**Практическое задание. Анализ защищённости веб-приложений**

**Что нужно сделать**

Проведите анализ защищённости уже знакомого вам приложения Juice Shop. В отчёте укажите только уязвимости из OWASP Top-10; CWE, которые их вызывают; а также рекомендации по их устранению.

Отчёт должен иметь следующую структуру:

1. Введение — описание приложения.
2. Результаты статического анализа — общие, можно без детализации.
3. Уязвимости из OWASP Top-10, обнаруженные в результате статического анализа, — минимум пять штук.
4. Демонстрация эксплуатации трёх уязвимостей из OWASP Top-10 — скриншоты эксплуатации, проведённой с помощью инструмента Burp Suite. Выбор этих уязвимостей остаётся на ваше усмотрение.
5. Рекомендации по устранению к трём продемонстрированным уязвимостям — можно взять основу [с сайта MITRE ATT&CK](https://attack.mitre.org/) под найденные CWE.

В отчёте обязательно должны присутствовать:

1. Скриншоты (минимум два) или выгрузка результатов статического сканирования в пункте 2.
2. Список уязвимостей из OWASP Top-10 с доказательствами в пункте 3 (в виде скриншотов, найденных анализатором уязвимостей; отдельно от остальных уязвимостей).
3. Скриншоты из Burp Suite в пункте 4, а также обязательно текстовое описание эксплуатации: что необходимо сделать, чтобы воспроизвести уязвимость.

**Формат сдачи**

Итоговый отчёт необходимо загрузить в формате DOCX или PDF на свой гит. Приложите ссылку на отчёт в форму для ответа.

1. **Введение**

Juice Shop - это веб-приложение, созданное специально для тестирования уязвимостей и обучения в области безопасности веб-приложений. Это приложение разработано как искусственно уязвимый набор для практического обучения разработчиков и тестировщиков на практических примерах.

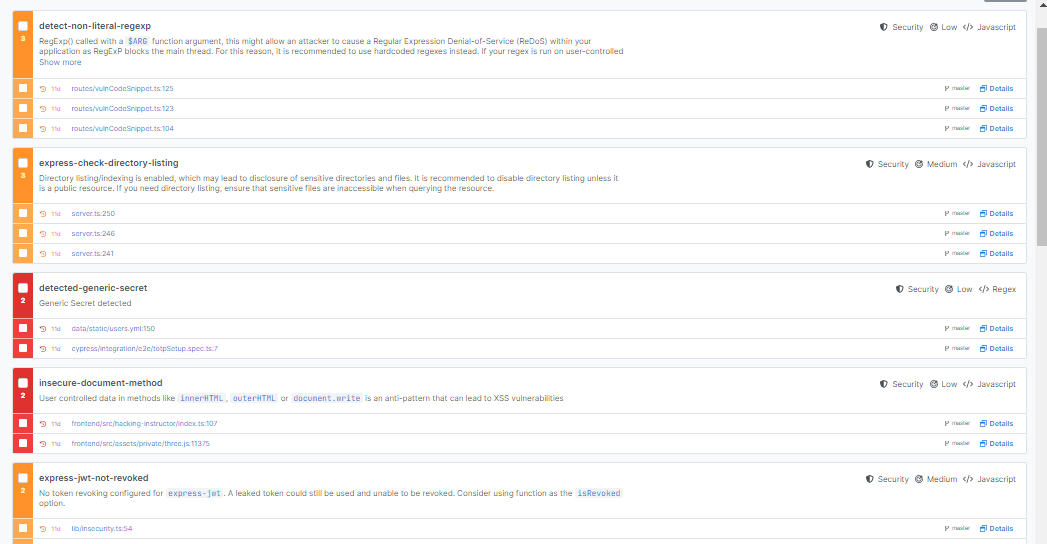
1. **Результаты статического анализа**

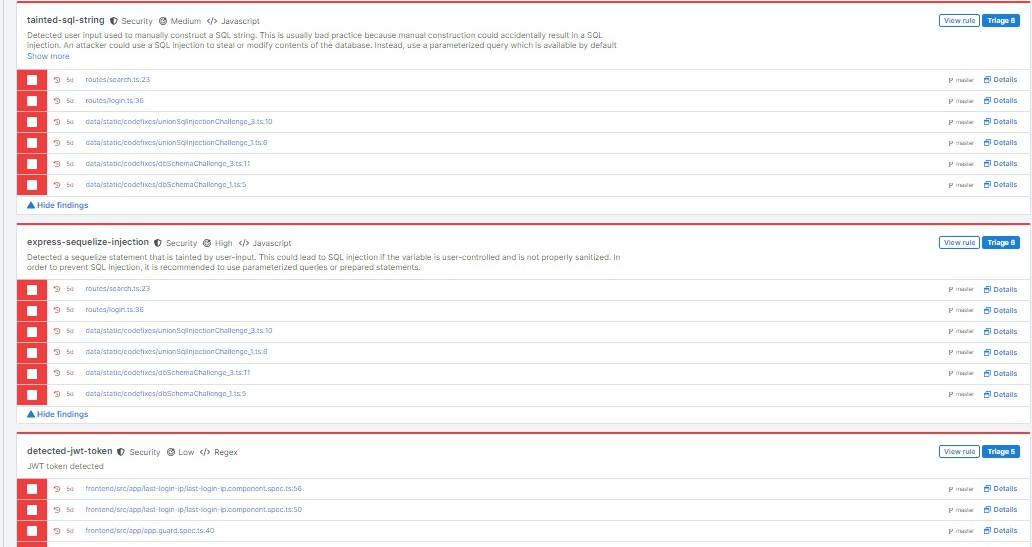
Для проведения статического анализа данного веб-приложения воспользуемся бесплатным статическим анализатором кода – Semgrep. В результате анализа данным средством выявлено большое количество уязвимостей из OWASP Top 10.

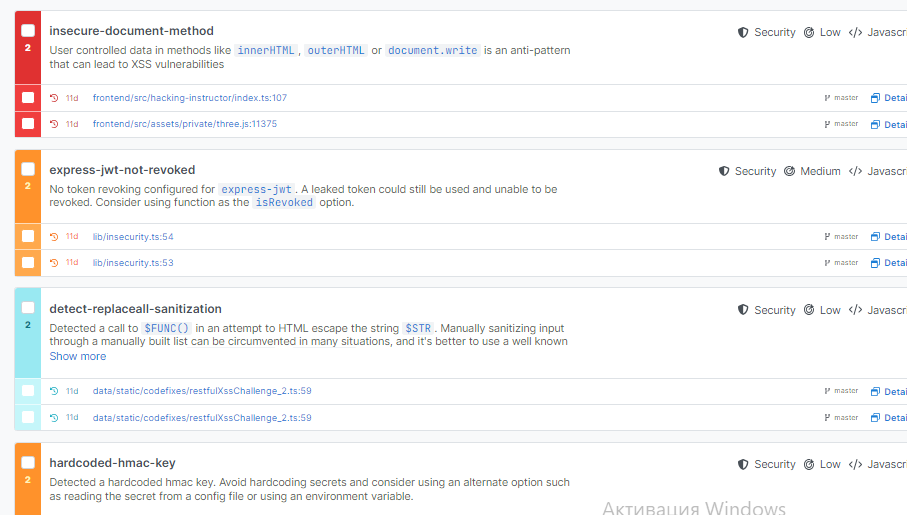
В частности, такие уязвимости, как:

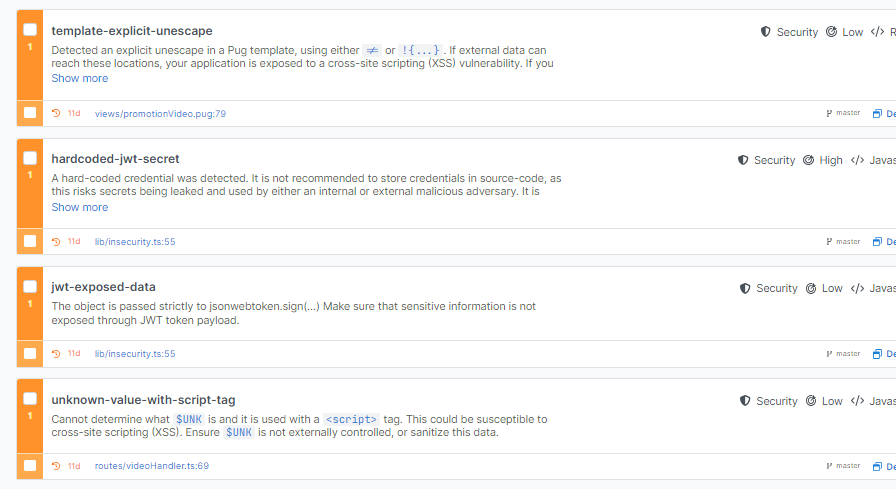
* SQL-инъекции
* XSS (межсайтовый скриптинг)
* CSRF (межсайтовая подделка запроса)
* Недостаточная авторизация и аутентификация
* Уязвимости в безопасности сессии.

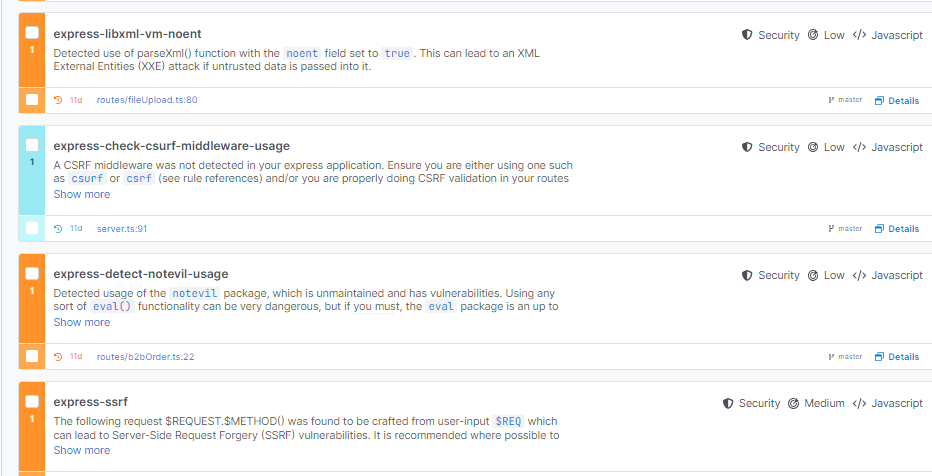
Найденные уязвимости в результате статического анализа:











1. **Уязвимости из OWASP Top-10**

1.SQL-инъекции – express-sequelize-injection

2.Недостаточная авторизация и аутентификация – detected-jwt-token

3.Межсайтовая подделка запроса (Cross-Site Request Forgery, CSRF/XSRF) – express-ssrf

4.Межсайтовый скриптинг – XSS (Cross Site Scripting) – insecure-document-method, unknown-value-with-script-tag

5.Уязвимость в безопасности сессии

1. **Демонстрация уязвимостей через BurpSuite**

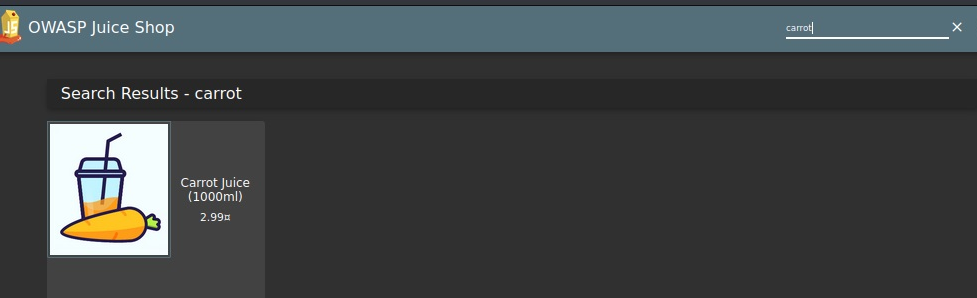
Продемонстрируем эксплуатацию уязвимостей на примере SQL-инъекций, а также на примере нарушения аутентификации.

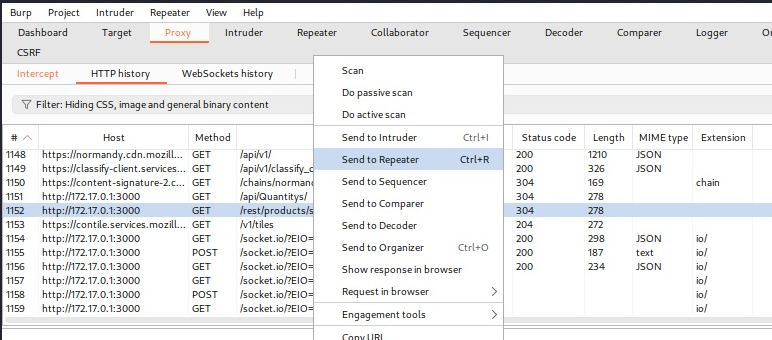
- database schema (sql-инъекция):

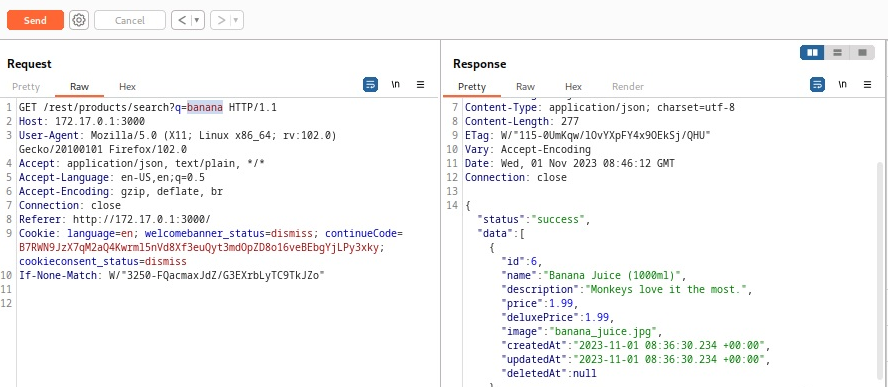
Используя burp, перехватим HTTP-запрос для поиска продукта. Видим, что искомый продукт q= непустой. Добавляя значения, получаем ошибку **SQLITE\_ERROR: означает, что база данных - это sqlite.**

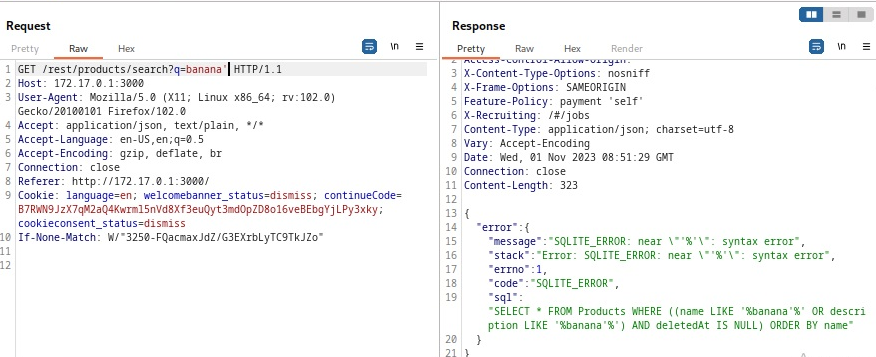
Далее нужна атака union для подключения к другой базе данных.

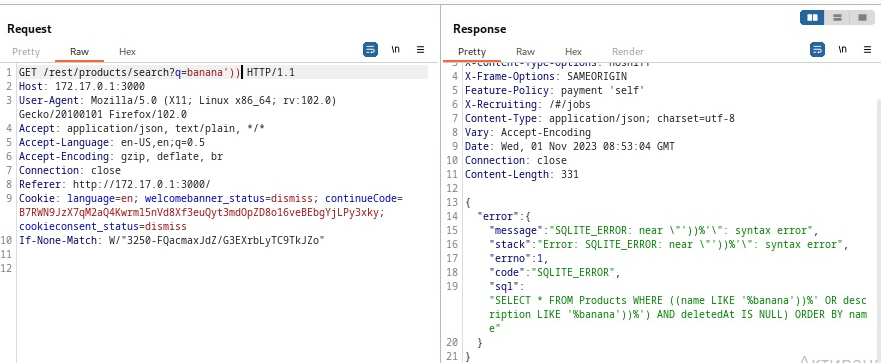
Мы получаем сообщение об ошибке, в котором говорится, что необходимо добавить одинаковое количество столбцов. Это означает, что нам нужно начать перебор количества столбцов. Подбираем значение 9.

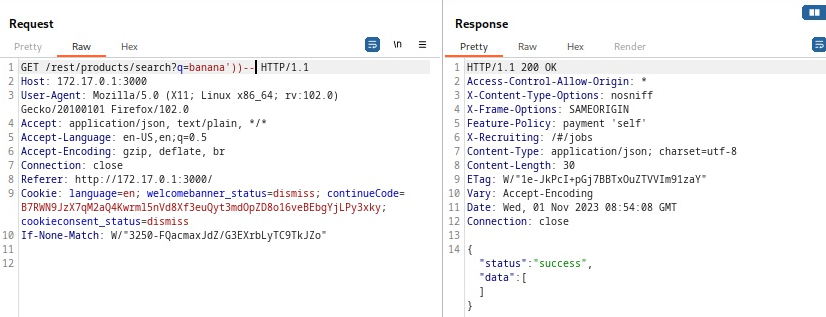


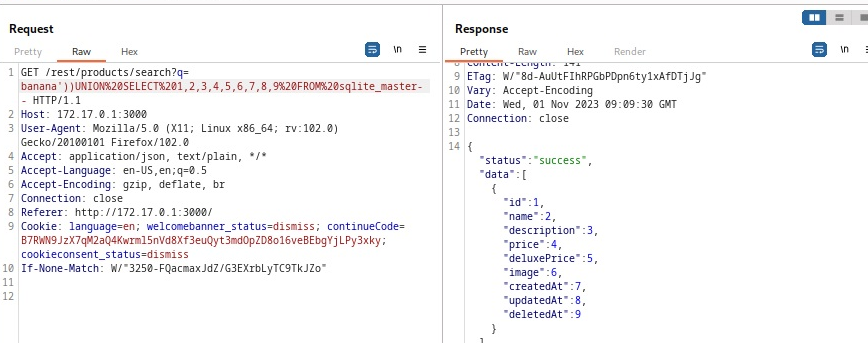


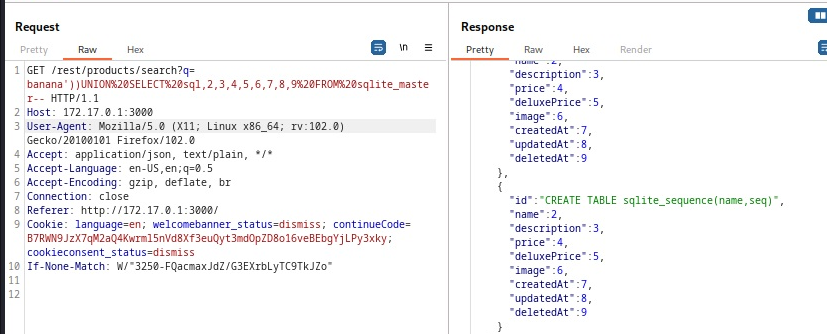








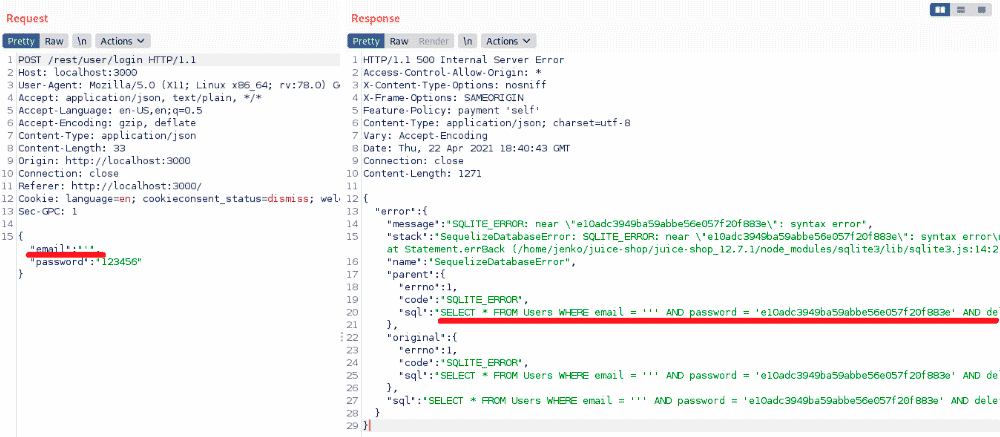


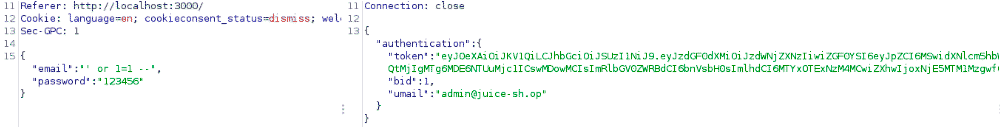


- login admin:

Для воспроизведения уязвимости необходимо в форме авторизации ввести какие-либо данные в полях e-mail и password. Далее через BurpSuite находим необходимые поля (email в частности) и запрос перебрасываем в Repeater. Находим интересующий нас sql-запрос с нужным полем email, подставляем значение и пробуем провести атаку.

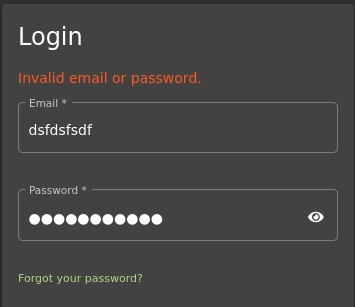


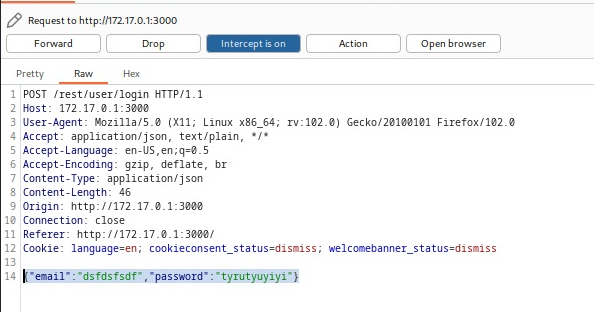


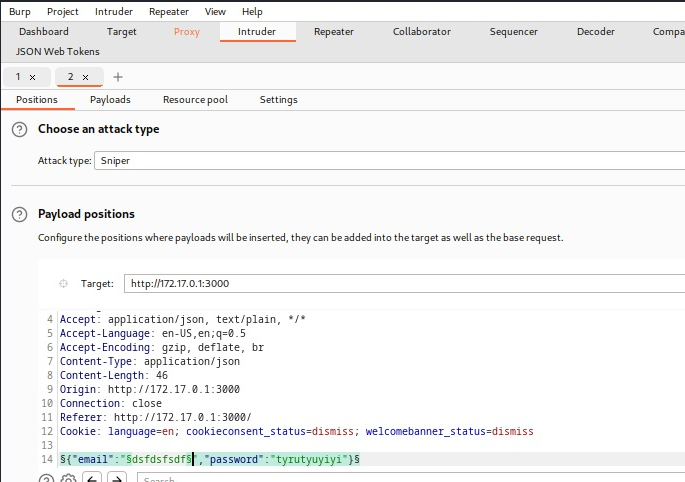


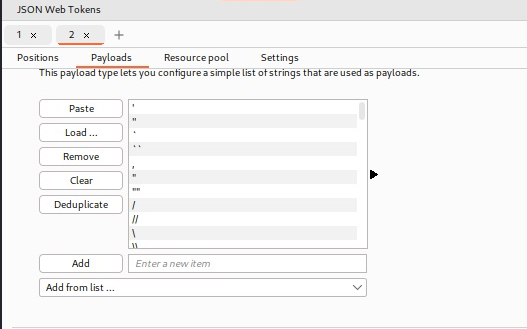
- нарушение аутентификации:

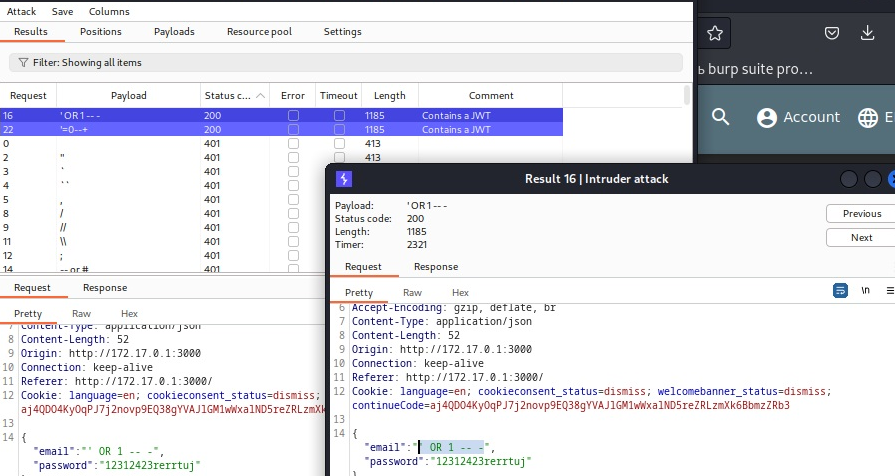
В форме ввода учетных данных осуществляем ввод произвольных символов. Для понимания, что происходит запускаем BurpSuite, перехватываем полученный запрос и осуществляем атаку из загруженного словаря.











1. **Рекомендации по устранению уязвимостей**

Для устранения уязвимостей в Juice Shop, связанных с инъекциями (Injection) и нарушением аутентификации (Broken Authentication), можно придерживаться следующих правил и рекомендаций:

- использование параметризованных запросов для работы с базой данных (вместо конкатенации строк для формирования SQL запроса использовать подстановку параметров);

- проверка пользовательского ввода на наличие недопустимых символов;

- проведение регулярных обновлений библиотек и фреймворков для получения последних исправлений уязвимостей.

При нарушении аутентификации (Broken Authentication):

- установка сложных паролей (должны быть длинные пароли, содержащие буквы, цифры и специальные символы);

- использование двухфакторная аутентификация (2FA);

- блокировка учетных записей (автоматическая блокировка учетных записей после нескольких неудачных попыток входа);

- использование безопасных методы хранения и передачи сессионной информации, такие как HTTPS и использование безопасных куки;

- регулярное обновление паролей;

- проводить мониторинг активности пользователей для выявления подозрительных действий.