**Лабораторная работа №6**
Тема: XSS-уязвимости и способы защиты от них
Дисциплина: Кибербезопасность

**1. Цель работы**
Познакомиться с уязвимостью Cross-Site Scripting (XSS), понять механизмы её эксплуатации и способы защиты, а также применить Content Security Policy (CSP) для предотвращения вредоносного выполнения JavaScript-кода.

**2. Технические требования**
- Docker
- Docker Compose
- cURL / Postman / Insomnia
- Браузер
- Исходный код прошлой ЛР

**3. Ход работы**
3.1. Приложение было запущено командой:
docker compose up -d --build

3.2. Проверка работы через:
curl http://localhost:3000/health

3.3. XSS-атака была выполнена путём отправки сообщения:
<img src='x' width='0' height='0' onerror='alert("XSS")'>

3.4. Уязвимость была устранена с помощью CSP и экранирования HTML.

**4. Защита от XSS**
В файл public/index.html добавлена CSP-политика:
Content-Security-Policy: default-src 'self'; script-src 'self'; object-src 'none';
Теперь браузер запрещает выполнение inline-скриптов и опасных атрибутов типа onerror.

**5. Контрольные вопросы**

1. XSS — это внедрение и выполнение стороннего JS в браузере.
2. Методы защиты: экранирование, CSP, валидация, DOMPurify.
3. CSP — политика безопасности контента, регулирующая источники ресурсов.