

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

*Факультет программной инженерии и компьютерной техники  
Информационная безопасность*

**Отчёт по лабораторной работе №3  
Аудит безопасности веб-приложения**

Выполнил:  
Бабенко Даниил  
Александрович,  
Р3434

Санкт-Петербург  
2025г

## Отчёт об аудите безопасности:

### Краткое резюме

Для проведения аудита безопасности веб-приложения была скачана утилита OWASP ZAP. С её помощью было проведено DAST-сканирование требуемого приложения (OWASP Juice Shop).

По завершении сканирования утилита смогла обнаружить следующие уязвимости:

The screenshot shows the OWASP ZAP interface. On the left, there's a tree view of contexts and sites. A context named 'Контекст по умолчанию' is selected. Under 'Сайты', two sites are listed: 'https://cdnjs.cloudflare.com' and 'http://localhost:3000'. On the right, a detailed view of a specific vulnerability is shown. The title is 'HTTP/1.1 500 Internal Server Error'. The details pane contains the following JSON response from the server:

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#jobs
Content-Type: application/json; charset=utf-8
Vary: Accept-Encoding
Date: Sat, 08 Nov 2025 15:11:05 GMT
{
  "error": {
    "code": 500,
    "message": "Internal Server Error"
  }
}
```

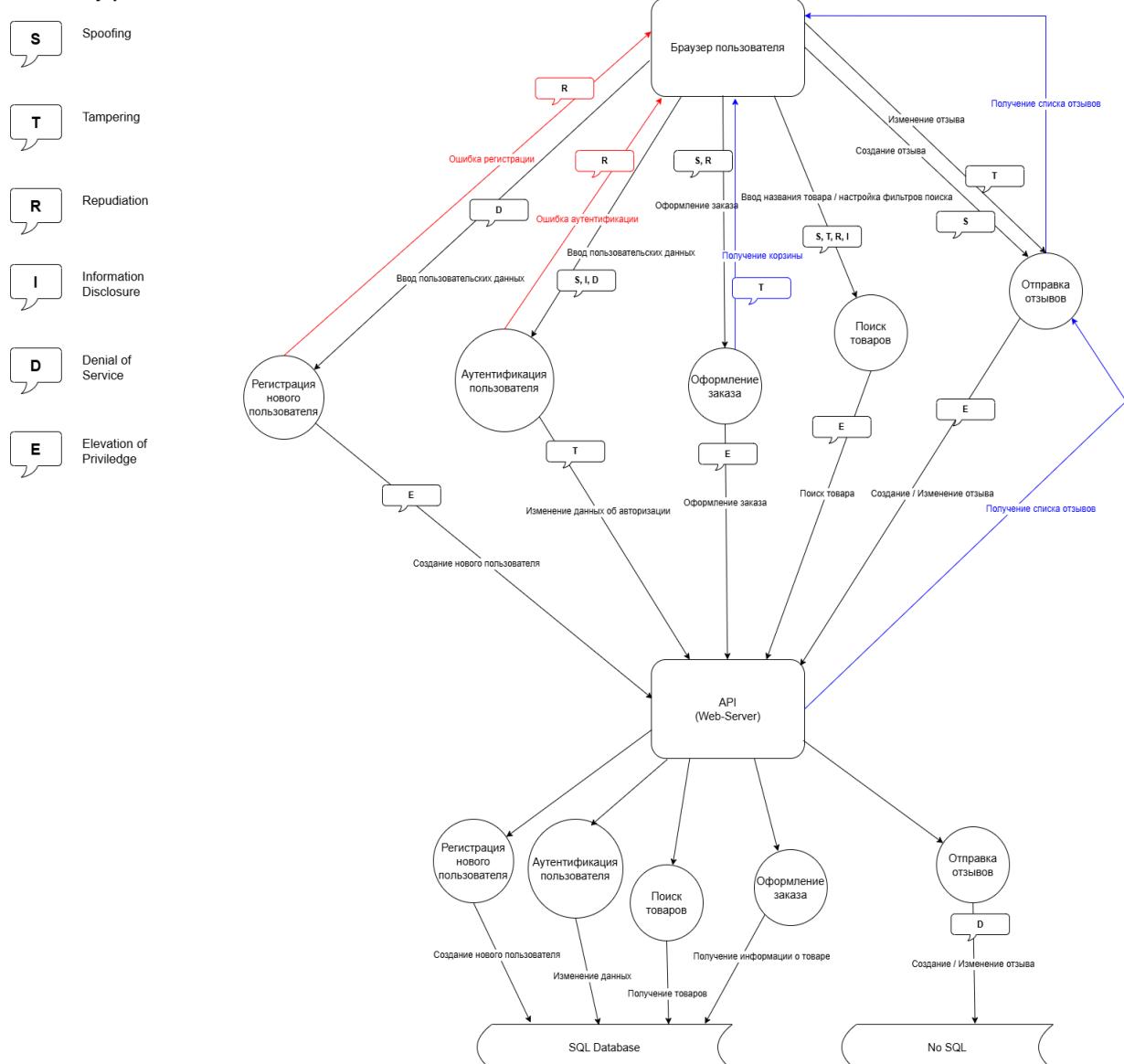
Below this, the 'Output' tab is active, showing the raw HTTP response. The 'Opportunities' tab is also visible. A red box highlights the 'SQL-инъекция' section under 'Оповещения (13)'. This section lists various SQL injection findings, such as 'Заголовок Content Security Policy (CSP) не задан (73)' and 'Идентификатор (ID) сеанса при перезаписи URL (50)'. To the right of the list, detailed information about a specific finding is provided, including the URL, risk level (High), parameter ('q'), attack ('('), and a note that it may lead to a SQL injection.

Для дальнейшей верификации найденных уязвимостей также была использована встроенная в сайт Таблица результатов (Score Board), которая предлагает пользователям самим найти уязвимости (в том числе и те, которые утилита OWASP ZAP не обнаружить).

The screenshot shows the OWASP Juice Shop Score Board interface. At the top, it displays completion statistics: 13% for Hacking Challenges, 0% for Programming Tasks, and 14/172 challenges solved. Below this is a search bar and a navigation menu with filters for different challenge types like XSS, Sensitive Data Exposure, and Broken Access Control. A note at the bottom left says '17 испытаний не готовы на Docker из-за проблем с безопасностью или технической несовместимостью!'. The main area shows four challenge cards: 'Score Board' (Miscellaneous), 'DOM XSS' (XSS), 'Bonus Payload' (XSS), and 'Privacy Policy' (Miscellaneous). Each card has a brief description and a 'Tutorial' link.

# Диаграмма DFD (с разметкой угроз по STRIDE)

Разметка угроз по STRIDE



## Угрозы по STRIDE

### Spoofing

- “Аутентификация пользователя” - есть возможность получить доступ к чужой учётной записи, воспользовавшись SQL-инъекцией (закончить ввод логина “`--`”, тем самым можно будет ввести любой пароль и войти в чужой аккаунт).
- “Оформление заказа” - есть возможность совершения CSRF-атаки, благодаря чему возможно оформить заказ без ведома настоящего владельца аккаунта.

- “Поиск товаров” - изменение токена JWT и возможность подделать его без проверки подписи позволяет проводить поиск товаров от лица пострадавшего.
- “Отправка отзывов” - путём манипуляций с PUT-запросами на сервер можно отправлять отзывы от лица других пользователей.

## Tampering

- “Аутентификация пользователя” - есть возможность изменения пароля чужой учётной записи через SQL-инъекцию, Forget Password или через надлежащий запрос HTTP GET, позволяющий заменить пароль.
- “Оформление заказа” - есть возможность изменить `bid` пользователя в `SessionStorage`. Таким образом, можно получить доступ к чужой корзине, изменяя её содержимое.
- “Поиск товаров” - данная секция уязвима к SQL-инъекциям и XSS, поэтому манипуляции с запросами в строке поиска могут привнести вредоносный код в приложение.
- “Отправка отзывов” - есть возможность модификации чужих отзывов при редактировании запросов на сервер.

## Repudiation

- “Аутентификация пользователя” - возможность изменения пользователями JWT-токенов позволяет искажать информацию, записываемую в логи приложения.
- “Регистрация нового пользователя” - так как нет проверок валидности используемого в поле `email` при регистрации, отрицание факта регистрации пользователя с данным логином.
- “Поиск товаров” - поисковая строка подвержена различного рода XSS-атакам, которые могут добавить вредоносный код на сайт. Однако из-за отсутствия детального логирования будет трудно установить пользователя, который внёс в систему вредоносный скрипт.
- “Оформление заказа” - есть возможность совершения CSRF-атак, из-за чего система может считать незаконную покупку как совершенную легально самим пользователем, что невозможно будет опровергнуть.

## Information Disclosure

- “Аутентификация пользователя” - имеет место жёсткое кодирование данных в клиентской части приложения. Таким образом, можно узнать действующие credentials для входа в систему, проинспектировав код.
- “Поиск товаров” - данная секция уязвима к SQL-инъекциям. Данные о товарах и о пользователях находятся в одном и том же хранилище SQL, что позволяет через строку поиска вводить запросы и о базе данных с пользователями.

## Denial of Service

- “Аутентификация пользователя” - ограничений на частоту запросов и количество попыток входа в систему не имеется, поэтому возможно нагрузить систему до состояния, когда она будет отказывать в авторизации настоящим пользователям.
- “Регистрация нового пользователя” - нет кроме наличия знака @ в email’е, на сайте не имеется никакой проверки валидности email. Таким образом, один пользователь может создать бесчисленное множество аккаунтов, нагружая систему до неработоспособного состояния.
- “Отправка отзывов” - с помощью манипуляций с бек-эндом API можно увидеть, что секция с отзывами уязвима к DoS-атакам, и подставив в URL команду sleep(), можно заставить сервер “спать”.

## Elevation of Privilege

- “Регистрация нового пользователя” - при регистрации система допускает подмену атрибута роли, что позволяет получить права администратора без надлежащей валидации.
- “Поиск товаров” - манипуляция с JWT-токенами позволяет изменить токен и получить права администратора, что даёт доступ к скрытым функциям сайта.
- “Оформление заказа” - есть возможность незаконного получения клиентом “премиум-статуса”, что улучшает некоторые условия обслуживания.

## Таблица уязвимостей

Название	Описание	Уровень риска (CVSS)	Категория OWASP Top 10	Предложения по устранению
SQL-инъекция	<p>Злоумышленник может вставить вредоносный SQL-код через пользовательские входные данные, манипулируя запросами к БД.</p> <p>В пользовательских запросах к БД с продуктами сайта параметр <code>q</code> уязвим к инъекциям. Внедрив в данный параметр SQL-скрипт, можно получить из БД данные пользователей.</p>	8.6 (High)	A03:2021-Injection	<p>Использовать параметризованные запросы для взаимодействий с БД;</p> <p>Использовать ORM;</p> <p>Применить whitelisting для параметра <code>q</code>.</p>
XSS	<p>Политика безопасности содержимого (CSP) помогает обнаруживать и смягчать определенные типы атак, включая XSS и атаки с внедрением данных. Эти атаки используются для всего: от кражи данных до порчи сайта или распространения вредоносных программ.</p> <p>Поисковая строка позволяет вставлять внутрь себя различные скрипты JavaScript, которые тут же исполняются при нажатии на кнопку</p>	6.1 (Medium)	A05:2021-Security Misconfiguration	<p>Экранировать пользовательский ввод с помощью программных библиотек;</p> <p>Внедрить политику безопасности CSP;</p> <p>Установить заголовок X-Content-Type-Option, равным "nosniff";</p> <p>Применять валидацию и санацию данных на сервере перед отображением.</p>

	(тестирова-лось на безобидном для системы примере, где внутрь строки был записан запрос для вызова alert).			
Insecure Direct Object Reference (IDOR)	<p>Сайт предоставляет прямой доступ к внутренним объектам на основе предоставленного пользователем идентификатора без надлежащей проверки прав доступа.</p> <p>С помощью DevTools браузера можно заменить значение bid в SessionStorage, тем самым получив доступ к данным другого пользователя (например, к содержимому корзины) без надобности входа в его аккаунт.</p>	6.5 (Medium)	A01:2021-Broken Access Control	<p>Хранить bid текущей сессии на сервере, а не на клиенте;</p> <p>Заменять предсказуемые значения id на криптографически стойкие UUID;</p> <p>Внедрить проверку прав доступа на уровне каждого запроса.</p>
Отсутствие требований по отношению к слабым паролям (CWE-521)	<p>Атака, основанная на подборе паролей. Чаще всего возникает, если приложение использует однофакторную аутентификацию для пользователей.</p> <p>При этом в системе нет никаких ограничений на создание пароля при регистрации нового юзера, поэтому могут</p>	9.8 (Critical)	A07:2021-Identification and Authentication Failures	<p>Использовать обязательной 2FA;</p> <p>Ограничение количества попыток на ввод верного пароля;</p> <p>Добавить обязательные требования к сложности паролей</p>

	использоваться любые, даже самые примитивные и ненадёжные пароли, чем легко можно воспользоваться (так, например, пароль админа сайта - admin123).			
JWT-уязвимость	<p>Уязвимость, позволяющая злоумышленнику повысить уровень своих прав в системе, тем самым, получая доступ к защищённым и важным данным путём манипуляций с JWT-токеном.</p> <p>С помощью DevTools браузера зарегистрированный пользователь может получить свой JWT-токен, декодировать его и на основании полученного результата изменить свой токен, выдав себе дополнительные права (заменив role на "admin" и выключив проверку подписи)</p>	9.1 (Critical)	A02:2021-Cryptographic Failures	<p>Использовать механизм Access-Refresh токенов;</p> <p>Явно запретить обработку неподписанных токенов;</p> <p>Валидировать подпись на стороне сервера;</p> <p>Разрешение использования только определённых алгоритмов (например, RS256, HS256).</p>

## Общие рекомендации по устранению рисков

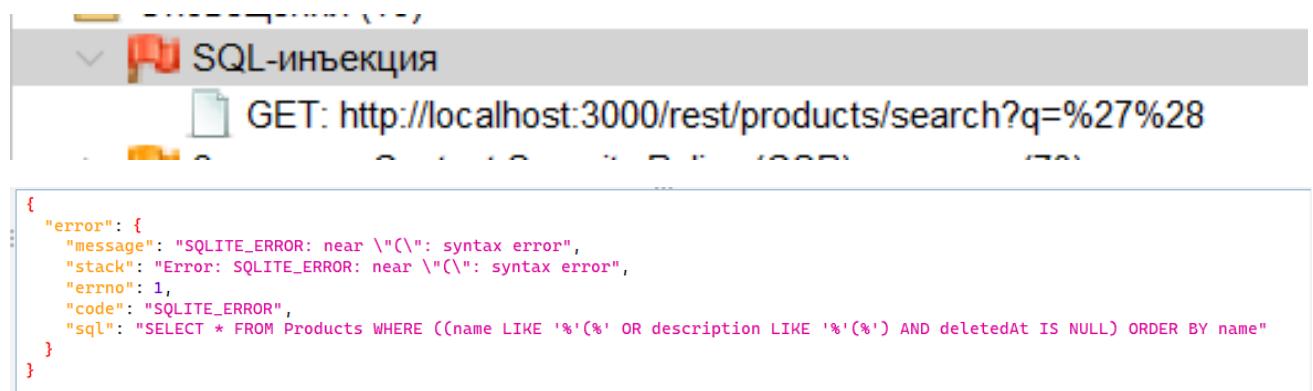
1. Внедрить единый строгий фреймворк для контроля доступа на основе роли и контексте пользователя.

2. Вся критичная бизнес-логика (включая проверку прав доступа, валидацию и санацию данных, должна выполняться на стороне сервера).
  3. Реализовать многоуровневую защиту аутентификации.
  4. Установить безопасные заголовки HTTP, политики и заголовки (CSP, HttpOnly, X-Frame-Options).

## Скриншоты, подтверждающие наличие уязвимостей

## 1. SQL-инъекция.

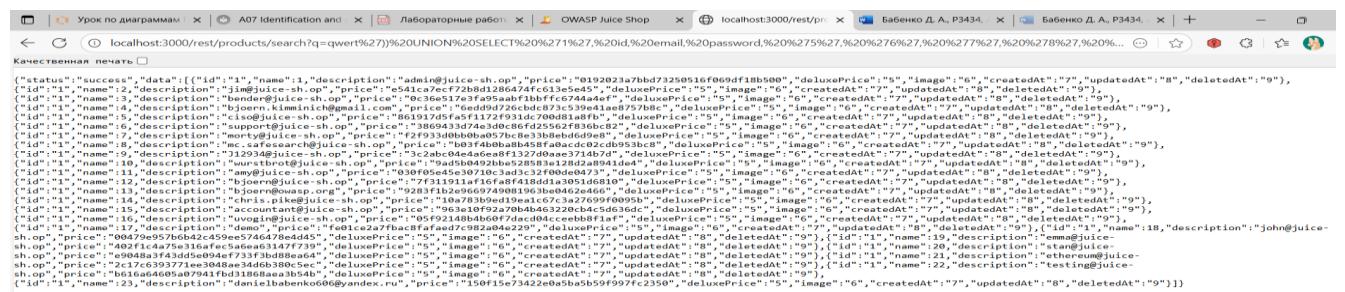
OWASP ZAP даёт подсказку, где можно найти SQL-инъекцию, а именно в параметре q при переходе на адрес /rest/products.



Также тут видно, каким образом происходит запрос к базе данных, и поэтому, зная кол-во столбцов в БД с продуктами, в текст запроса возможно вставить вредоносный SQL-скрипт.

Например, вставив данную строку параметр q, можно получить список всех юзеров вместе с их закодированными паролями:

*qwerty')) UNION SELECT '1', id, email, password, '5', '6', '7', '8', '9' FROM Users--*



Примечание: так как я не являюсь экспертом в хакинге, то в подтверждении большинства уязвимостей в целях самопроверки я сверялся с заданиями в Score Board.



2. XSS - базовый пример, который показывает, как можно вставить собственный скрипт на сайт через строку поиска (DOM XSS). Необходимо вставить в поисковую строку данный запрос: <iframe src="javascript:alert('xss')">.

You successfully solved a challenge: DOM XSS (Perform a DOM XSS attack with <iframe src='javascript:alert('xss')'>.)

3. В качестве проверки уязвимости, принадлежащей категории Broken Access Authentication попытаемся просмотреть содержимое корзины другого юзера.

Key	Value
bid	6
itemTotal	5.97

Заменив вручную `bid` текущего юзера, осуществляю переход в корзину и, по сути, получаю доступ к корзине другого юзера.

You successfully solved a challenge: View Basket (View another user's shopping basket.)

Your Basket  
(danielbabenko606@yandex.ru)

Total Price: 0¤

Checkout

You will gain 0 Bonus Points from this order!

Storage

- Local storage
- Session storage
  - http://localhost:3000
- Extension storage
  - IndexedDB
- Cookies
  - Private state tokens
  - Interest groups
- Shared storage
  - Cache storage
  - Storage buckets

Background services

- Back/forward cache
- Background fetch
- Background sync
- Bounce tracking miti...

Key	Value
bid	7
itemTotal	5.97

4. Пароль администратора сайта является до смешного простым, так что злоумышленникам не составит труда войти в аккаунт администратора простым перебором паролей (можно использовать также и SQL-инъекцию, но ей уже уделили внимание ранее).

## Login

Email\*  
admin@juice-sh.op

Password\*  
admin123

Forgot your password?

Log in

Remember me

or

 Log in with Google

Not yet a customer?

**5. Сайт никаким образом не проверяет подпись JWT-токена, поэтому злоумышленники может его легко можно подделать, выдав себе права администратора.**

Ответ, получаемый обычным юзером при попытке зайти на панель администратора:

В файлах cookies находим JWT-токен и декодируем его:

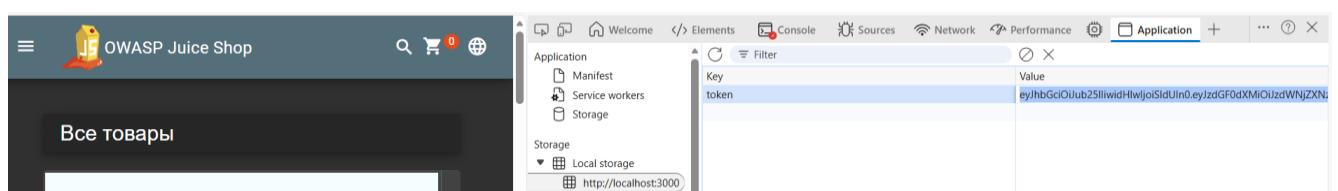
Name	Value	Do...	Path	Expi...	Size	Htt...	Sec...	Sa...	Part...	Cro...	Prio...
_mkto_trk	id:713-XSC-918&token:_mch-cl...	.clo...	/	202...	82						Me...
cfz_google-analytics_v4	%7B%22nzc...	.clo...	/	202...	1451	✓	✓	Lax			Me...
continueCode	qeb6arZJVwo7dxVt6t3cofEWuW...	loc...	/	202...	72						Me...
cookieconsent_status	dismiss	loc...	/	202...	27						Me...
Idea-3767b9b4	e094ca91-757c-42ac-a050-e83c...	loc...	/	202...	49	✓		Strict			Me...
Idea-46145655	4794a28e-9a6e-4325-a6cd-5e3...	loc...	/	202...	49	✓		Strict			Me...
language	ru_RU	loc...	/	202...	13						Me...
OptanonConsent	isGpcEnabled=0&datestamp=M...	.clo...	/	202...	506			Lax			Me...
Pycharm-5aec7632	84117545-7ebc-48f8-82a3-beb...	loc...	/	202...	52	✓		Strict			Me...
token	eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9eyJzdGF0dXMiOiJzdWNjZXNzIwiZGF0YSl6eyJpZC16MjMsInVzZXJuYW1ljoilwiZW1haWwiOjkyYW5pZWxiYWJlbmtvNja2QHlhbmRleC5ydSlslnBhc3N3b3JkjoMTUwZjE1ZTczNDlyZTBhNWJhNWl1OWY5OTdmYzlzNTAiLCjb2xljoiY3VzdG9tZXliCJkZWXteGVUb2tbi6lilslmxhc3RMb2dpbkwljoil2Fzc2V0cy9wdWjsaWMvaWThZzVzL3wbG9hZHMsVGVmYXVsdsC5zdmciLCJ0b3RwU2VjcmV0joilwiwaXNBY3RpdmUiOnRydWUsImNyZWFOZWRBdC16jlwMjUtMTEtMDggMTU6NDM6MjMuNj4lCswMDowMcIslnVwZGF0ZWRBdC16jlwMjUtMTEtMDggMTU6NDk6NDUuMjMxlCswMDowMcIslnRlbGVZWRBdC16bnVsbH0slmlhdCl6MTc2Mjc4MjgxN30.vbVgdNSZ98h2Zf-XsRdmASCXh6Y8eTgsiEsxpUgE2S8GIV_25CO7KU0jdWgTjOsKahuFGoRDCFmtL573mxMzL259-3G7V2sIH95FnvGVSCjCfsOO51pRAxwZKPbxm-CJy_5Op78Uv4JpW0l6DNpgsu1Sg3-LHhn8lvd0zk	loc...	/	202...	749						Me...
welcomebanner_status	dismiss	loc...	/	202...	27						Me...

## DECODED PAYLOAD

```
JSON CLAIMS TABLE COPY ↗

{
  "status": "success",
  "data": {
    "id": 23,
    "username": "",
    "email": "danielbabenko606@yandex.ru",
    "password": "150f15e73422e0a5ba5b59f997fc2350",
    "role": "customer",
    "deluxeToken": "",
    "lastLoginIp": "",
    "profileImage": "/assets/public/images/uploads/default.svg",
    "totpSecret": "",
    "isActive": true,
    "createdAt": "2025-11-08 15:43:23.628 +00:00",
    "updatedAt": "2025-11-08 15:49:45.231 +00:00",
    "deletedAt": null
  },
  "iat": 1762782817
}
```

Затем кодируем токен назад, изменяя значение role на “admin”, а также меняя значения поля алгоритма проверки подписи на “none”, и вставляем данный токен в качестве токена юзера.



The screenshot shows the Chrome DevTools interface with the Application tab selected. On the left, the OWASP Juice Shop application is visible, displaying a list of products. On the right, the Application tab's storage panel shows local storage for the domain http://localhost:3000. A single item named 'token' is listed under the 'Storage' section. The key 'token' is highlighted in blue, and its value is a long, encoded JWT string: eyJhbGciOiJub25lIiwidHlwIjoiSlUih0.eyJzdGF0dXMiOiJzdWNjZXN... .

The screenshot shows the OWASP Juice Shop administration interface at the URL [localhost:3000/#/administration](http://localhost:3000/#/administration). The top navigation bar includes links for 'Аккаунт' (Account), 'Корзина' (Cart) with a count of 0, and 'RU'. The main content area has two sections: 'Администрирование' (Administration) on the left and 'Отзывы клиентов' (Customer Reviews) on the right.

**Зарегистрированные пользователи**

**Отзывы клиентов**

Рейтинг	Комментарий	Автор	Действия
★★★	I love this shop! Best products in town! Highly recommended!	(***in@juice-sh.op)	...
★★★	Great shop! Awesome service!	(***@juice-sh.op)	...
★	Nothing useful available here!	(***der@juice-sh.op)	...
★	Please send me the juicy chatbot NFT in my wallet at /juicy-nft : "purpose betray marriage blame crunch monitor spin slide donate sport lift clutch"	(***eruum@juice-sh.op)	...
★★	Incompetent customer support! Can't even upload photo of broken purchase! Support Team: Sorry, only order confirmation PDFs can be attached to complaints!	(anonymous)	...
★★★	This is the store for awesome stuff of all kinds!	(anonymous)	...

## Отчёт OWASP ZAP

<https://github.com/DanielBabenko/Infobez-LR3-Babenko/blob/main/2025-11-12-ZAP-Report-.html>