Федеральное государственное автономное образовательное учреждение высшего образования

«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

Факультет Информационных технологий  
Кафедра «Информационная безопасность»

Направление подготовки/ специальность: Информационная безопасность 10.03.01

ОТЧЕТ

по проектной практике

Студент: Тимошкин Роман Витальевич Группа: 241-352

Место прохождения практики: Московский Политех, кафедра информационной безопасности.

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

Руководитель практики: Кесель С. А.

Москва 2025

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ**3**

Общая информация о проекте3

Название проекта3

Цели и задачи проекта3

Описание задания по проектной практике5

Описание достигнутых результатов по проектной практике5

ЗАКЛЮЧЕНИЕ 7

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ8

ВВЕДЕНИЕ

Веб-приложения активно взаимодействуют с базами данных для хранения и обработки критически важной информации: учетных записей пользователей, платежных данных, контента и других структур. Однако неправильная обработка пользовательского ввода и недостаточная защита механизмов взаимодействия с БД могут привести к серьезным уязвимостям, эксплуатируемым злоумышленниками.

В данном проекте исследуются ключевые уязвимости, связанные с атаками на базы данных через веб-приложения: **SQL-инъекции (SQLi)**, **командные инъекции (Command Injection)**, **SSRF (Server-Side Request Forgery)** и **XXE (XML External Entity)**. Каждая из этих уязвимостей представляет высокий риск, так как может привести к утечке данных, несанкционированному доступу и даже полной компрометации инфраструктуры.

1. Общая информация о проекте:

**Название:** Киберполигон.

**Цели проекта**:

* Уменьшить финансовые и временные затраты на

организацию и проведение киберучений за счет использования

виртуальной среды.

* Создать платформу, которая позволит моделировать

различные сценарии кибератак и технологические процессы,

адаптируя их под конкретные потребности и условия.

* Предоставить доступ к практическому обучению и развитию

навыков для людей с нулевой подготовкой, что позволит

повысить общий уровень квалификации специалистов в

области кибербезопасности.

**Задачи проекта:**

* Разработка киберполигона:

Создание виртуальной платформы для проведения

киберучений.

* Интеграция различных сценариев кибератак:

Внедрение модулей для моделирования различных типов

кибератак и технологических процессов.

* Обучение и подготовка пользователей:

Разработка учебных материалов и программ для

обучения пользователей с нулевой подготовкой.

* Тестирование и оптимизация платформы:

Проведение тестирования платформы и внесение

необходимых улучшений для повышения ее

эффективности.

1. Общая характеристика деятельности организации *(заказчика проекта)*

**Заказчик:** Московский политехнический университет.

**Организационная структура:** Организационная структура университета по виду относится к линейно функциональным структурам.  
Линейно-функциональная структура – структура, при которой  
специалисты одного профиля объединяются в структурные  
подразделения и принимают решения, обязательные для  
подразделений.

**Описание деятельности:**Вуз выпускает инженеров по широкому спектру направлений, в том числе специалистов в сфере информационных технологий (IT), биотехнологии, интеллектуальной энергетики, беспилотного транспорта и машиностроения. Также здесь представлены и гуманитарные, социально-экономические, творческие направления.

1. Описание задания по проектной практике

**Название:** Анализ типовых тактик при атаке на базы данных посредством веб-приложений.

**Цели проекта**:

* Изучить, как веб-приложения взаимодействуют с базами данных и какие уязвимости встречаются чаще всего (например, SQL-инъекции).
* Рассмотреть, как такие атаки классифицируются OWASP и MITRE ATT&CK, и какие этапы обычно включает атака.
* Развернуть учебное уязвимое веб-приложение, провести практические атаки на базу данных и зафиксировать результат.
* Проанализировать последствия атак и предложить способы защиты.
* Описание достигнутых результатов по проектной практике.

1. Описание достигнутых результатов по проектной практике.

1) Создан статический сайт визитка

2) Теоретические исследования

* Проведен анализ механизмов взаимодействия веб-приложений с базами данных, выявлены наиболее распространенные уязвимости.
* Изучена классификация атак по стандартам **OWASP Top 10** и **MITRE ATT&CK**, определены этапы их проведения (разведка, эксплуатация, эскалация, кража данных).

3)Практическая реализация

* Для практики использовался онлайн сервис Portswigger.
* Проведены успешные атаки на тестовую базу данных:
* SQL-инъекции.
* Командные инъекции.
* SSRF.
* XXE.

4) Разработанные меры защиты

На основе анализа уязвимостей предложены эффективные способы защиты:

* Технические меры
* Организационные меры

**Распределение часов (всего: 72 часа)**

| **Этап работы** | **Часы** |
| --- | --- |
| Теоретические исследования | 16 |
| Практическая реализация атак | 24 |
| Разработка мер защиты | 12 |
| Создание сайта-визитки | 12 |
| Документирование и оформление | 8 |
| **Итого** | **72** |

ЗАКЛЮЧЕНИЕ

В ходе выполнения данного проекта было проведено комплексное исследование уязвимостей веб-приложений, связанных с взаимодействием с базами данных. На первом этапе мы проанализировали теоретические основы, включая принципы взаимодействия веб-приложений с СУБД, механизмы возникновения уязвимостей и их классификацию по стандартам OWASP Top 10 и MITRE ATT&CK. Особое внимание было уделено четырем ключевым типам уязвимостей: SQL-инъекциям, командным инъекциям, SSRF и XXE-атакам, которые представляют наибольшую опасность для современных веб-приложений.

На основе проведенного анализа были разработаны комплексные меры защиты, включающие как технические решения (использование подготовленных выражений, ORM-систем, WAF), так и организационные меры (принцип минимальных привилегий, регулярные аудиты безопасности). Особый акцент был сделан на важность валидации и санитизации пользовательского ввода на всех уровнях приложения.

Результаты исследования подтвердили, что несмотря на постоянное развитие средств защиты, рассмотренные уязвимости остаются актуальной угрозой для веб-приложений. Полученные выводы могут быть использованы как для проведения аудитов безопасности существующих приложений, так и для разработки новых систем с учетом современных требований кибербезопасности.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. OWASP Foundation. OWASP Top 10 (2021) - Руководство по основным уязвимостям веб-приложений.
2. OWASP Foundation. Руководство по тестированию безопасности веб-приложений.
3. OWASP. Шпаргалки по безопасности (SQL-инъекции, XXE, SSRF).
4. MITRE ATT&CK® Framework - Матрица тактик и техник кибератак.
5. Статтард Д., Пинто М. "Руководство хакера по веб-приложениям" (2-е изд.). Wiley, 2011.
6. Ховард М., Леблан Д. "Написание безопасного кода" (2-е изд.). Microsoft Press, 2003.
7. Кларк Дж. "Атаки SQL-инъекциями и защита от них" (2-е изд.). Syngress, 2012.
8. Клайн К., Клайн Д., Хант Б. "SQL в nutshell" (4-е изд.). O'Reilly, 2020.
9. Халфонд В.Г., Виегас Дж., Орсо А. "Классификация атак SQL-инъекциями и методы защиты". IEEE, 2006.
10. Стандарты безопасного программирования CERT.