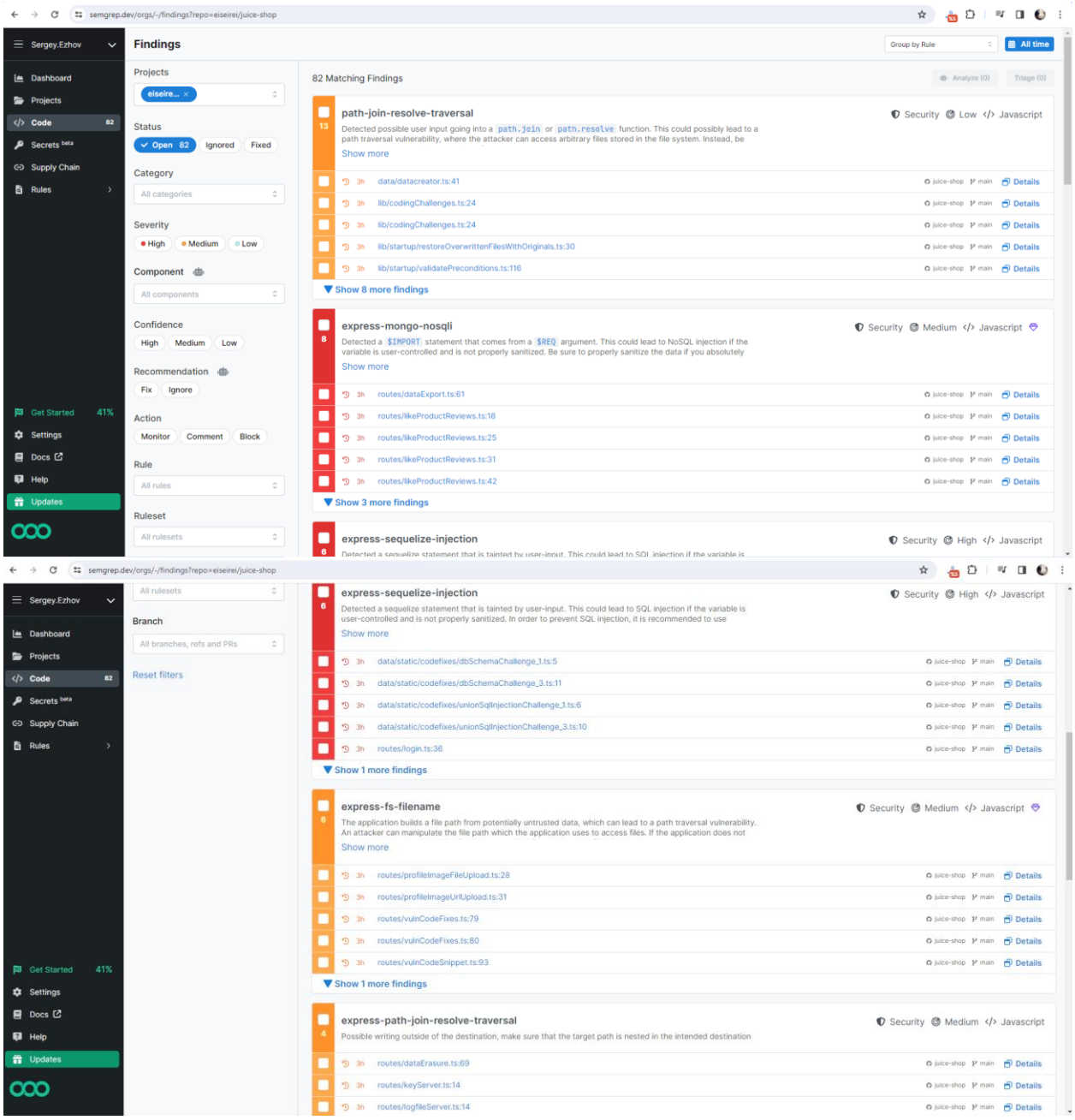
Отчёт по анализу защищённости Juice Shop

Введение

OWASP Juice Shop — это веб-приложение с открытым исходным кодом для демонстрации самых распространенных уязвимостей. Поддерживается некоммерческой организацией Open Web Application Security Project (OWASP) и волонтерами.

Результаты статического анализа

Проведём статический анализ кода приложения – SAST. Будем использовать бесплатный облачный инструмент Semgrep. Для этого предварительно поместим исходный код приложения на платформе GitHub. После этого запустим сканирование. Результаты сканирования:

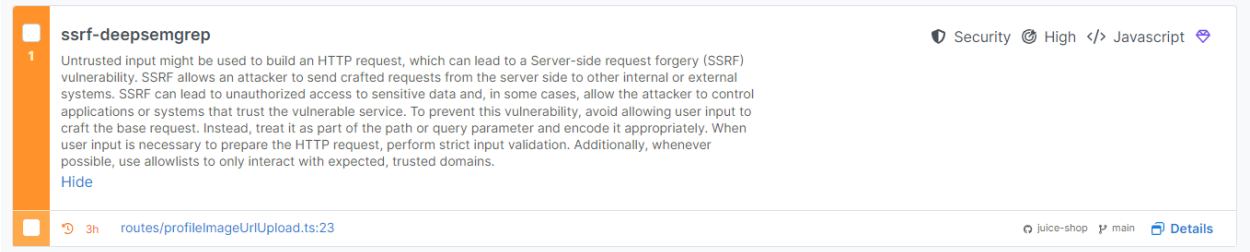


Обнаруженные уязвимости из OWASP Top-10

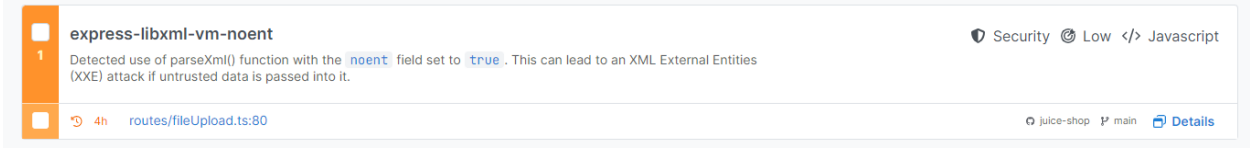
В результатах статистического анализа кода приложения Juice Shop мы обнаружили следующие уязвимости:

1. CWE-22: Path Traversal (OWASP Broken Access Control)

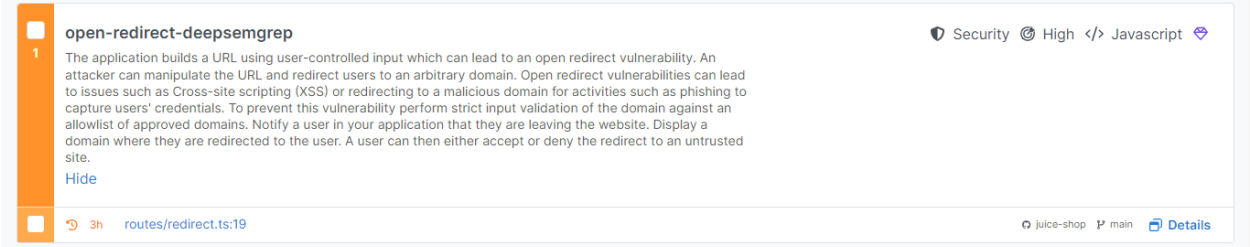
2. CWE-918: Server-Side Request Forgery (OWASP Broken Access Control)



3. CWE-611: XML External Entities (OWASP Security Misconfiguration)



4. CWE-79: Cross-site Scripting (OWASP Injection)



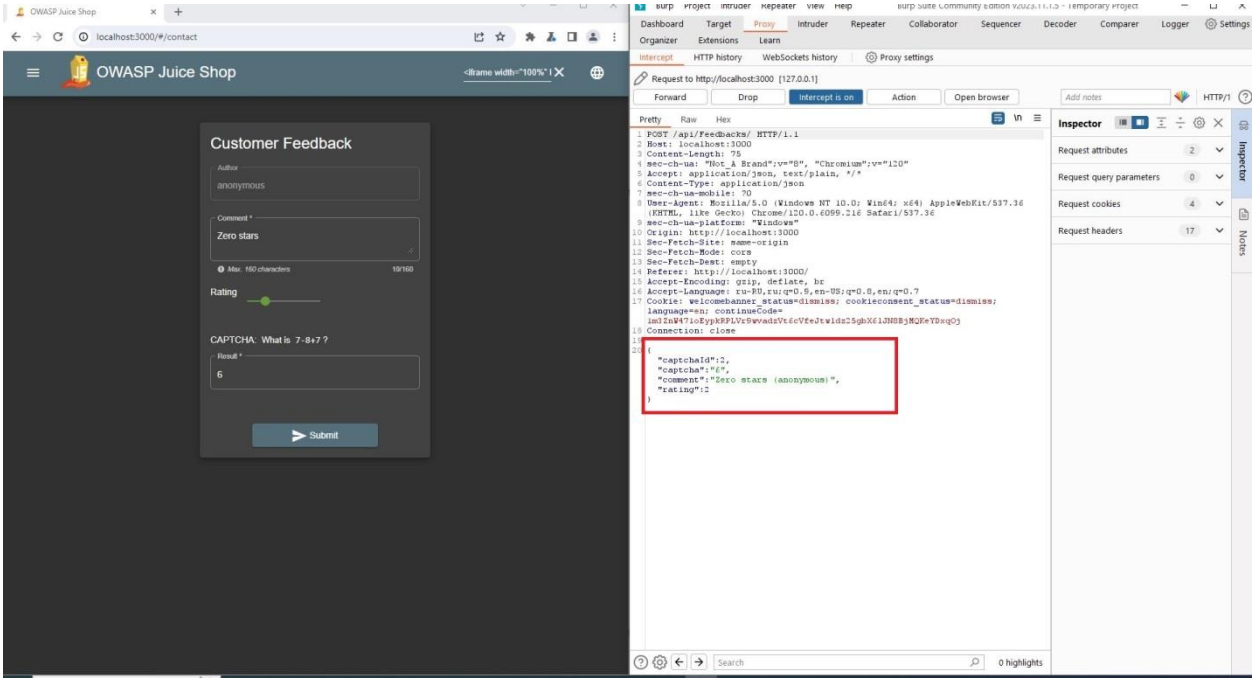
5. CWE-89: SQL Injection (OWASP Injection)

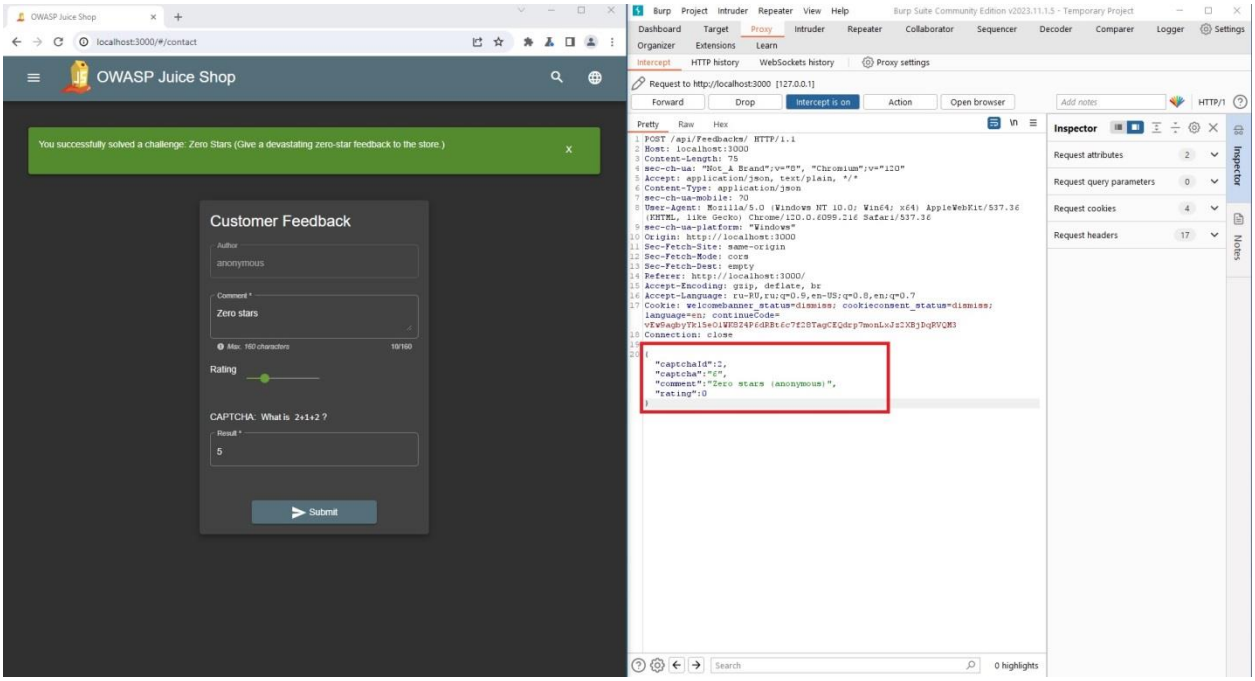
Эксплуатация уязвимостей из OWASP Top-10

Покажем, как можно эксплуатировать найденные уязвимости в приложении Juice Shop:

1. CWE-20: Improper Input Validation (OWASP Injection)

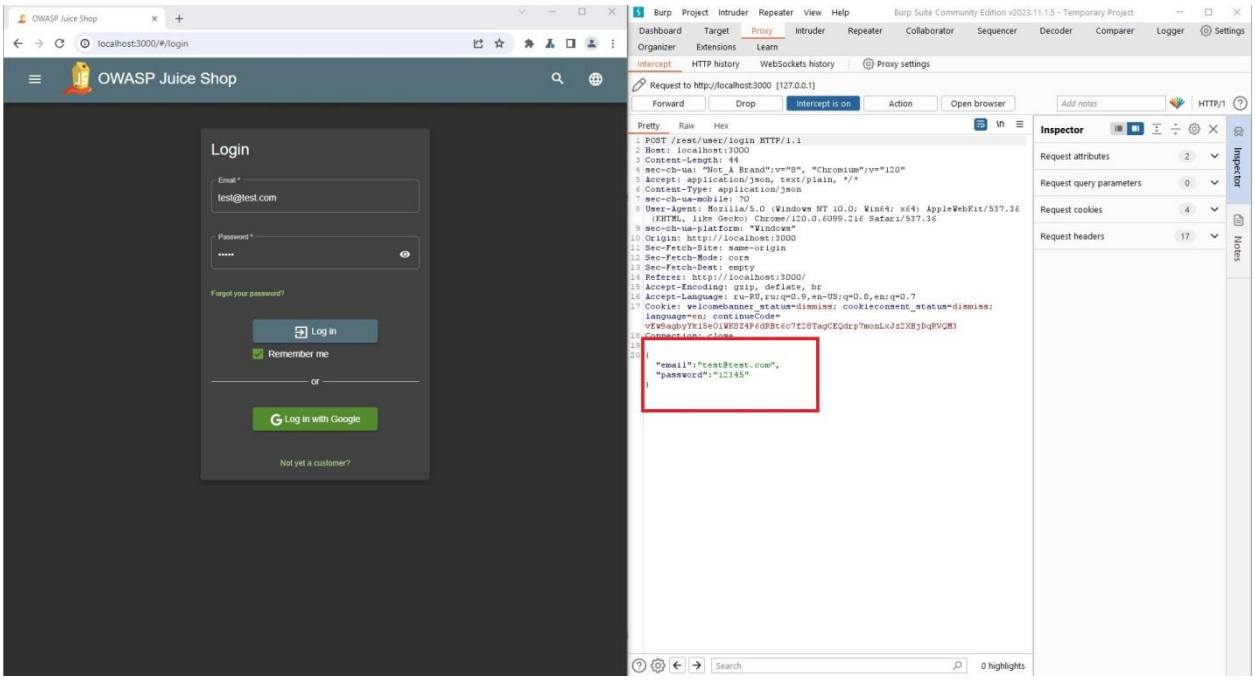
Заходим на страницу для отправки отзывов (http://localhost:3000/#/contact), где пишем текст и решаем задачу для капчи. Количество звёзд ставим любое. После чего включаем перехват запросов в Burp Suite. В перехваченном запросе нам надо поменять значение "rating" на цифру 0. После чего отправить изменённый запрос.

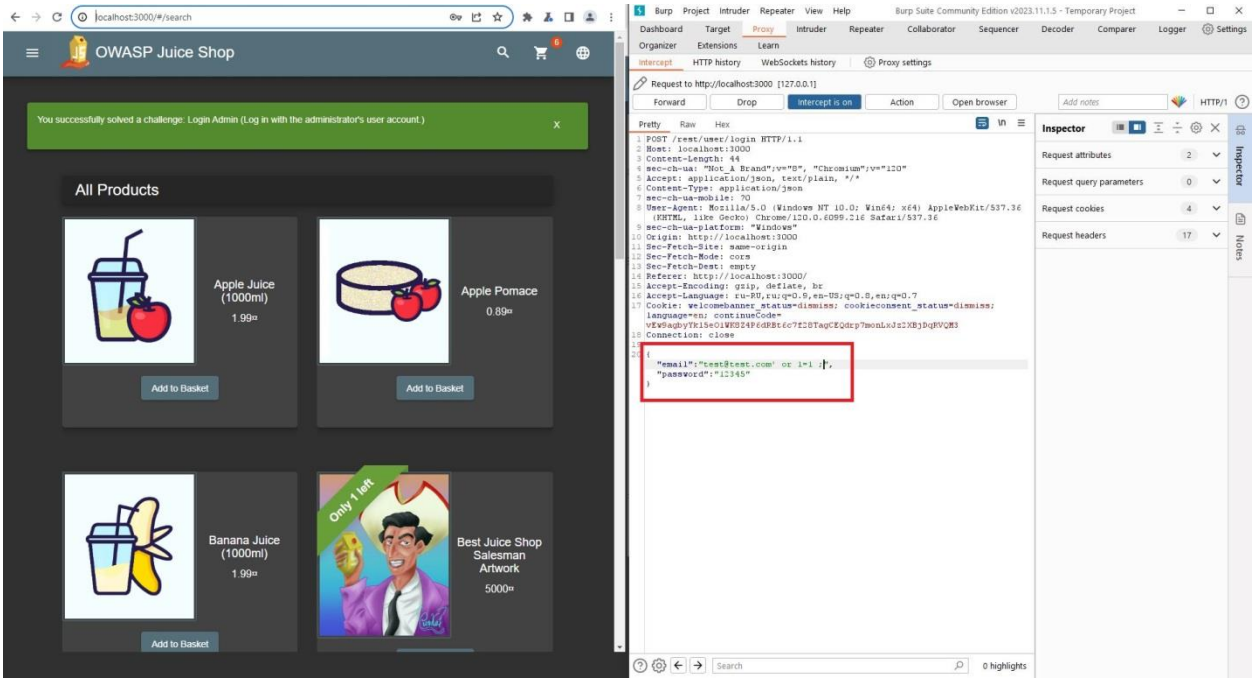




2. CWE-89: SQL Injection (OWASP Injection)

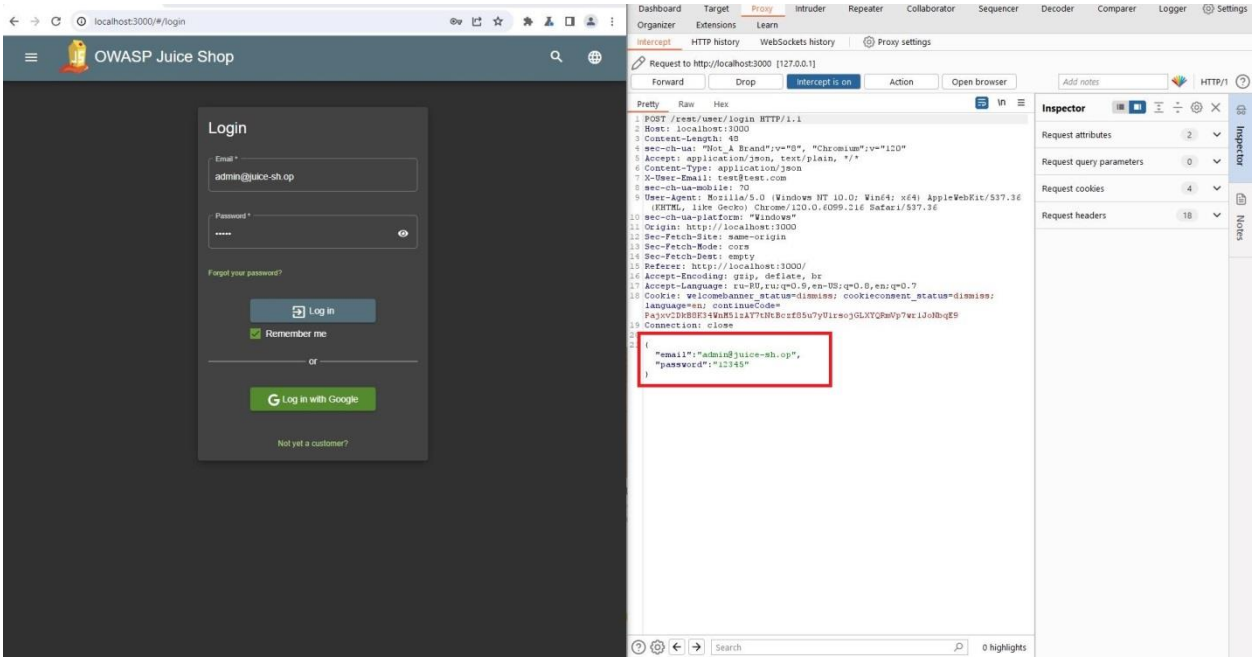
Заходим на страницу авторизации (http://localhost:3000/#/login), где указываем любой адрес почты и пароль. После чего включаем перехват запросов в Burp Suite. В перехваченном запросе нам надо дописать в значение "email" следующие символы "email' or 1=1 ;". После чего отправить изменённый запрос.

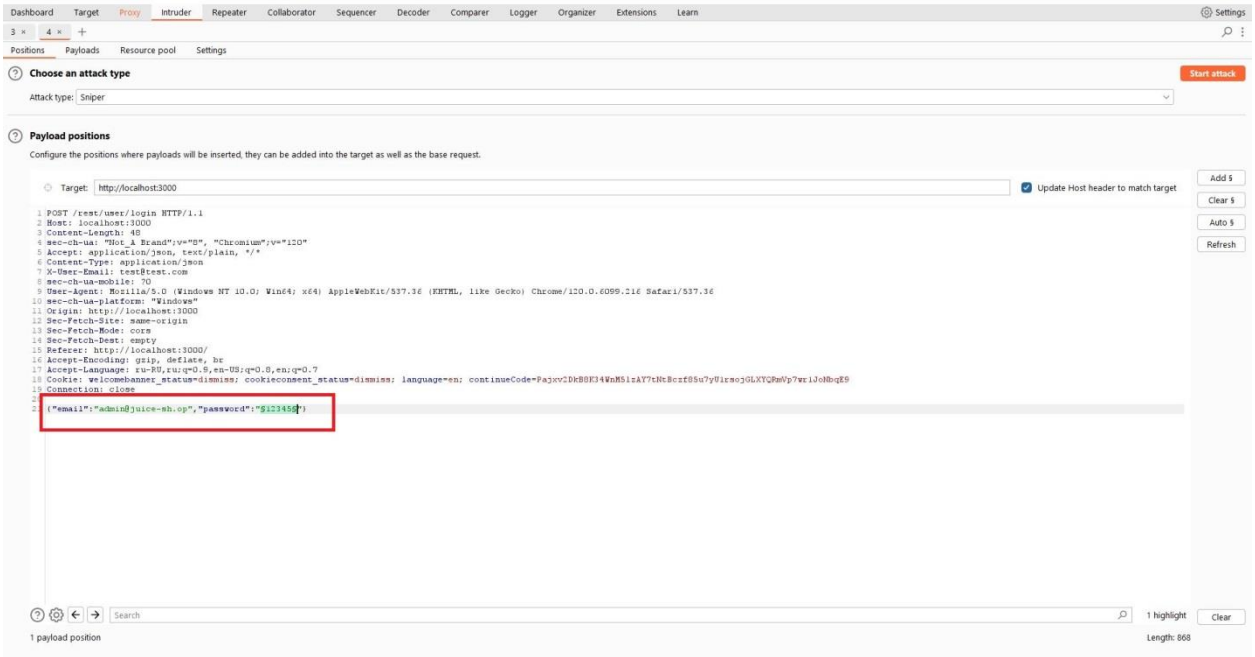


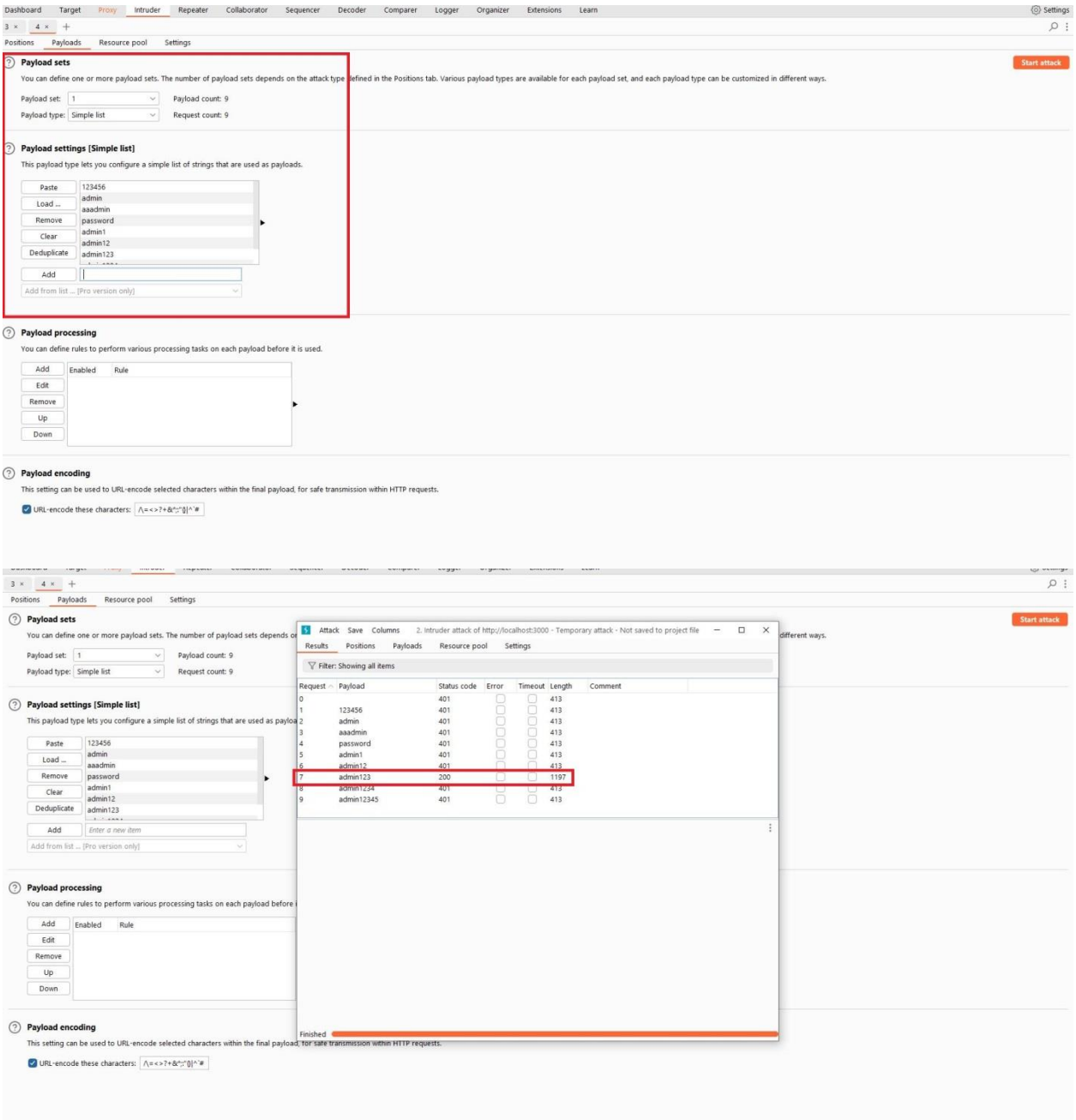


3. CWE-307: Improper Restriction of Excessive Authentication Attempts (OWASP Identification and Authentication Failures)

Теперь попробуем подобрать пароль администратора, зная его электронную почту admin@juice-sh.op. Также заходим на страницу авторизации (http://localhost:3000/#/login), где указываем почту администратора и любой пароль. После чего включаем перехват запросов в Burp Suite. Передаём перехваченный запрос в Intruder. Так указываем, что значение "password" будет переменной, которую мы будем перебирать. Настраиваем полезную нагрузку, указывая возможные варианты паролей для перебора. После этого запускаем атаку перебора. Смотрим успешный ответ с заголовком 200. Видно, что успешный ответ на пароль admin123.







Рекомендации по устранению уязвимостей из OWASP Top-10

Рекомендации по устранению к трём продемонстрированным уязвимостям:

1. CWE-20: Improper Input Validation (OWASP Injection)

Для защиты от этой атаки необходима дополнительная проверка отправляемых данных на стороне сервера. Даже если злоумышленник подменит значения, генерируемые формой, то логика на стороне сервера не даст вставить «некорректные» данные.

2. CWE-89: SQL Injection (OWASP Injection)

Для защиты от этой атаки необходимо дополнительно экранировать передаваемые данные, чтобы помещать злоумышленнику внедрять управляющие символы SQL в обычные данные. Это помещает выполнению вредоносной команды, и она будет обработана как текстовые данные.

3. CWE-307: Improper Restriction of Excessive Authentication Attempts (OWASP Identification and Authentication Failures)

Для защиты от этой атаки необходимо предусмотреть временной лимит между отправками запросом на авторизацию и блокировки учётной записи на некоторое время при нескольких неудачных попытках подряд. Ещё можно обезопасить форму авторизации, добавив капчу, что усложнит перебор.