МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ

Федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет ИТМО»

Информационная безопасность

Работа 3
Аудит безопасности веб-приложения

Выполнил:

Румский Александр Максимович

Группа:

P3407

Преподаватель:

Маркина Татьяна Анатольевна

Санкт-Петербург, 2025 год

Содержание

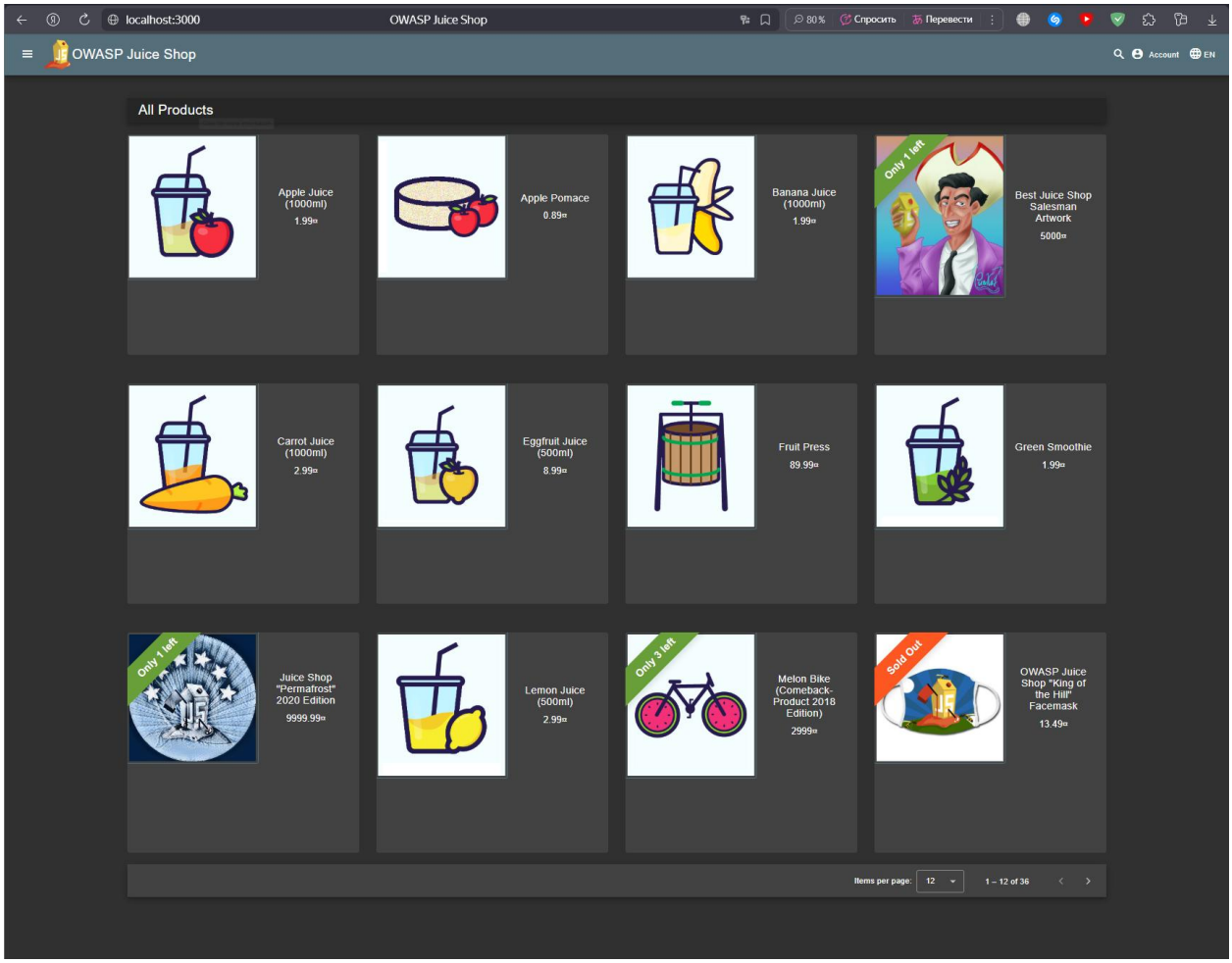
Подготовка 3
Zap 4
Результаты сканирования 4
Поиск уязвимостей 5
STRIDE 6
Таблица с найденными уязвимостями 6
Рекомендации по исправлению 6

Подготовка

Вместо предложенного в описании к работе OWASP Juce Shop был установлен bkimminich/juice-shop, так как juicyshop/juice-shop не существует/удален

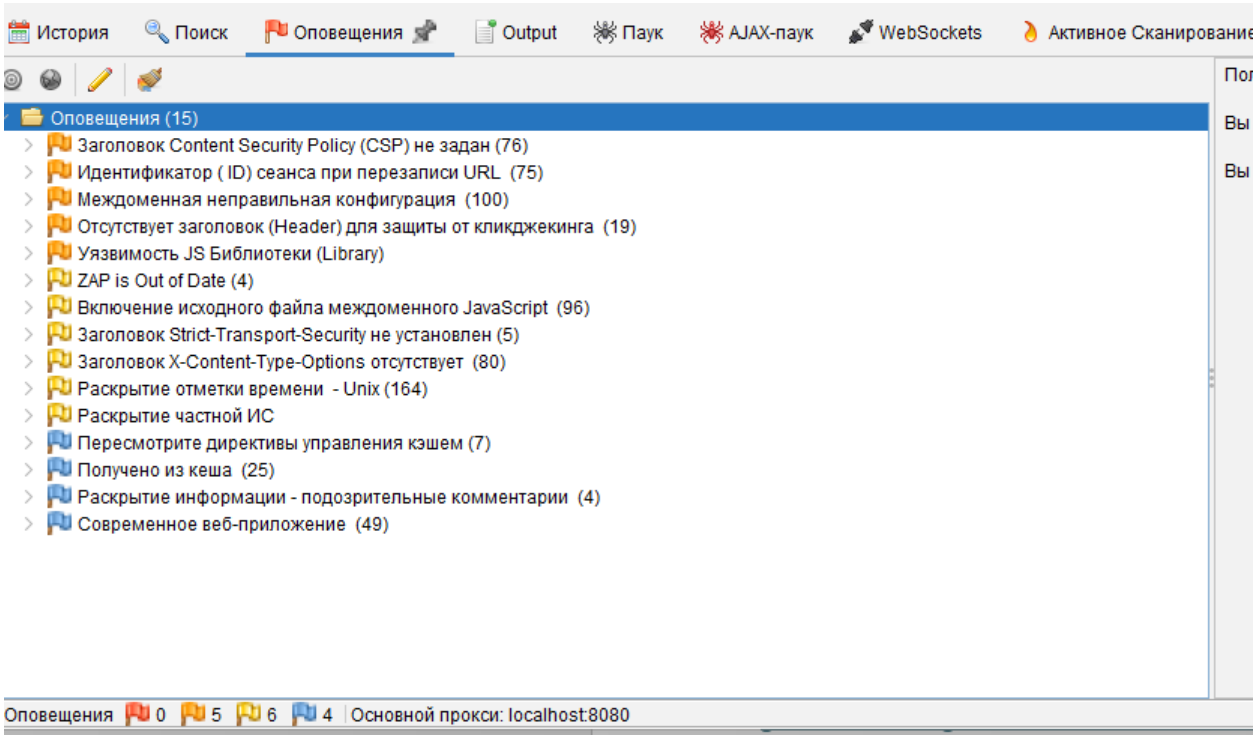
```
PS D:\ITMO\3-re\University\stage 4\autmn\Information security\lab3> docker run --rm -p 3000:3000 juicyshop/juice-shop
Unable to find image 'juicyshop/juice-shop:latest' locally
docker: Error response from daemon: pull access denied for juicyshop/juice-shop, repository does not exist or may requir
e 'docker login'

Run 'docker run --help' for more information
```

После выполнения docker run --rm -p 3000:3000 bkimminich/juice-shop в браузере стал доступен сайт OWASP Juice shop



Zap

Результаты сканирования



Поиск уязвимостей

Название	Описание и шаги воспроизведения	CVSS	OWASP Top 10	Рекомендация
SQL Injection в форме логина	В поле email введено: ' OR 1=1--. Аутентификация выполнена без знания пароля	9.8 (Critical)	A03:2021 - Injection	Использовать параметризованные SQL-запросы
Reflected XSS в поиске товаров	В строке поиска введено: <iframe src="javascript:alert(`xss`)"> Скрипт выполняется в браузере	6.1 (Medium)	A03:2021 - Injection	Экранировать пользовательский ввод перед выводом
Exposure of Sensitive Data (metrics)	Незащищенный доступ к метрикам по адресу /metrics	8.0 (High)	A03:2021 - Injection	Фильтрация доступа
Exposure of Sensitive Data (ftp)	Через /ftp и обман санитайзера(прим. добавить окончание %2500.md) можно скачать файлы, которые не должны быть доступны	7.5 (High)	A05:2021 - Security Misconfiguration	Ограничить анонимный доступ
Email Enumeration при восстановлении пароля	Форма восстановления пароля позволяет определить, зарегистрирован ли email в системе, по различию в реакции от сервера	5.3 (Medium)	OWASP Top 10: A07:2021 – Identification and Authentication Failures	Использовать одинаковое поведение

STRIDE

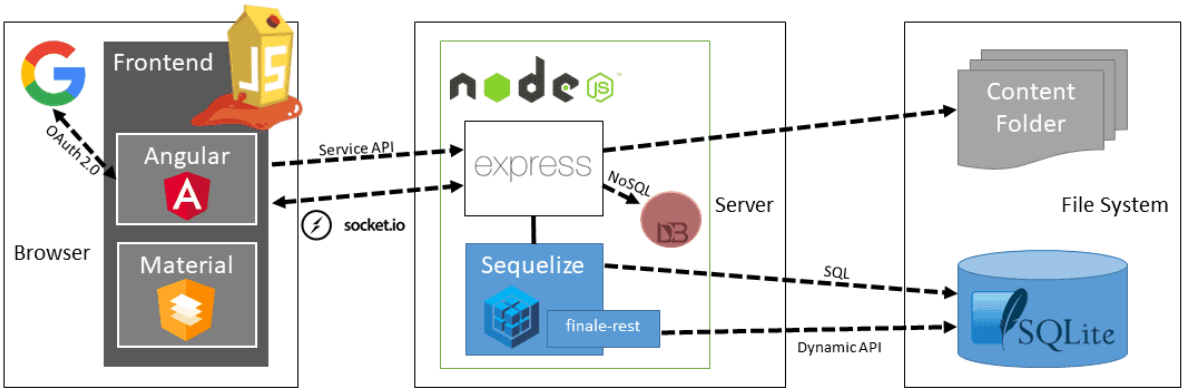


Таблица с найденными уязвимостями

Категория	**Пример угрозы**
Spoofing	Подмена JWT-токена после его кражи через XSS
Tampering	Изменение описания товаров через PUT запрос к API
Repudiation	Отсутствие надежных логов действий пользователя
Information Disclosure	Получение данных других пользователей через модификацию запросов к API
Denial of Service	Отправка большого количества запросов к поиску
Elevation of Privilege	Получение прав администратора через Broken Access Control

Рекомендации по исправлению

Внедрить строгую серверную валидацию данных

Запрет небезопасных символов

Использование allow-list

Использовать безопасную аутентификацию

HttpOnly + Secure cookies

Ограниченный срок жизни JWT

Реализовать централизованный контроль доступа

Проверка ролей для каждого API-эндпоинта

Включить Content Security Policy (CSP)

Для предотвращения XSS-атак

Настроить аудит и логирование

Фиксация действий пользователей

Защита логов от модификации