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

Информационная безопасность

Работа 3

Аудит безопасности веб-приложения

Группа: P3416

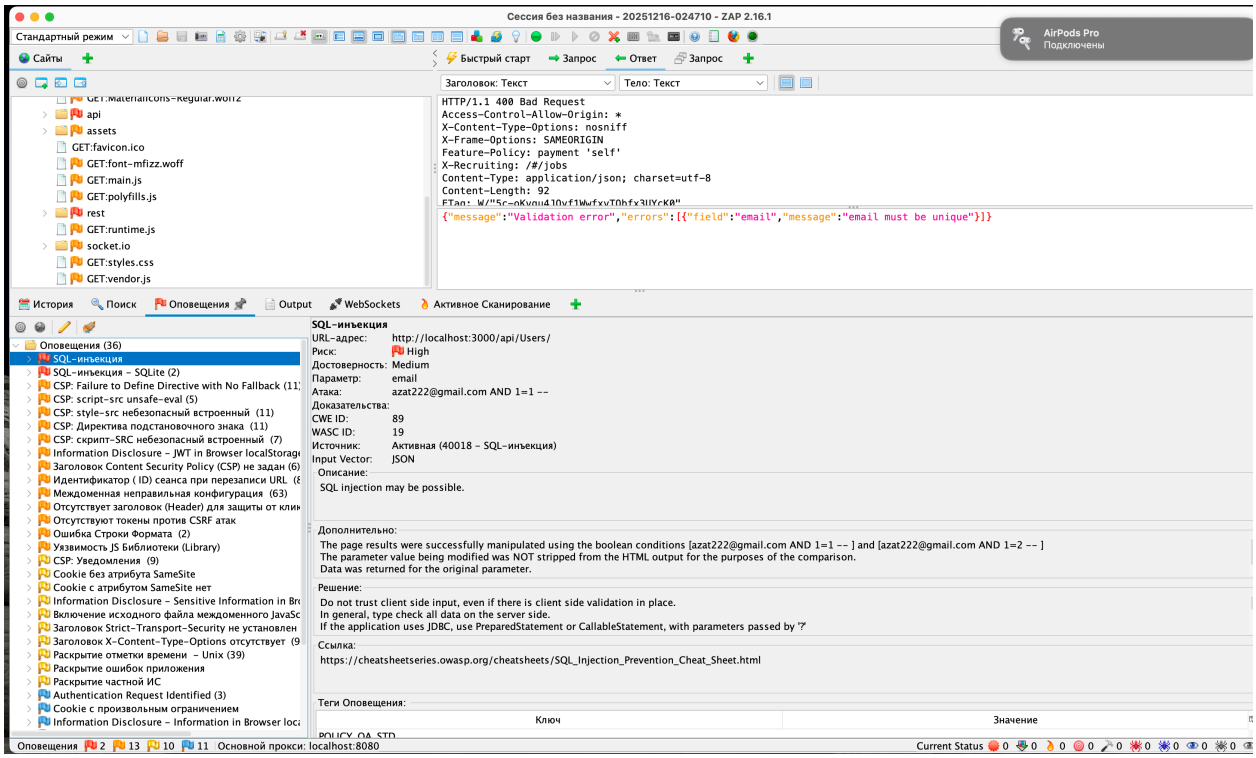
Выполнил:

Сиразетдинов Азат Ниязович

г. Санкт-Петербург

2025

Выполнение

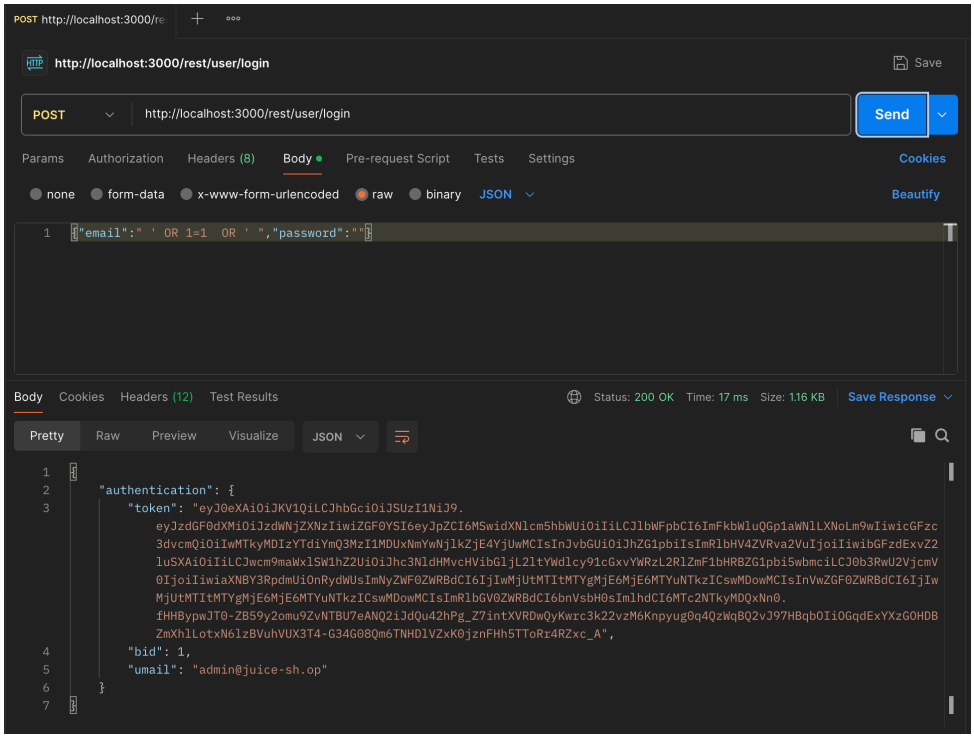


Я запустил докер контейнер juice-shop и провел сканирование на уязвимости с помощью программы ZAP

Резюме по найденным уязвимостям:

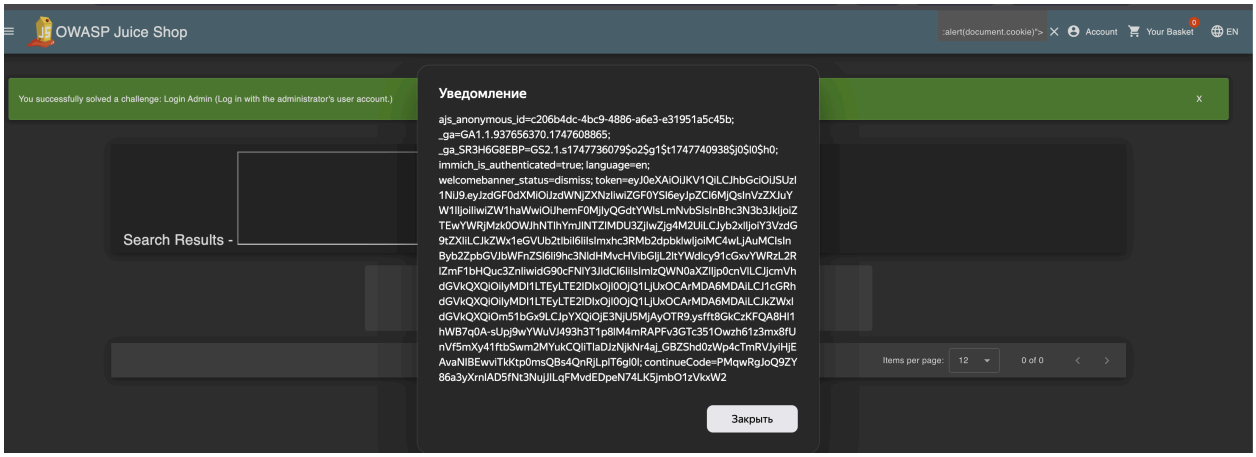
SQL-Injection

Сервис не экранирует строки в SQL инъекции, что позволяет получить доступ для не аутентифированных пользователей



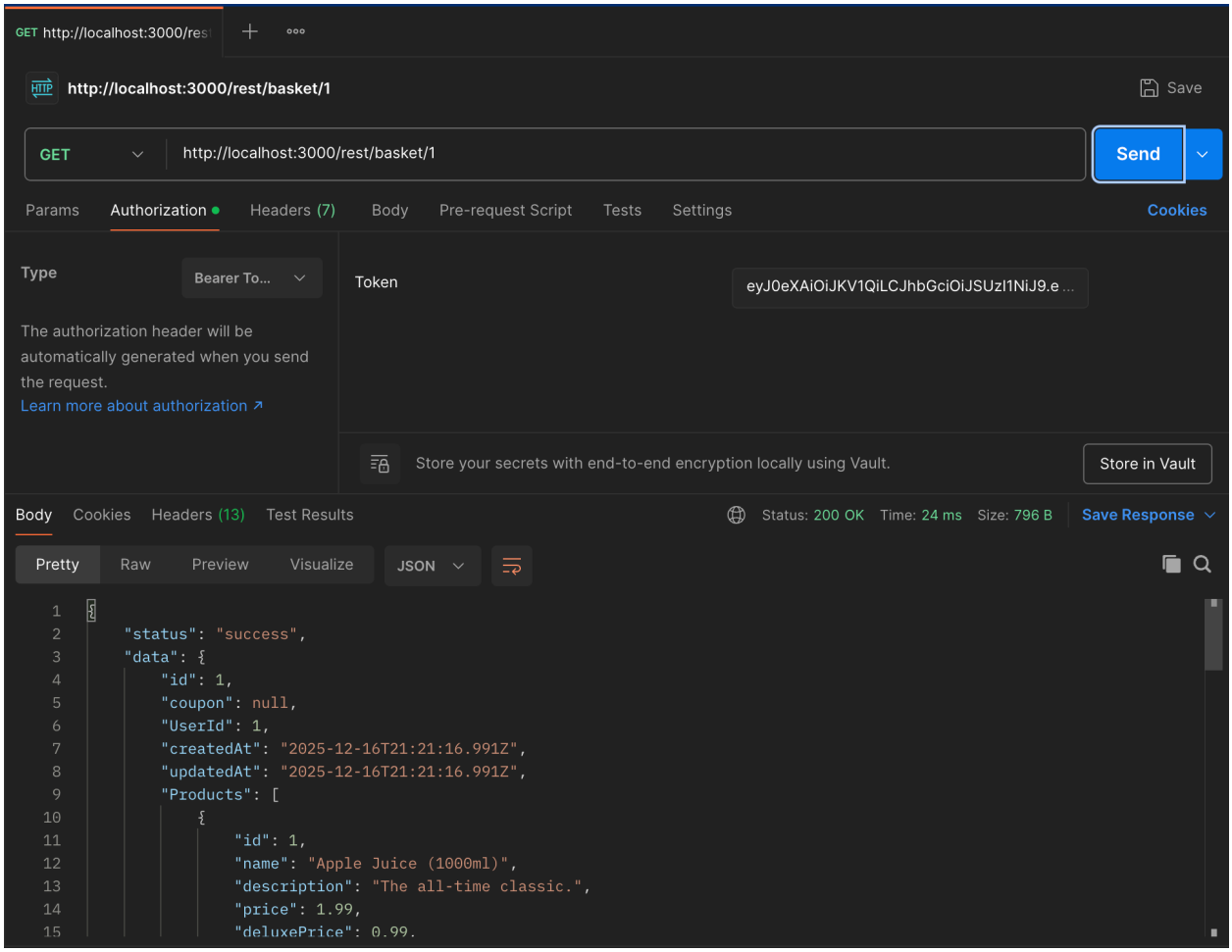
XSS

Для срабатывания скрипта достаточно вставить <iframe src="javascript:alert(document.cookie)"> в строку поиска товара. Куки в дальнейшем могут быть направлены на сторонний ресурс



Broken access control

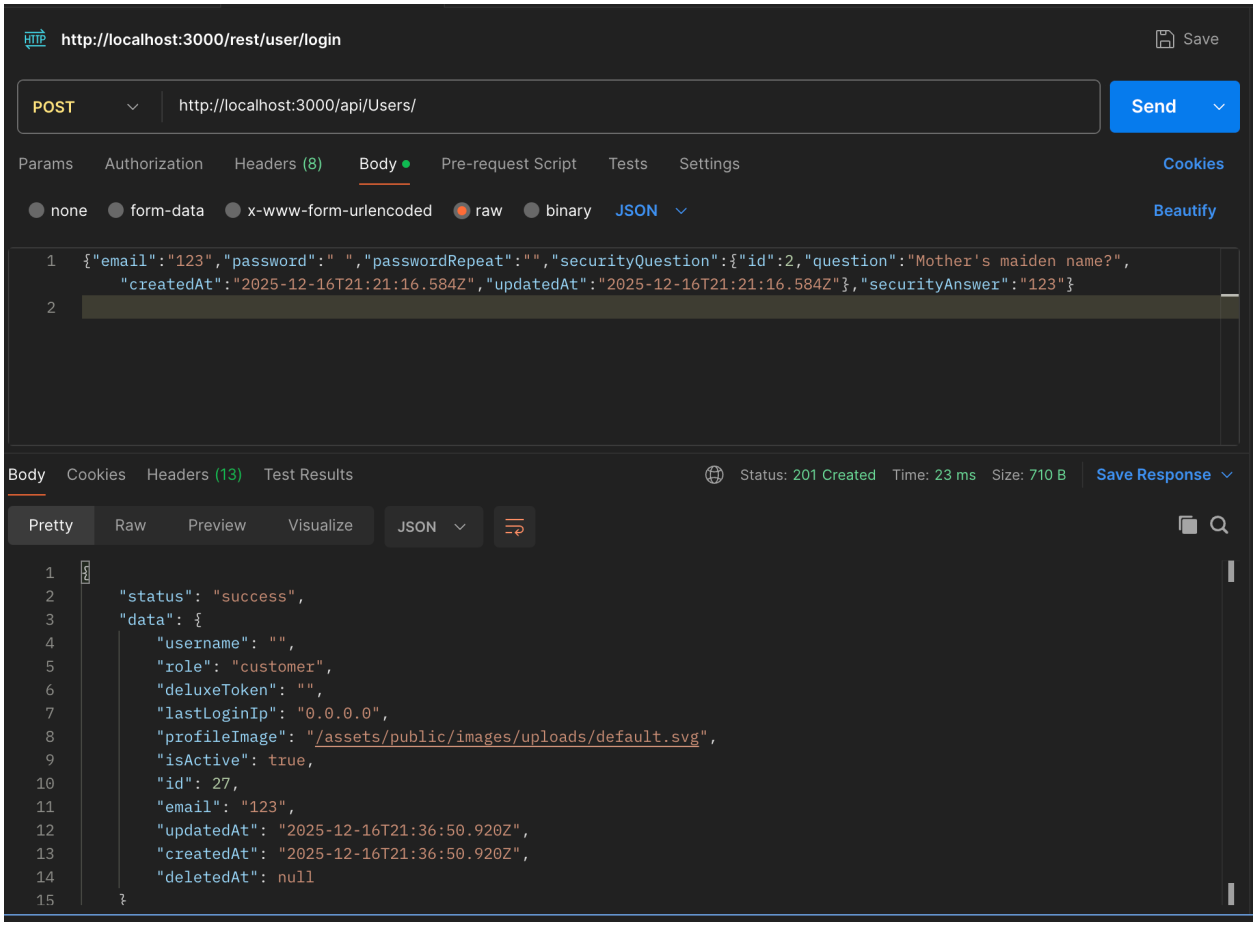
В сервисе нет проверки на получение чужой корзины товаров: я могу просто подставить другой ID корзины в запросе



Off-site redirect

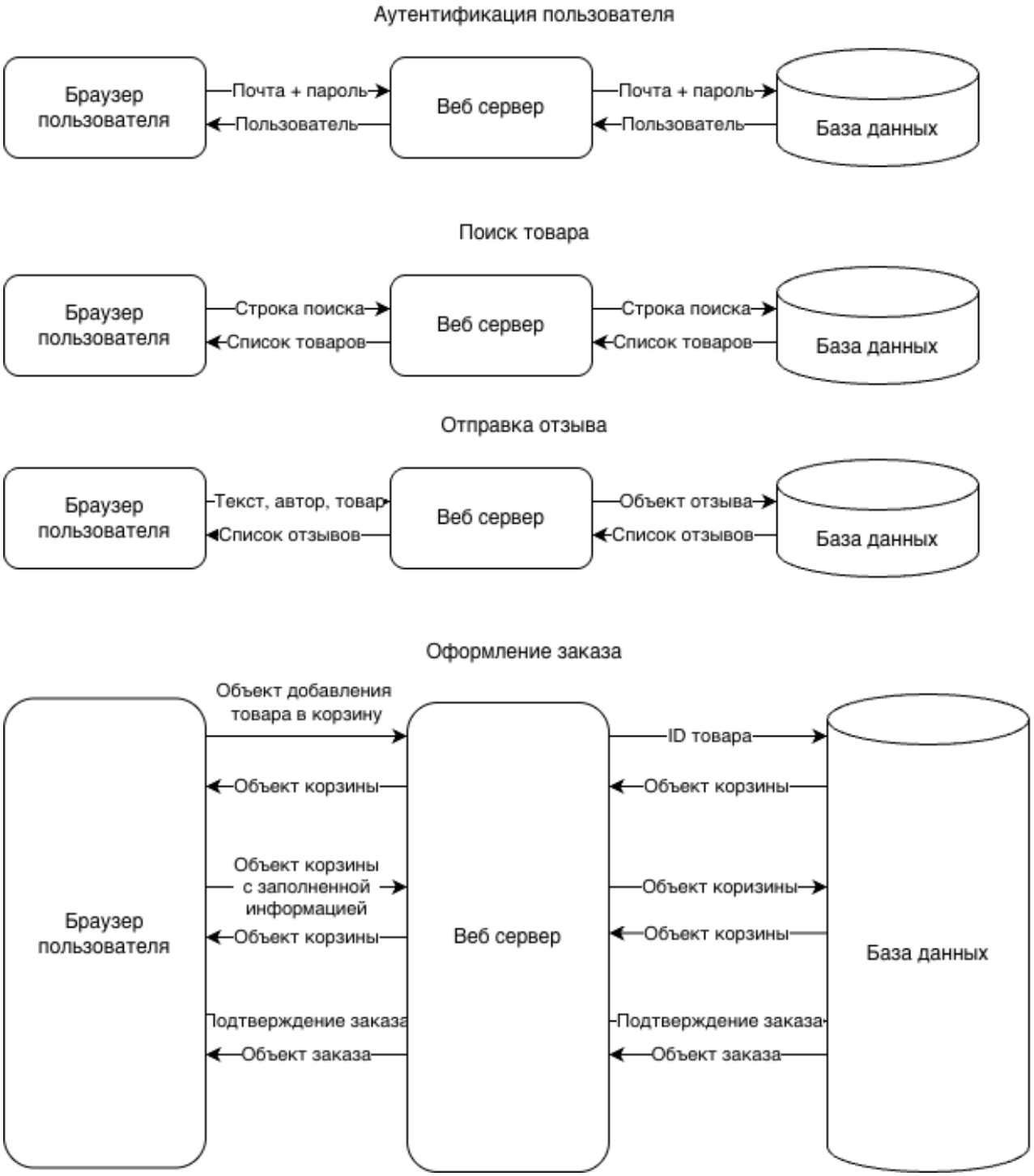
При переходе по ссылке http://localhost:3000/redirect?to=https://github.com/juice-shop/juice-shop сайт автоматически переадресовывает на нашу ссылку, что может использоваться для фишинга

Отсутствие валидации вводимых данных



Позволило мне зарегестрироваться с невалидной почтой, и несовпадающими password и passwordRepeat, и небезопасным паролем

Диаграмма потока данных



Разметка угроз по STRIDE

S - spoofing:

- На потоке данных «Аутентификация» можно перехватить сессионные данные через XSS

T – tampering:

- На потоке «Отправка отзывов» можно передать другое имя автора, товара, сообщение в обход валидации на фронте.
- На потоке «Отправка отзывов» можно изменить отзыв другого человека, заменив параметры HTTP-запроса
- На потоке «Аутентификация» можно зайти через пользователя с пустыми логином и/или паролем через изменение HTTP-запроса

R – repudiation:

- На каждом из потоков есть вероятность возникновения Repudiation, потому что логи по заказам и пользователям не ведутся

I – information disclosure:

- На потоке «Отправка отзывов» пользователь может опубликовать XSS, который будет отсылать cookie всех пользователей, зашедших в отзывы
- На потоке «Аутентификация» с помощью SQL-инъекции можно перебрать всех доступных пользователей

D – Denial of Service:

- На любом из потоков есть вероятность «положить» сервис путем DDoS-атаки

E – Elevation of privilege:

- На потоке «Аутентификация» можно зайти под любым пользователем с помощью SQL-инъекции
- На потоке «Отправка отзывов» можно изменить отзыв другого человека, заменив параметры HTTP-запроса
- На потоке «Создание заказа» можно получить доступ к корзине другого пользователя

Таблица уязвимостей

Название	Описание	Уровень риска			Категория OWASP	Предложения по исправлению
		В	Т	Е		
SQL Injection при аутентификации	В запросе аутентификации можно вместо email вставить SQL инъекцию	10	8.8	8.8	A03:2021 – Injection	Использовать параметризованные запросы
XSS в поиске	Вставить в поле HTML тег, который отобразиться как тег	8.3	7.3	7.3	A03:2021 – Injection	Экранировать ввод пользователя, не отображать текста как теги, использовать Content-Security-Policy
Off-site redirect	Переход по ссылке localhost/redirect?to=url редиректит на указанную страницу	4.3	3.8	3.8	A05:2021 – Security Misconfiguring	Создать список доменов разрешенных для редиректа
Доступ к чужой корзине	Выполнить запрос получения корзины с чужим токеном	6.3	5.6	5.6	A01:2021 – Broken access control	Перед выдачей ответа валидировать владельца корзины
Создание пустого пользователя	Зарегестрировать пользователя с невалидными данными	7.6	6.7	6.7	A01:2021 – Insecure Design	Валидировать данные на сервере
Отправка отзывов от лица другого пользователя	При создании отзыва можно создать отзывы от лица другого пользователя	7.6	6.7	6.7	A01:2021 – Broken access control	Получать имя пользователя из JWT токена
Редактирование чужого отзыва	Вручную изменить другой отзыв подставив ID	8.2	7.2	7.2	A01:2021 – Broken access control	Получать имя пользователя из JWT токена
DDOS атаки	Начать DDOS атаку большим количеством запросов	7.5	6.6	6.6	A05:2021 – Security Misconfigured	Настроить необходимые защитные меры против DDOS атак

Общие рекомендации

- Спроектировать систему по принципу «минимального доверия». Все входные данные необходимо валидировать вне зависимости от проверок на стороне клиента. Возвращать информацию о ресурсе только после проверки, что пользователь действительно имеет к нему доступ
- Взаимодействовать с базой через ORM и параметризированные запросы с минимально необходимыми правами
- Использовать экранирование и очистку пользовательского ввода, внедрить заголовки
- безопасности в ответы HTTP.
- Для предотвращения автоматизированных атак реализовать механизмы ограничения частоты запросов

Отчет OWASP ZAP

https://disk.yandex.ru/d/gvuFvV394tAFBw