

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\autumn\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 require '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

The screenshot shows a web application interface for 'OWASP Juice Shop'. At the top, there's a header bar with various icons and links. Below it, a main content area titled 'All Products' displays a grid of items. The items are arranged in three rows:

- Row 1:** Apple Juice (1000ml) 1.99€, Apple Pomace 0.89€, Banana Juice (1000ml) 1.99€, Best Juice Shop Salesman Artwork 5000€.
- Row 2:** Carrot Juice (1000ml) 2.99€, Eggfruit Juice (500ml) 8.99€, Fruit Press 89.99€, Green Smoothie 1.99€.
- Row 3:** Juice Shop "Permafrost" 2020 Edition 9999.99€, Lemon Juice (500ml) 2.99€, Melon Bike (Comeback-Product 2018 Edition) 2999€, OWASP Juice Shop "Wipe of the Hill" Facemask 13.49€.

Each item card includes a small icon representing the product, its name, and its price. Some cards also feature a green diagonal banner with text like 'Only 1 left' or 'Sold Out'.

Zap

Результаты сканирования

The screenshot shows the ZAP (Zed Attack Proxy) interface. The title bar reads "Zap" and "Результаты сканирования". The menu bar includes "История", "Поиск", "Оповещения" (highlighted in blue), "Output", "Паук", "AJAX-паук", "WebSockets", and "Активное Сканирование". Below the menu is a toolbar with icons for history, search, notifications, output, spider, AJAX spider, websockets, and active scanning. The main pane displays a list of findings under the heading "Оповещения (15)". The findings are categorized by icon and count:

- Yellow folder icon: Заголовок Content Security Policy (CSP) не задан (76)
- Yellow folder icon: Идентификатор (ID) сеанса при перезаписи URL (75)
- Yellow folder icon: Междоменная неправильная конфигурация (100)
- Yellow folder icon: Отсутствует заголовок (Header) для защиты от кликджекинга (19)
- Yellow folder icon: Уязвимость JS Библиотеки (Library) (1)
- Yellow folder icon: ZAP is Out of Date (4)
- Yellow folder icon: Включение исходного файла междоменного JavaScript (96)
- Yellow folder icon: Заголовок Strict-Transport-Security не установлен (5)
- Yellow folder icon: Заголовок X-Content-Type-Options отсутствует (80)
- Yellow folder icon: Раскрытие отметки времени - Unix (164)
- Yellow folder icon: Раскрытие частной ИС (1)
- Blue folder icon: Пересмотрите директивы управления кэшем (7)
- Blue folder icon: Получено из кеша (25)
- Blue folder icon: Раскрытие информации - подозрительные комментарии (4)
- Blue folder icon: Современное веб-приложение (49)

At the bottom of the interface, there is a footer bar with the text "Оповещения" followed by four colored icons (red, yellow, green, blue) with counts: 0, 5, 6, 4 respectively, and the text "Основной прокси: localhost:8080".

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

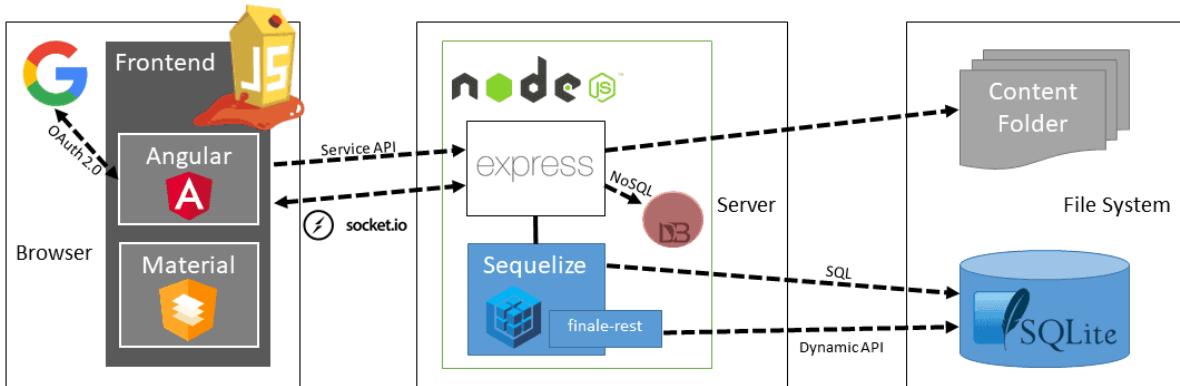


Таблица с найденными уязвимостями

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