Федеральное государственное автономное образовательное учреждение высшего образования

«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

Факультет информационных технологий  
Кафедра «Информационная безопасность»

Направление подготовки/ специальность: 10.05.03 Информационная безопасность автоматизированных систем

ОТЧЕТ

по проектной практике

Студент: Кондраков Валерий Игоревич Группа: 241-371

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

Отчет принят с оценкой \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Дата \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Руководитель практики: Гневшев Александр Юрьевич

Москва 2025

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ**3**

Общая информация о проекте3

Название проекта3

Цели и задачи проекта3

Описание задания по проектной практике4

Описание достигнутых результатов по проектной практике7

ЗАКЛЮЧЕНИЕ 11

СПИСОК ЛИТЕРАТУРЫ 12

ПРИЛОЖЕНИЯ 12

Общая информация о проекте

Название проекта: INVADE

Цели и задачи проекта:

**Цель проекта:** Создание сюжетного игрового проекта, сочетающего элементы 3D-платформера, метроидвании, стелс-хоррора с менеджментом ресурсов и RPG. Игра предлагает уникальный игровой опыт в научно-фантастической/хоррор эстетике, привлекает новую аудиторию в отечественный инди-сектор и способствует развитию научной фантастики.

**Задачи проекта:**

1. Провести исследование целевой аудитории и её предпочтений в жанрах, представленных в игре.
2. Изучить современные игровые тренды и успешные проекты с похожими механиками.
3. Разработать концепцию игры, включая сюжет, сеттинг и геймплейные механики.
4. Определить ключевые технические требования и инструменты разработки.
5. Создать ранний прототип (демоверсию) с основными игровыми механиками.
6. Разработать художественное оформление (модели, анимации, дизайн уровней).
7. Реализовать систему сохранений, уровни сложности и взаимодействие с NPC.
8. Провести тестирование на различных этапах разработки, анализируя отзывы игроков.
9. Оптимизировать производительность игры и исправить выявленные ошибки.
10. Подготовить маркетинговую стратегию и каналы распространения игры.

Описание задания 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 репозиториев использовался [GitHub](https://github.com/).

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](https://github.com/)  на основе предоставленного [шаблона](https://github.com/mospol/practice-2025-1).
* Освоить базовые команды Git: клонирование, коммит, пуш и создание веток.
* Регулярно фиксировать изменения с осмысленными сообщениями к коммитам.
* Примерное время: 5 часов.

1. 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.

1. 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****

* **Изучены и применены технологии CSS** для стилизации веб-сайта проекта INVADE, включая адаптивный дизайн, анимации элементов интерфейса и создание единой визуальной концепции;
* **Наполнение сайта контентом** выполнено с учётом требований проекта:
  + Разработаны уникальные страницы (главная, "О проекте", "Участники", "Журнал", "Ресурсы");
  + Добавлены графические материалы: скриншоты игрового процесса, концепт-арты, диаграммы (SWOT, карта пути пользователя);
  + Реализована навигация между разделами с помощью CSS-стилей для кнопок и меню;
* **Проведён анализ логов веб-сервера (**Nginx) с выявлением подозрительной активности:
  + Отфильтрованы запросы, содержащие признаки **SQL**
  + Обнаружены попытки **Brute-force атак** на админ-панель
  + Зафиксированы **подозрительные User-Agent**
* **Составлены карточки инцидентов информационной безопасности** по шаблону, включающему:
  + **Тип инцидента** (например, "Попытка SQL-инъекции");
  + **Время и дата** события;
  + **IP-источник** атаки;
  + **Уровень критичности** (низкий/средний/высокий);
  + **Принятые меры (**блокировка IP через fail2ban, обновление правил WAF).

В результате работы получен практический опыт по вёрстке и дизайну веб-сайтов, анализу угроз на основе логов веб-сервера и документированию инцидентов. Все тестовые атаки проводились в изолированной среде с последующей очисткой логов.

Изображение выглядит как снимок экрана, текст, программное обеспечение, Мультимедийное программное обеспечение

Контент, сгенерированный ИИ, может содержать ошибки.

*Рисунок 1. Как выглядит работа*

Изображение выглядит как снимок экрана, текст

Контент, сгенерированный ИИ, может содержать ошибки.

*Рисунок 2. Вид Логов*

Изображение выглядит как текст, снимок экрана, Шрифт, информация

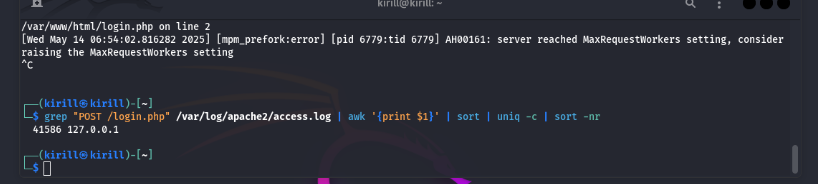
Контент, сгенерированный ИИ, может содержать ошибки.

*Рисунок 3. Логи*

Фильтрация атак

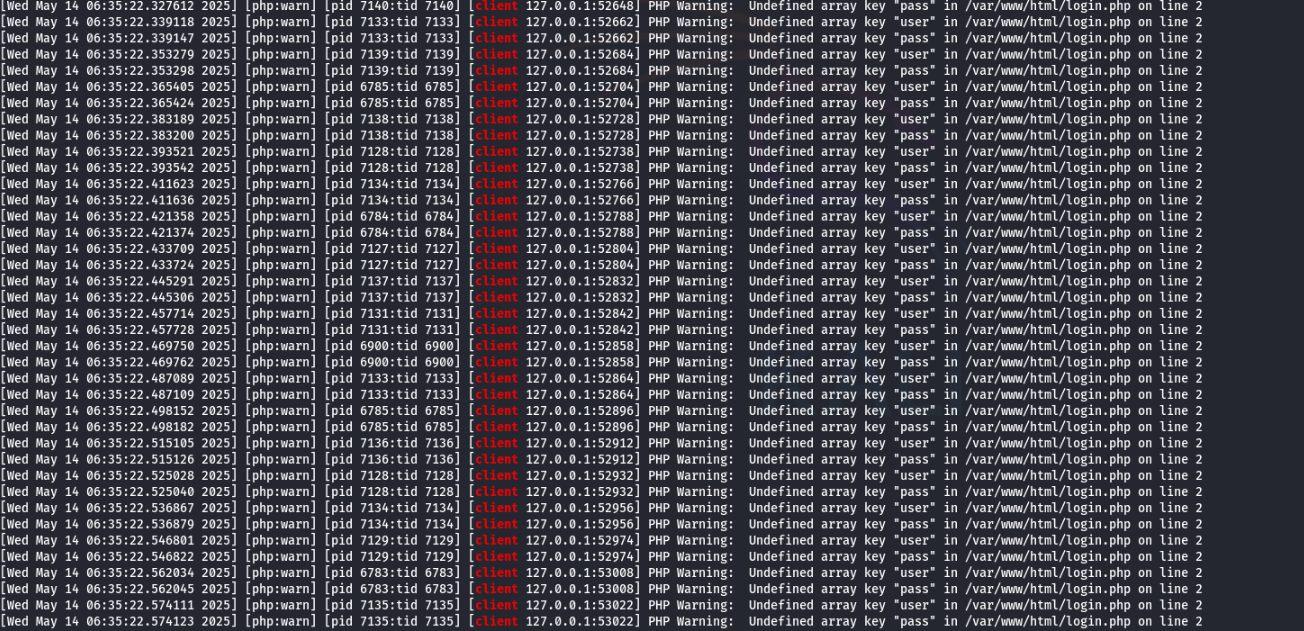
Brute-force атаки (на login.php):

grep "POST /login.php" /var/log/apache2/access.log | awk '{print $1}' | sort | uniq -c | sort –nr



SQL-инъекции (через sqltest.php)

grep "sqltest.php" /var/log/apache2/access.log | grep -Ei "union|select|or|and|order|--|%27|%22"

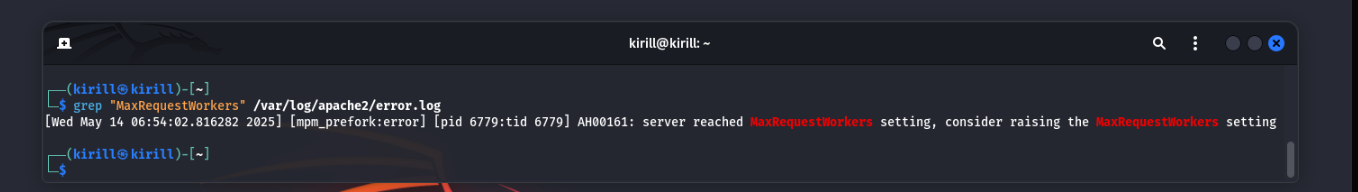


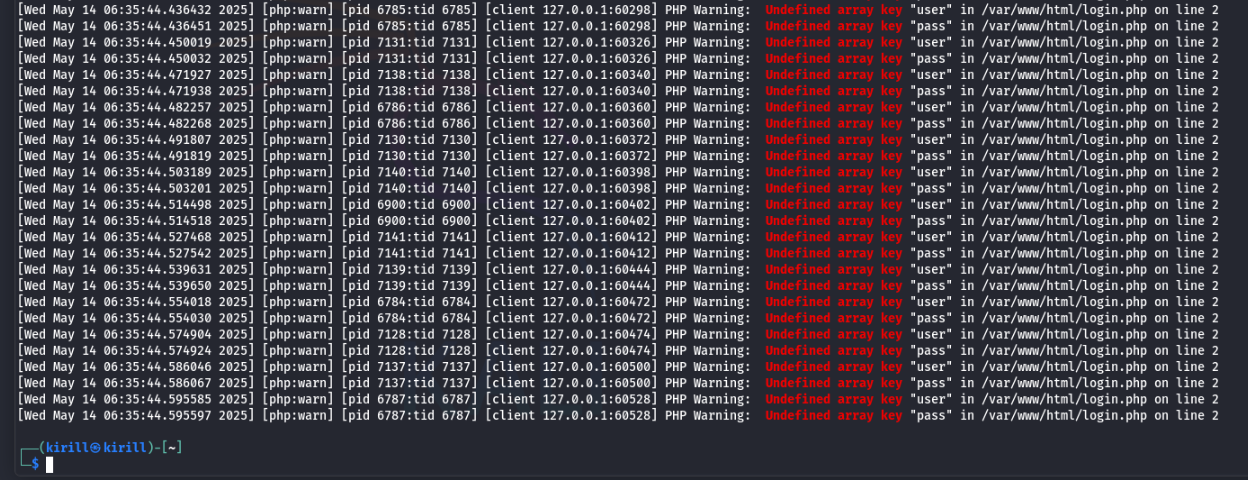
DoS-атаки (Slowloris)

grep "MaxRequestWorkers" /var/log/apache2/error.log

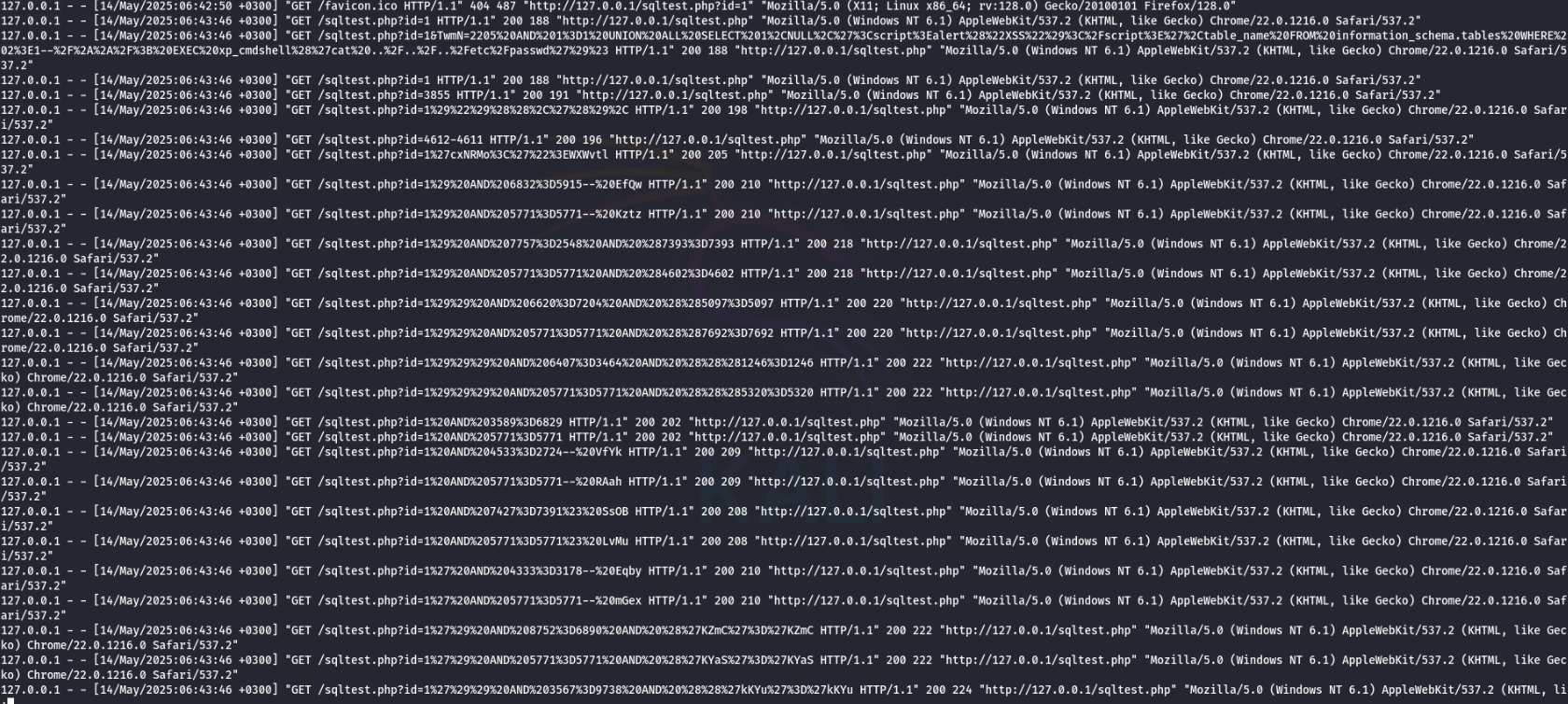
и

grep "Undefined array key" /var/log/apache2/error.log





Общая фильтрация всех GET с подозрительными параметрами



Заключение

В ходе проектной практики были успешно выполнены все поставленные задачи, что позволило не только закрепить теоретические знания, но и получить ценный практический опыт в области веб-разработки, информационной безопасности и управления проектами.

**Ключевые достижения:**

1. **Веб-разработка:**
   * Создан статический веб-сайт проекта INVADE, включающий все необходимые разделы: главную страницу, описание проекта, информацию об участниках, журнал прогресса и ресурсы.
   * Реализован адаптивный дизайн, обеспечивающий корректное отображение сайта на различных устройствах.
   * Применены современные технологии CSS, для создания удобного и визуально привлекательного интерфейса.
2. **Работа с системами контроля версий:**
   * Освоены базовые и продвинутые команды Git, включая работу с ветками, разрешение конфликтов и совместную разработку в групповом репозитории на GitHub.
   * Все изменения фиксировались с осмысленными комментариями, что упростило отслеживание прогресса и взаимодействие между участниками команды.
3. **Информационная безопасность:**
   * Проведён анализ логов для выявления потенциальных угроз, таких как SQL-инъекции, Brute-force и DoS-атаки.
   * Разработан шаблон карточки инцидента, который может быть использован для оперативного реагирования на угрозы в будущем.
4. **Командная работа:**
   * Эффективное распределение задач между участниками проекта позволило достичь высоких результатов в сжатые сроки.
   * Регулярное обсуждение прогресса и возникающих сложностей способствовало оперативному решению проблем.

**СПИСОК ЛИТЕРАТУРЫ**

* [Технологии CSS](https://practicum.yandex.ru/blog/chto-takoe-css/)
* [Логи](https://sky.pro/wiki/javascript/osnovnye-metody-zashity-ot-ddos-atak/)

**ПРИЛОЖЕНИЯ**

* [Github команды](https://github.com/swelock/PRACTIC_1_KURS/tree/main)