

Федеральное государственное автономное образовательное учреждение высшего
образования

«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

Факультет информационных технологий
Кафедра «Информационная безопасность»

Направление подготовки/ специальность: Безопасность компьютерных систем

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: Кесель Сергей Александрович

Москва 2025

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ	
Общая информация о проекте	
Название проекта	
Цели и задачи проекта.....	
Описание задания по проектной практике	
Описание достигнутых результатов по проектной практике	
ЗАКЛЮЧЕНИЕ	
ПРИЛОЖЕНИЯ	

ЗАДАНИЕ ПО ПРОЕКТНОЙ ПРАКТИКЕ

Задание на проектную практику разделялось на базовую и вариативную части. Трудоёмкость практики составляла 72 академических часа. Задание выполнялось в составе группы из 2 человек (Ильин К.А(241-353), Кондраков В.И(241-371)). Для управления версиями использовался Git, для написания документации — Markdown, а для создания статического веб-сайта — языки разметки HTML и CSS. В качестве платформы для размещения репозитория использовался [GitHub](#). Задание состоит из двух частей. Первая часть является общей и обязательной для всех студентов. Вторая часть вариативная. Задание на вторую (вариативную) часть было получено от ответственного за проектную практику на выпускающей кафедре.

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 по развёртыванию веб-сервера, организации логирования, реализации тестовых атак. Все действия проводились в рамках изолированной среды и сопровождалась регистрацией действий для последующего документирования.

Кроме того, я являлся тимлидом нашей команды и проверял все файлы сокомандника. (Изучение требований работы заняло 3 часа, редакция текста на сайте заняла 4 часа, создание GitHub-репозитория, проверка его наполнения - 9 часов, посещение всех организационных онлайн-собраний - 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:
```

Рисунок 1. Установка Apache

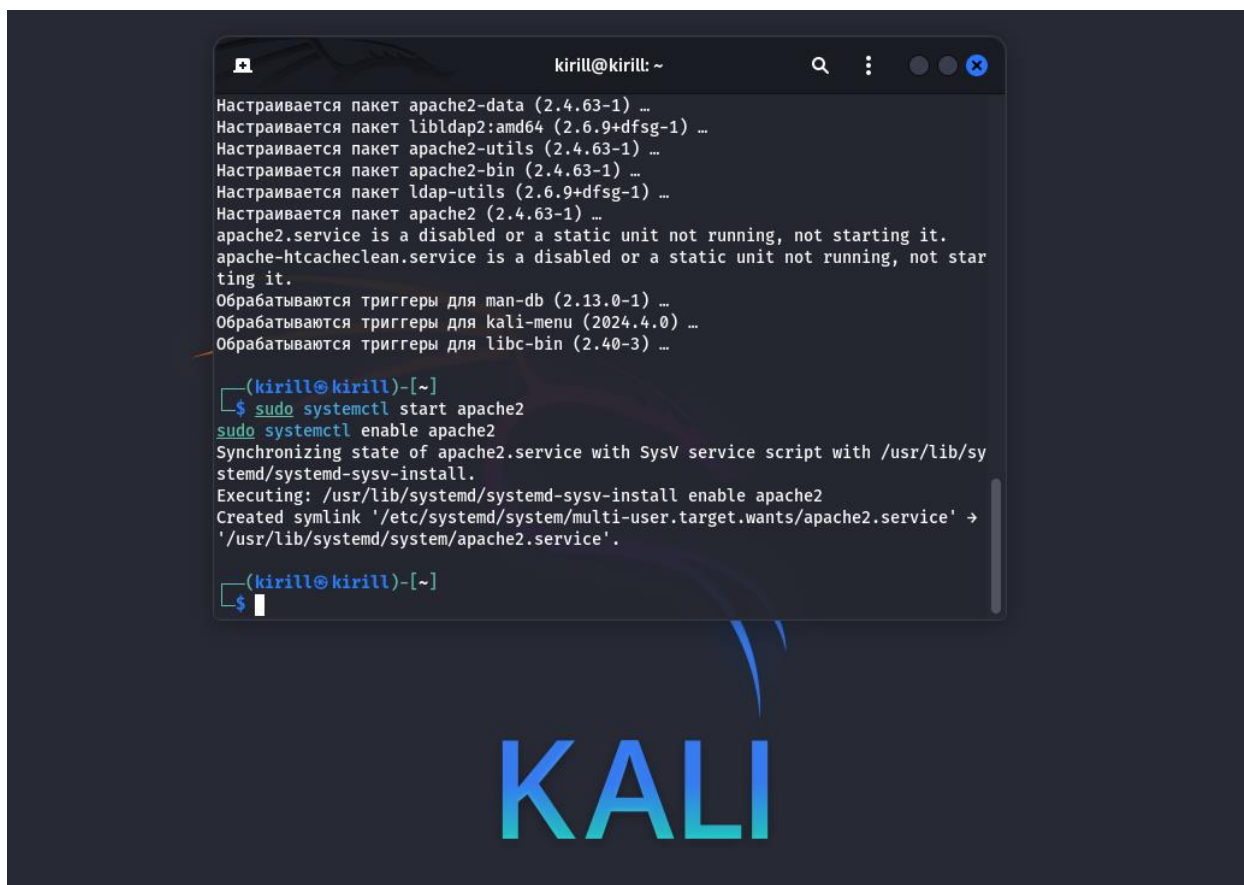


Рисунок 2. Проверка работоспособности

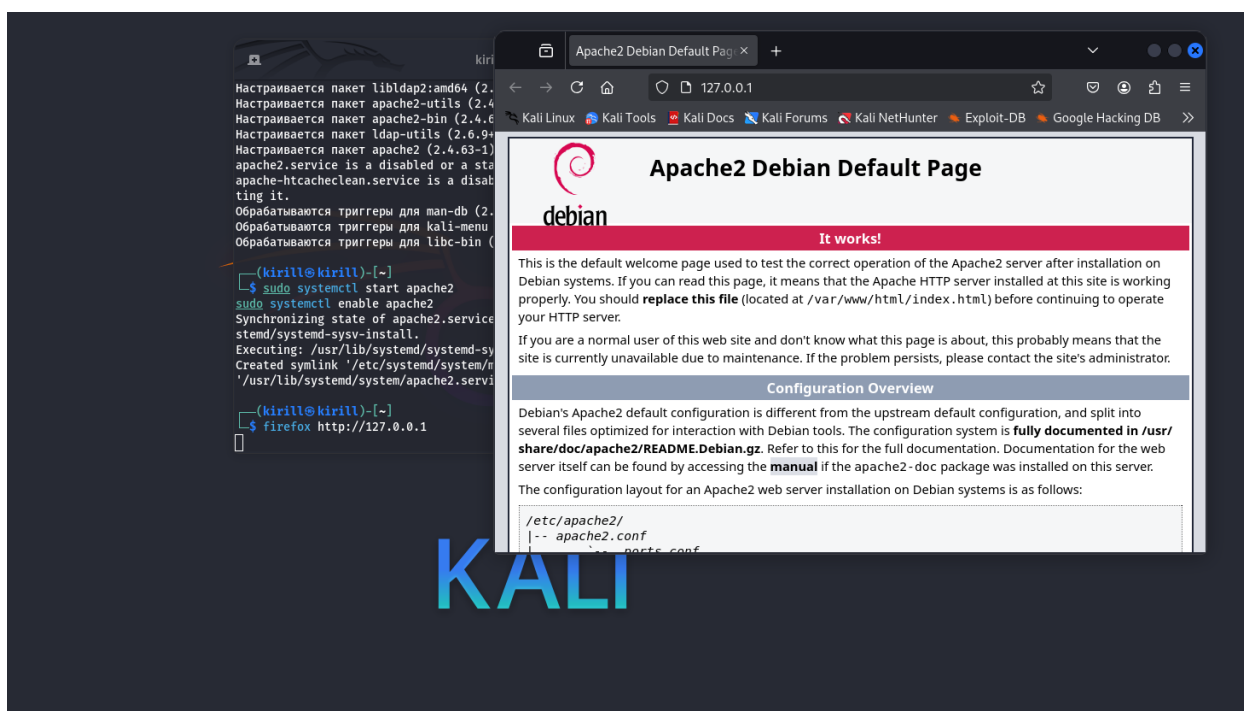
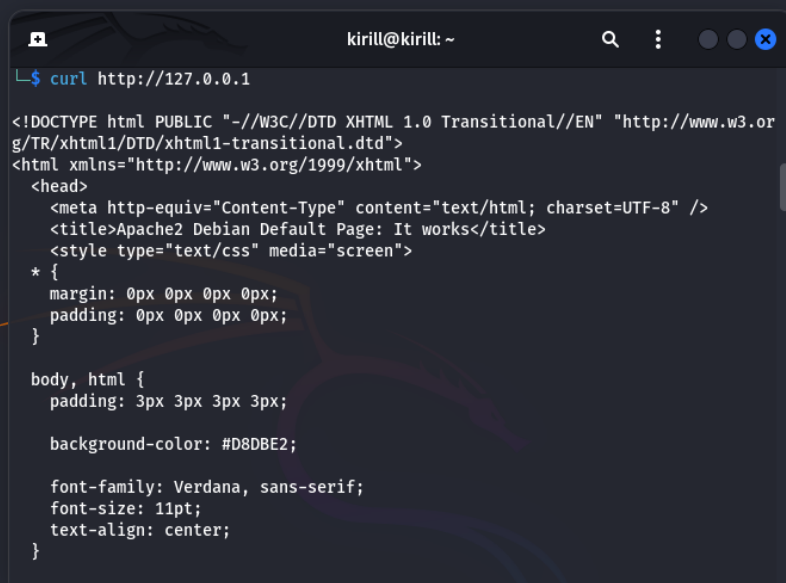


Рисунок 3. Проверяем локальную доступность



```
kirill@kirill: ~  
$ curl http://127.0.0.1  
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">  
<html xmlns="http://www.w3.org/1999/xhtml">  
  <head>  
    <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />  
    <title>Apache2 Debian Default Page: It works</title>  
    <style type="text/css" media="screen">  
      * {  
        margin: 0px 0px 0px 0px;  
        padding: 0px 0px 0px 0px;  
      }  
  
      body, html {  
        padding: 3px 3px 3px 3px;  
  
        background-color: #D8DBE2;  
  
        font-family: Verdana, sans-serif;  
        font-size: 11pt;  
        text-align: center;  
      }  
    </style>  
  </head>  
</html>
```

KALI

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

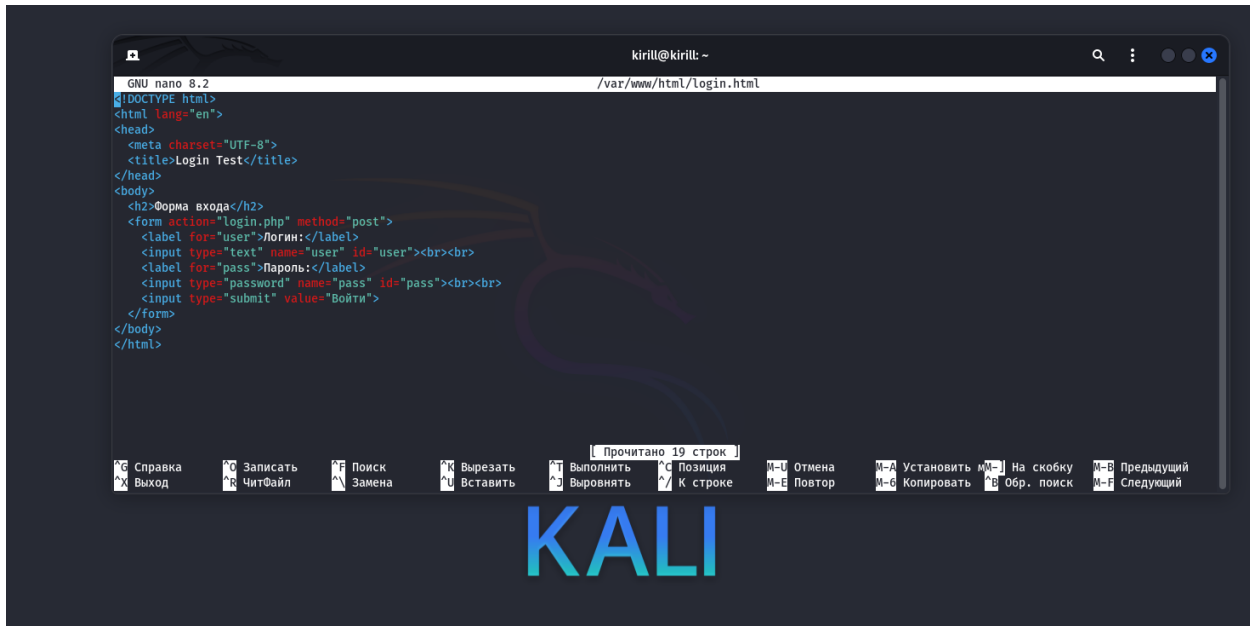


Рисунок 7. Создаём простую форму входа на сайт

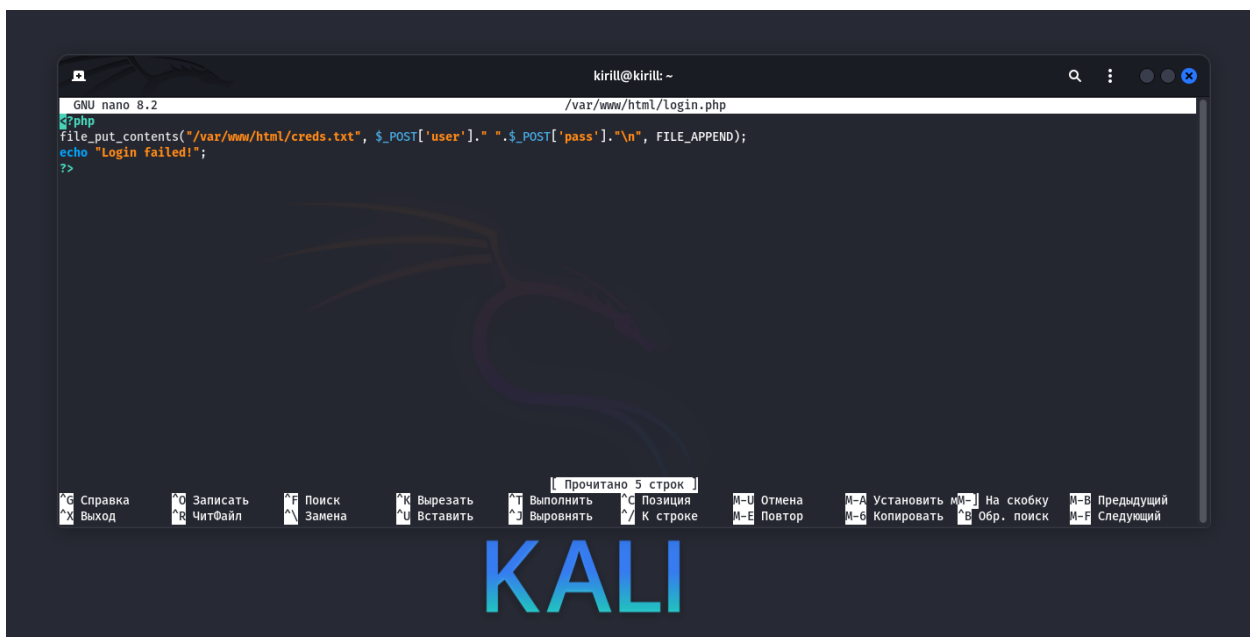


Рисунок 8. Создаём простую форму входа на сайт

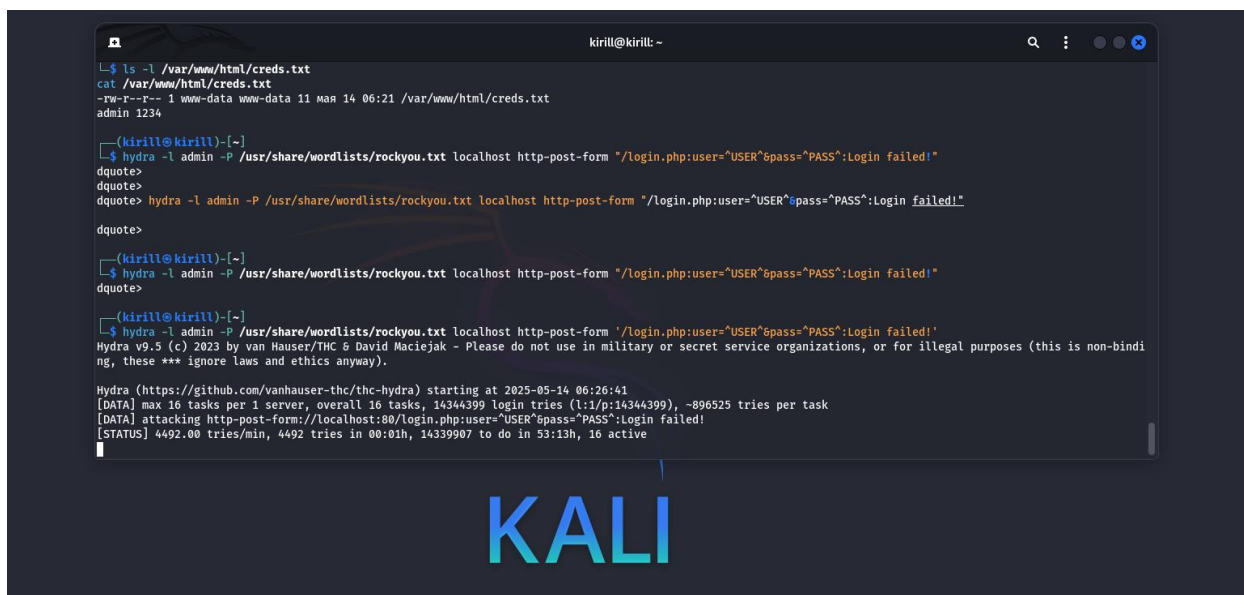


Рисунок 9. Запуск атаки

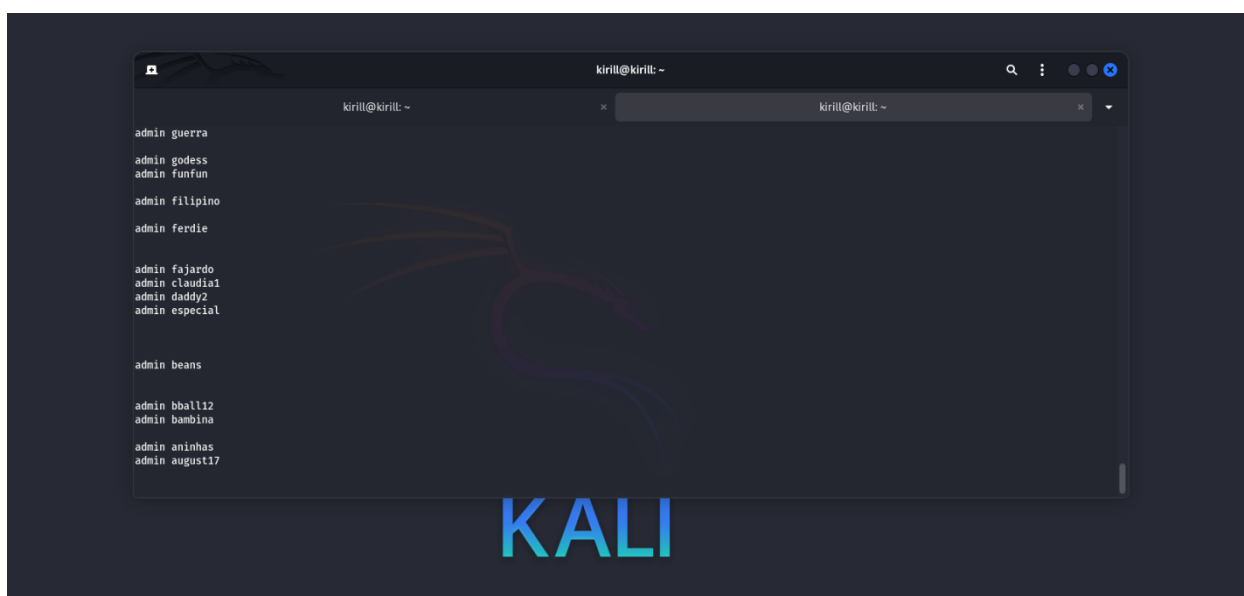


Рисунок 10

SQL-инъекция

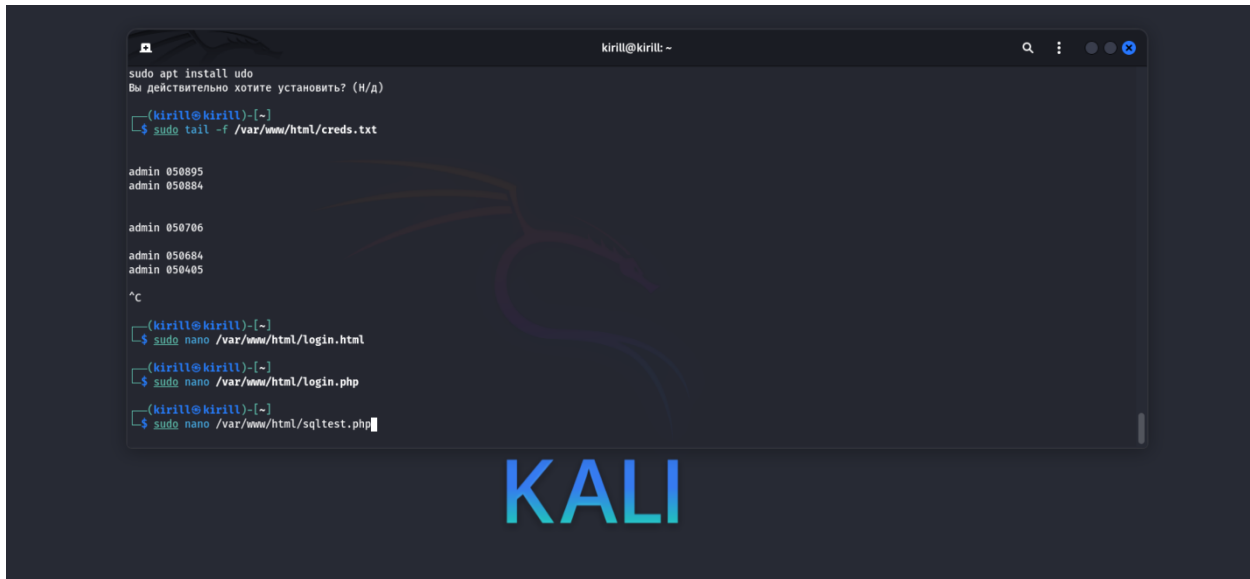


Рисунок 11. Создаём уязвимый скрипт

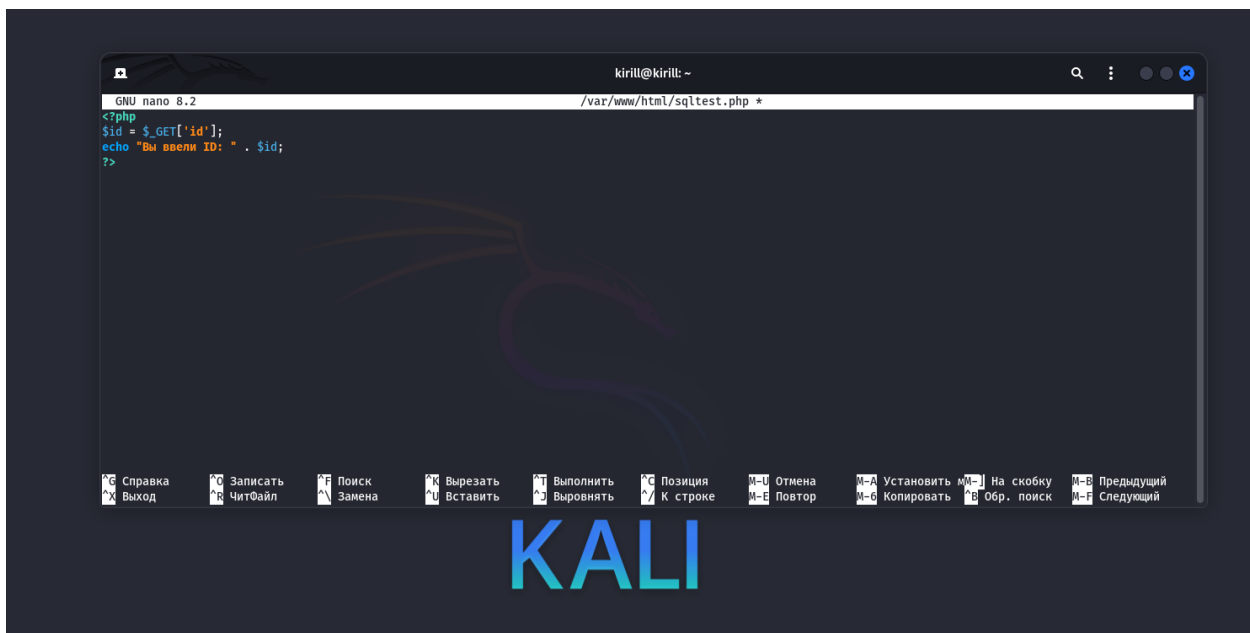


Рисунок 12. Создаём уязвимый скрипт

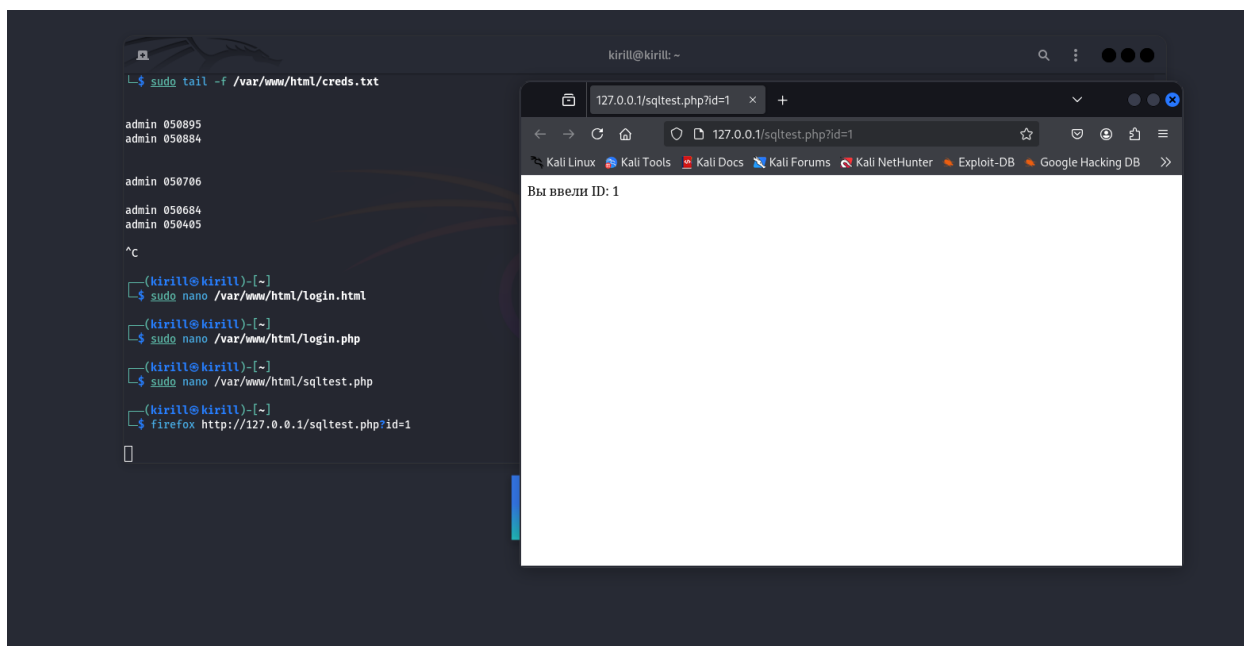


Рисунок 13. Создаём уязвимый скрипт

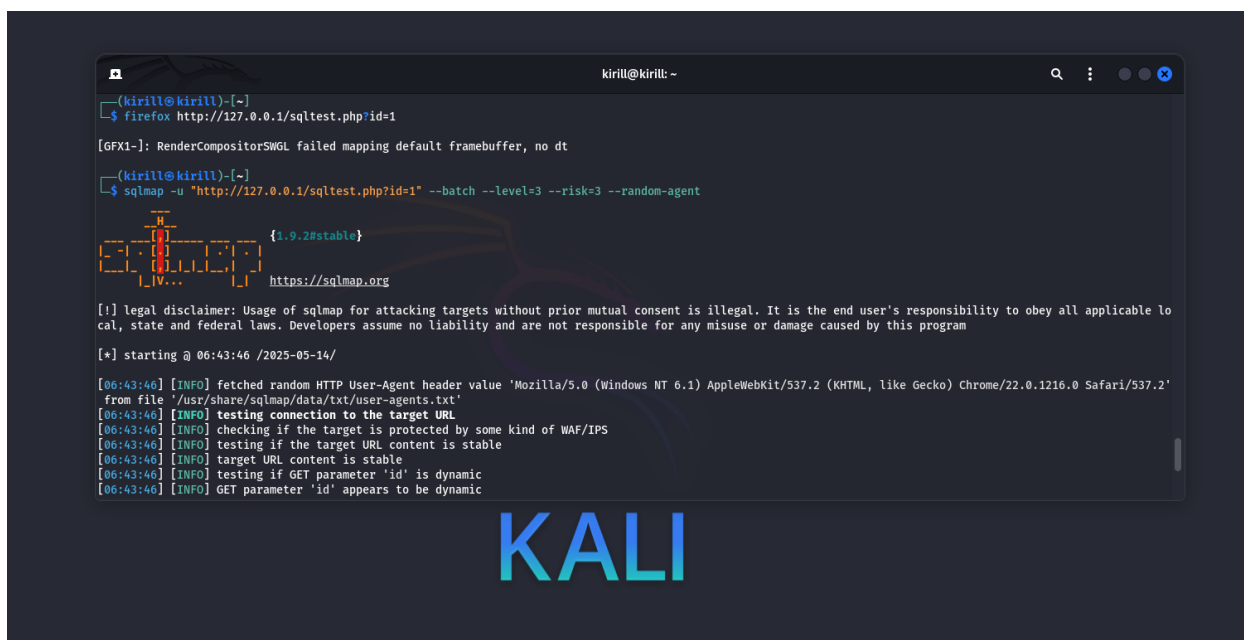


Рисунок 14. Эмулируем атаку

--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 17

DoS-Атака

[illegible]

Рисунок 18. Запускаем атаку

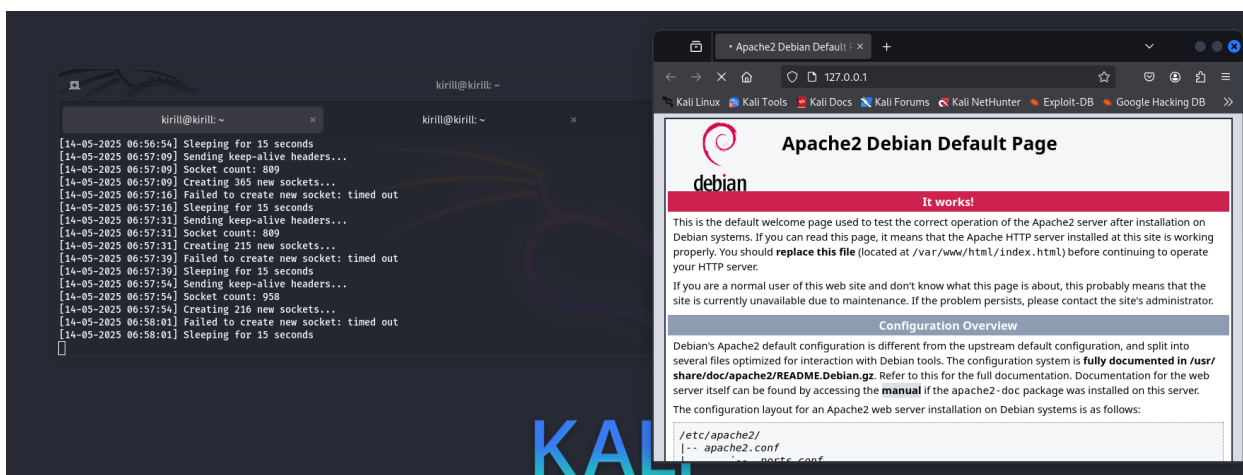


Рисунок 19. Страница бесконечно пытается обновиться, значит атака работает

```

$ sudo tail -f /var/log/apache2/error_log
[Wed May 14 06:35:44.539650 2025] [php:warn] [pid 7139:tid 7139] [client 127.0.0.1:60444] PHP Warning: Undefined array key "pass" in /var/www/html/login.php on line 2
[Wed May 14 06:35:44.554018 2025] [php:warn] [pid 6784:tid 6784] [client 127.0.0.1:60472] PHP Warning: Undefined array key "user" in /var/www/html/login.php on line 2
[Wed May 14 06:35:44.554030 2025] [php:warn] [pid 6784:tid 6784] [client 127.0.0.1:60472] PHP Warning: Undefined array key "pass" in /var/www/html/login.php on line 2
[Wed May 14 06:35:44.574904 2025] [php:warn] [pid 7128:tid 7128] [client 127.0.0.1:60474] PHP Warning: Undefined array key "user" in /var/www/html/login.php on line 2
[Wed May 14 06:35:44.574924 2025] [php:warn] [pid 7128:tid 7128] [client 127.0.0.1:60474] PHP Warning: Undefined array key "pass" in /var/www/html/login.php on line 2
[Wed May 14 06:35:44.586046 2025] [php:warn] [pid 7137:tid 7137] [client 127.0.0.1:60500] PHP Warning: Undefined array key "user" in /var/www/html/login.php on line 2
[Wed May 14 06:35:44.586067 2025] [php:warn] [pid 7137:tid 7137] [client 127.0.0.1:60500] PHP Warning: Undefined array key "pass" in /var/www/html/login.php on line 2
[Wed May 14 06:35:44.595585 2025] [php:warn] [pid 6787:tid 6787] [client 127.0.0.1:60528] PHP Warning: Undefined array key "user" in /var/www/html/login.php on line 2
[Wed May 14 06:35:44.595597 2025] [php:warn] [pid 6787:tid 6787] [client 127.0.0.1:60528] PHP Warning: Undefined array key "pass" in /var/www/html/login.php on line 2
[Wed May 14 06:54:02.618282 2025] [mpm_prefork:error] [pid 6779:tid 6779] AH00161: server reached MaxRequestWorkers setting, consider raising the MaxRequestWorkers setting

```

Рисунок 20. Логги

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

Приложения:

[GitHub команды](#)