

# 🔖 Негативный кейс: Проверка XSS-уязвимости на странице Customer Feedback

---

## 🔖 Описание

Проверка, уязвима ли форма обратной связи (Customer Feedback) к XSS-атакам через ввод вредоносного скрипта. Цель — выяснить, фильтрует ли система потенциально опасные данные.

## 🔖 Шаги для воспроизведения:

1. Перейти на страницу Customer Feedback в OWASP Juice Shop.
2. Ввести в поле комментария следующий код:

```
<script>alert('XSS')</script>
```

3. Убедиться, что скрипт сохранён и отправлен.
4. Перейти на страницу просмотра отзывов и проверить, выполняется ли скрипт.

## 🔖 Ожидаемый результат:

Скрипт не должен исполняться. Должна быть предпринята фильтрация или экранирование HTML-содержимого.

## 🔖 Фактический результат:

Скрипт **не исполнился**. Запись не отобразилась или была отфильтрована системой.

## 🔖 Скриншоты:

!<https://imgur.com/a/1hhZPoS>

## 🔖 Среда

- Приложение: OWASP Juice Shop
- Версия: последняя (запущена через Docker)
- Браузер: Chrome 125.0.x
- ОС: Ubuntu 22.04