Отчет по проектной практике: Проект "JESTь"

## 1. Общая информация о проекте

Название проекта

### JESTь — платформа для погружения в мир кибербезопасности через интерактивные CTF-задачи (Capture The Flag).

Цели и задачи проекта

### Цель: Разработать образовательный веб-ресурс, позволяющий пользователям изучать и отрабатывать навыки выявления и эксплуатации уязвимостей веб-приложений в безопасной и контролируемой среде.

### Задачи:

Создать функциональный и удобный веб-сайт с интуитивно понятным интерфейсом.

Разработать шесть CTF-задач, охватывающих ключевые аспекты веб-безопасности, такие как XSS, SQL-инъекции, CSRF, IDOR и слабая аутентификация.

Обеспечить доступность задач через веб-интерфейс с подробным описанием и ссылками.

Документировать процесс разработки и подготовить развернутый отчет по итогам проектной практики.

Разместить исходный код проекта на GitHub для открытого доступа и обратной связи.

## 2. Общая характеристика деятельности организации (заказчика проекта)

Наименование заказчика

Проект выполнен в рамках учебной практики студентов групп 241-371 и 241-352 Московского политехнического университета (МосПолитех).

### Организационная структура

Заказчик — образовательное учреждение с иерархической структурой, включающей:

Учебные подразделения, ответственные за организацию образовательного процесса и практик.

Преподавательский состав, координирующий выполнение проектных заданий и оценивающий результаты.

Студенческие группы, выполняющие практические задания под руководством кураторов.

### Описание деятельности

МосПолитех готовит специалистов в области информационных технологий, включая разработку программного обеспечения, веб-технологии и кибербезопасность. Учебная практика направлена на развитие у студентов практических навыков через выполнение реальных проектов, таких как разработка веб-приложений, анализ их уязвимостей и создание образовательных инструментов. Проект "JESTь" вписывается в эту миссию, предоставляя студентам возможность углубить знания в области безопасности веб-приложений.

## 3. Описание задания по проектной практике

Задание заключалось в создании веб-сайта "JESTь", который служит платформой для размещения интерактивных CTF-задач по безопасности веб-приложений. Основные требования:

Разработать HTML-страницу с адаптивным дизайном, включающую разделы: "О нас", "Задачи", "Команда", "Контакты" и ссылку на отчет по практике.

Реализовать шесть уникальных CTF-задач, каждая из которых демонстрирует определенную уязвимость веб-приложений, с описанием и ссылками на отдельные страницы задач.

Обеспечить удобную навигацию по сайту и интеграцию внешних ресурсов (GitHub для исходного кода, Telegram для обратной связи).

Подготовить отчет, описывающий процесс разработки, достигнутые результаты и их ценность для заказчика.

Использовать современные веб-технологии (HTML, CSS, JavaScript) и обеспечить защиту сайта от внешних угроз, таких как вредоносные скрипты.

## 4. Описание достигнутых результатов по проектной практике

Проект "JESTь" успешно реализован, и все поставленные задачи выполнены. Ключевые результаты:

### Разработка веб-сайта:

Создана главная страница с адаптивным дизайном, включающая:

Заголовок и описание: Приветственное сообщение и краткое описание проекта.

Навигационное меню: Ссылки на разделы "О нас", "Задачи", "Команда", "Контакты" и отчет по практике.

### Разделы:

О нас: Описание команды и целей проекта.

Задачи: Список из шести CTF-задач с кратким описанием и ссылками.

Команда: Представление участников проекта с указанием их ролей и учебных групп.

Контакты: Ссылки на Telegram-каналы (@WHTeplo, @psayker77) и репозиторий GitHub.

Футер: Авторские права и слоган "Взламывайте с умом!".

Использованы HTML5, CSS3 и JavaScript для динамического взаимодействия. Сайт защищен от внешних угроз с помощью встроенного скрипта Cloudflare.

### CTF-задачи:

Реализованы шесть интерактивных задач, каждая из которых фокусируется на определенной уязвимости:

XSS Playground: Практика межсайтового скриптинга (XSS) для изучения ввода вредоносных скриптов.

SQL Injector: Отработка навыков эксплуатации SQL-инъекций.

AuthBuster: Анализ слабых механизмов аутентификации и их обход.

FileHunter: Поиск скрытых файлов на сервере.

CSRF Trap: Изучение уязвимостей межсайтовой подделки запросов (CSRF).

IDOR Leak: Практика эксплуатации уязвимостей IDOR (Insecure Direct Object References) для доступа к чужим данным.

Каждая задача сопровождается отдельной страницей с описанием и интерфейсом для взаимодействия.

### Техническая реализация:

Исходный код проекта размещен на GitHub (https://github.com/PsakerMosPOL/Project\_CTF), что обеспечивает прозрачность и возможность доработки.

Интеграция внешних ресурсов: Telegram для обратной связи и GitHub для хранения кода.

Сайт оптимизирован для работы на различных устройствах благодаря использованию мета-тега viewport.

### Документация:

Подготовлен настоящий отчет, включающий описание проекта, процесса разработки и достигнутых результатов.

Документация доступна через ссылку на сайте ("Отчет по практике").

### Заключение

Проект "JESTь" стал шагом в изучении веб-разработки и кибербезопасности. Команда создала платформу, которая выполняет поставленные учебные задачи. Реализованные CTF-задачи позволяют пользователям в интерактивной форме изучать уязвимости, что способствует повышению их квалификации в области кибербезопасности. Для заказчика (МосПолитех) проект является примером реализации студенческой инициативы, демонстрирующей практическое применение

знаний. В процессе работы студенты укрепили навыки командной разработки, работы с веб-технологиями и анализа уязвимостей, что делает проект значимым вкладом в их профессиональное развитие.

Список использованной литературы

OWASP Top Ten Project. — Режим доступа: https://owasp.org/www-project-top-ten/

W3Schools HTML and CSS Tutorials. — Режим доступа: https://www.w3schools.com/

MDN Web Docs: Web Security. — Режим доступа: https://developer.mozilla.org/en-US/docs/Web/Security

GitHub Documentation. — Режим доступа: https://docs.github.com/

Web Application Security: Exploitation and Countermeasures for Modern Web Applications / Andrew Hoffman. — O’Reilly Media, 2020.