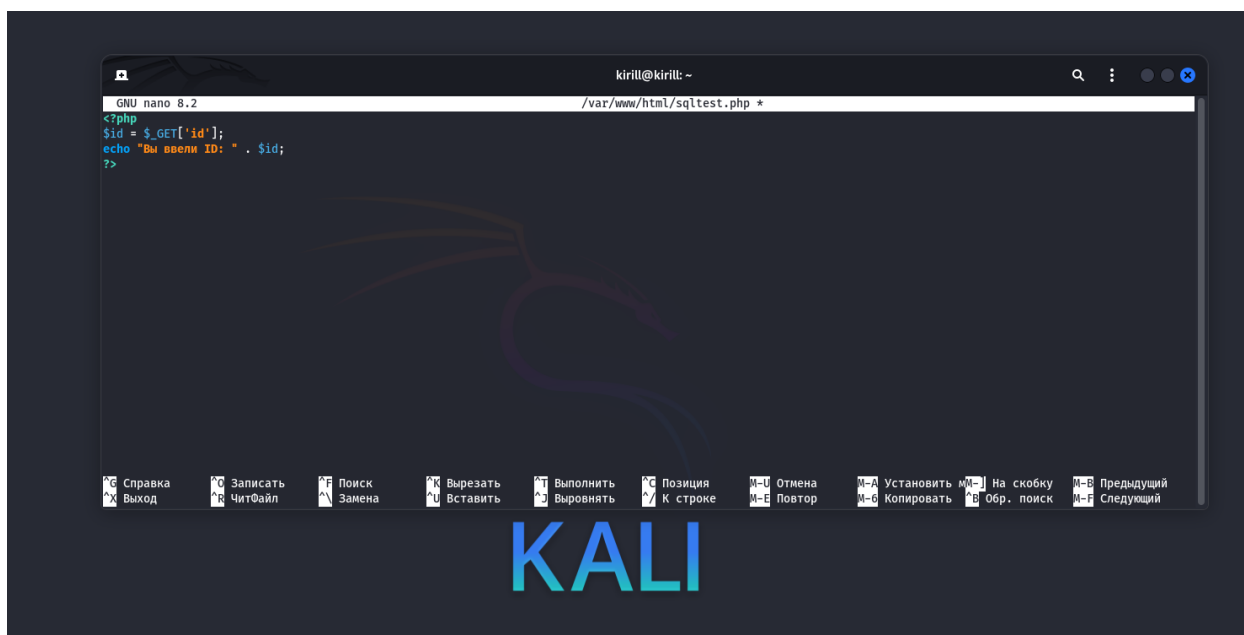


Рисунок 12. Пишем уязвимый скрипт

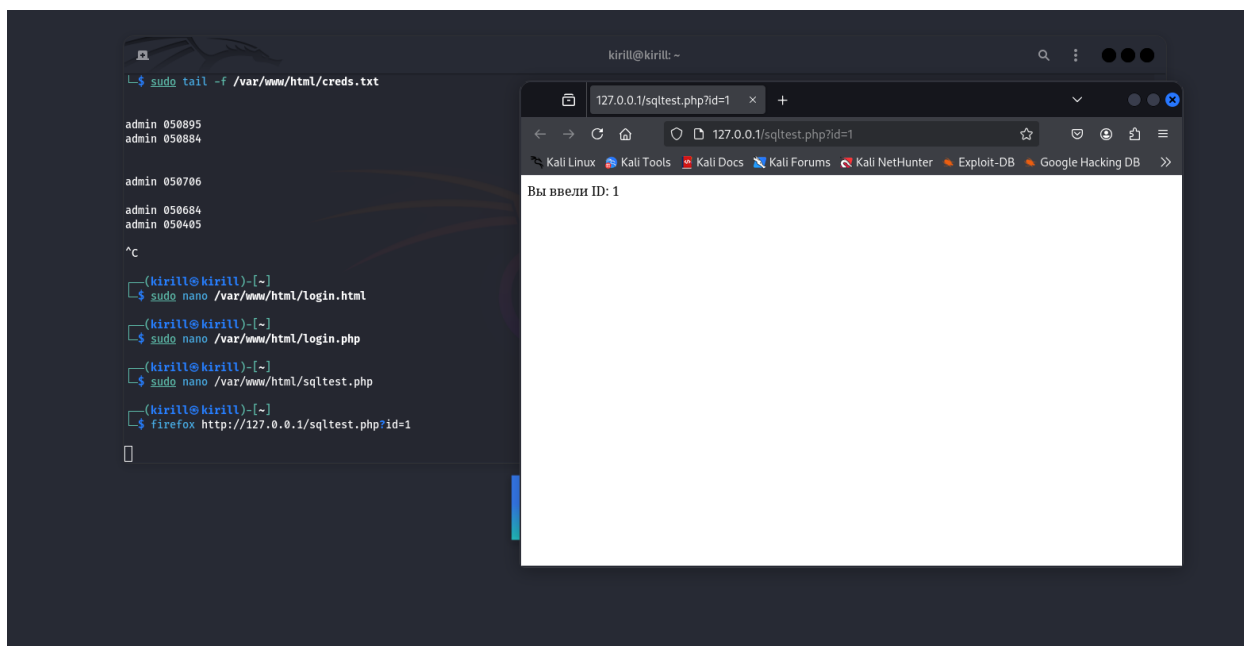


Рисунок 13. Пример работы уязвимого скрипта

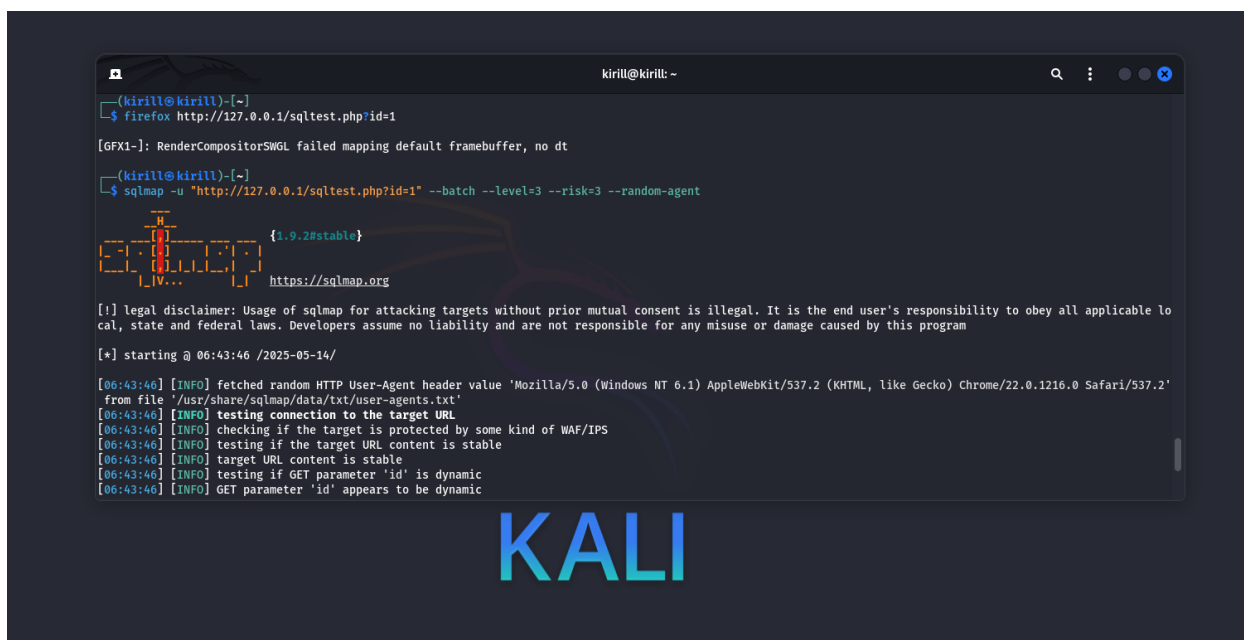


Рисунок 14. Эмулируем атаку

`--batch` — не задавать вопросы

`--level=3 --risk=3` — расширенный анализ

`--random-agent` — имитирует разные браузеры

SQLmap начнёт проверку уязвимостей. Даже если реальной БД нет — он всё равно будет писать в лог **попытки SQL-инъекции** (через URL-параметры)

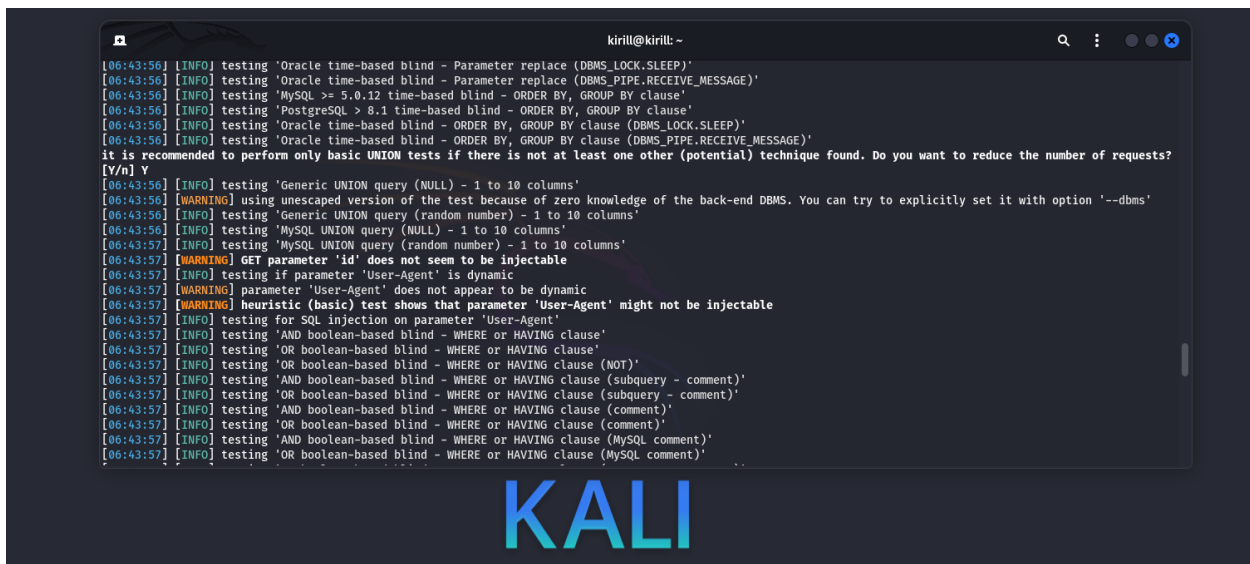


Рисунок 15. Вид как работает атака

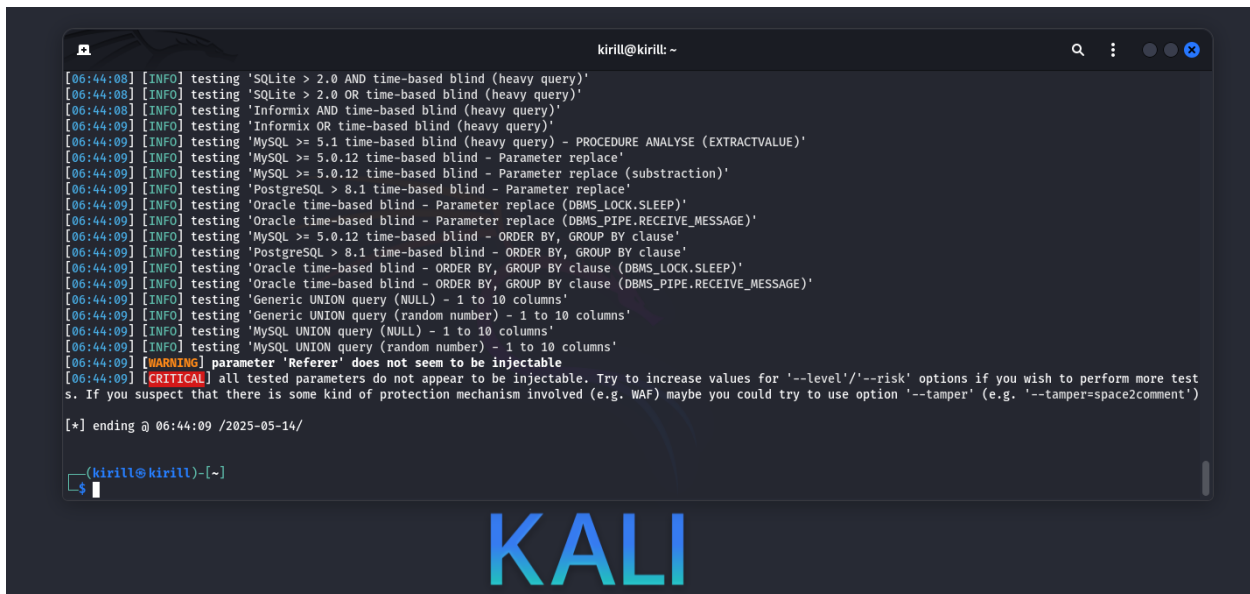


Рисунок 16. Конечный результат

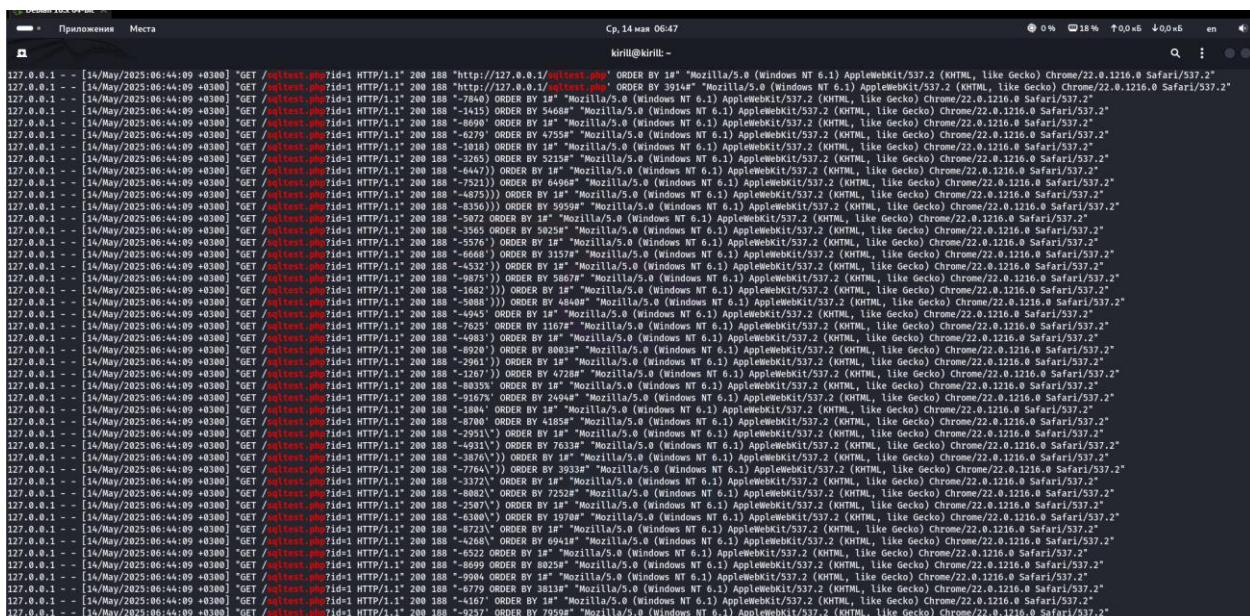


Рисунок 17. Вид Логов

DoS-Атака

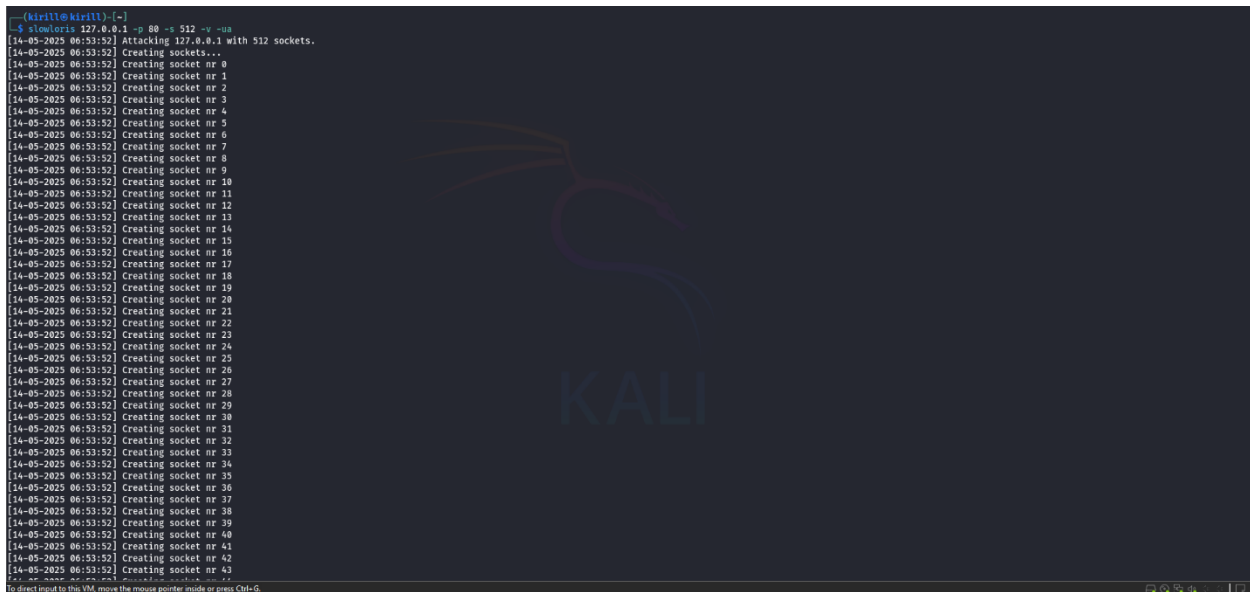


Рисунок 18. Запускаем атаку

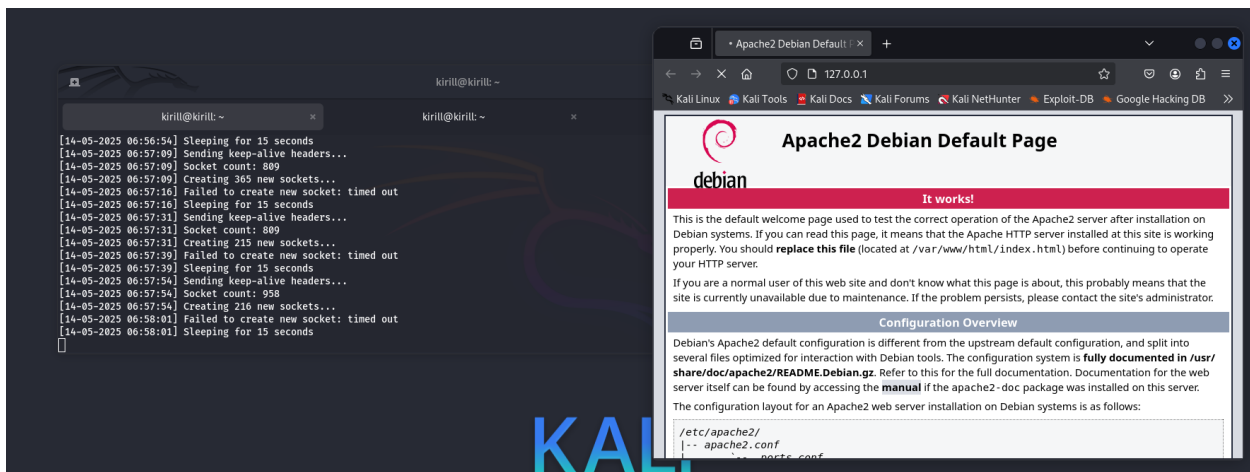


Рисунок 19. Страница бесконечно пытается обновиться, значит атака работает

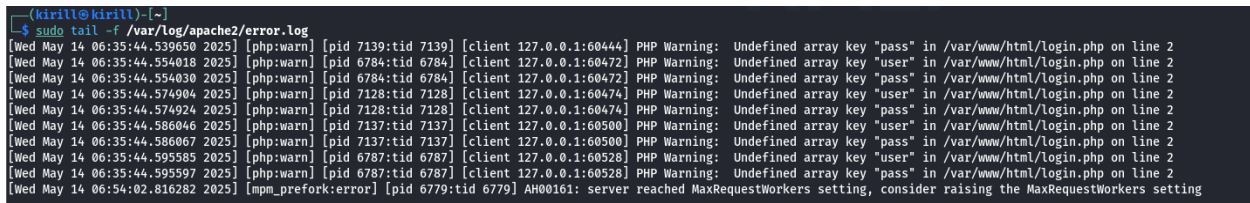


Рисунок 20. Логи

Заключение

В ходе проектной практики были достигнуты следующие результаты:

Настройка GitHub репозитория

Изучение HTML

Установлен и настроен веб-сервер Apache в изолированной среде (локальный сегмент 127.0.0.1);

Включено ведение логов доступа и ошибок (access.log и error.log);

Проведены три успешные имитации атак:

Brute-force с использованием утилиты hydra;

SQL-инъекция через sqlmap с реальной базой данных SQLite;

DoS-атака (Slowloris) с перегрузкой Apache;

Таким образом, поставленная цель — была успешно достигнута, задачи выполнены в полном объёме, результаты задокументированы и подтверждены логами и практическими тестами и коммитами на GitHub. Общее затраченное время: 76 часов

Список литературы:

1. [HTML основы](#)
2. [Настройка GitHub репозитория](#)
3. [Настройка веб-сервера](#)

Приложения:

[GitHub команды](#)