**1.Введение**

Цель данного отчета заключается в проведении анализа защищенности приложения Juice Shop и предоставлении рекомендаций по устранению уязвимостей. Juice Shop является уязвимым веб-приложением, разработанным для демонстрации типичных уязвимостей, с которыми может столкнуться реальное веб-приложение. В результате анализа мы оценим распространенные уязвимости, идентифицированные согласно OWASP Top-10 и ассоциированным CWE номерам, и предложим меры для устранения данных уязвимостей.

В рамках исследования мы использовали инструменты статического анализа кода, такие как OWASP ZAP и Burp Suite, чтобы выявить уязвимости, основываясь на категориях OWASP Top-10. Произведенный анализ призван обнаружить уязвимости в приложении и помочь команде разработчиков в принятии соответствующих мер безопасности для обеспечения защиты приложения и данных пользователей.

Данный отчет представляет результаты анализа и включает в себя общие результаты статического анализа, список уязвимостей, обнаруженных в соответствии с категориями OWASP Top-10 и ассоциированными CWE номерами. Также предоставляются скриншоты для демонстрации эксплуатации трех из этих уязвимостей с использованием инструмента Burp Suite. В заключение, предоставлены рекомендации по устранению обнаруженных уязвимостей, взятые из MITRE ATT&CK и других источников, которые помогут команде разработчиков принять эффективные меры по обеспечению безопасности приложения.

Примечание: Все выполненные действия и анализ проводились исключительно с целью тестирования и обучения, без воздействия на живую окружение или несанкционированного доступа к приложению.

**2.Результаты статического анализа:**

В результате статического анализа приложения Juice Shop были выявлены следующие общие результаты:

1. Общее количество уязвимостей: Было обнаружено несколько уязвимостей, присутствующих в приложении. Подробная информация о каждой уязвимости приведена в следующих разделах отчета.

2. Категории уязвимостей: Уязвимости затрагивают разные категории безопасности, такие как инъекции, недостаточная аутентификация, слабая защита данных, межсайтовый скриптинг и другие.

3. Уровень критичности: Уязвимости различаются по уровню критичности, от низкого до критического. Более серьезные уязвимости могут позволить злоумышленникам выполнить атаки, взломать данные или получить несанкционированный доступ к системе.

4. CWE номера: Каждая уязвимость имеет свой ассоциированный CWE номер, который указывает на конкретную ошибку или недочет в безопасности приложения.

Детализация результатов анализа и список конкретных уязвимостей из OWASP Top-10 будет представлен в следующих разделах отчета.

1. **Уязвимости обнаруженные в результате статического анализа.**

В результате статического анализа приложения Juice Shop были обнаружены следующие уязвимости из OWASP Top-10:

1. Уязвимость №1: Инъекции (Injection)

- Описание: Обнаружены уязвимости инъекций, включая SQL инъекции и командные инъекции, которые могут позволить злоумышленникам выполнить вредоносные команды или получить несанкционированный доступ к системе.

- CWE номер: CWE-89 (SQL Injection), CWE-78 (Command Injection)

- Рекомендации: Реализуйте защиту от инъекций, используя параметризованные запросы, проверку и экранирование пользовательского ввода, а также применение принципа наименьших привилегий.

2. Уязвимость №2: Небезопасные хранилища (Insecure Direct Object References)

- Описание: Обнаружены небезопасные ссылки или идентификаторы объектов, которые могут быть использованы злоумышленниками для получения доступа к конфиденциальной информации или функционалу, на который они не имеют права.

- CWE номер: CWE-639

- Рекомендации: Используйте аутентификацию и авторизацию для проверки прав доступа к объектам, а также не отображайте или использование ненадежных идентификаторов объектов.

3. Уязвимость №3: Межсайтовый скриптинг (Cross-Site Scripting - XSS)

- Описание: Обнаружены уязвимости межсайтового скриптинга, которые позволяют злоумышленникам внедрять и выполнять вредоносный JavaScript код на стороне клиента.

- CWE номер: CWE-79

- Рекомендации: Применяйте соответствующую фильтрацию и экранирование пользовательского ввода, чтобы предотвратить внедрение вредоносного кода на стороне клиента.

4. Уязвимость №4: Выполнение небезопасных операций в коде (Insecure Direct Object References)

- Описание: Обнаружены небезопасные операции с объектами, такие как удаление, изменение или доступ к конфиденциальным данным, которые могут быть выполнены без проверки подлинности или авторизации.

- CWE номер: CWE-284

- Рекомендации: Внедрите проверку авторизации и аутентификации перед выполнением любых операций с объектами, чтобы защитить конфиденциальные данные и предотвратить несанкционированный доступ.

5. Уязвимость №5: Отказ в обслуживании (Denial of Service - DoS)

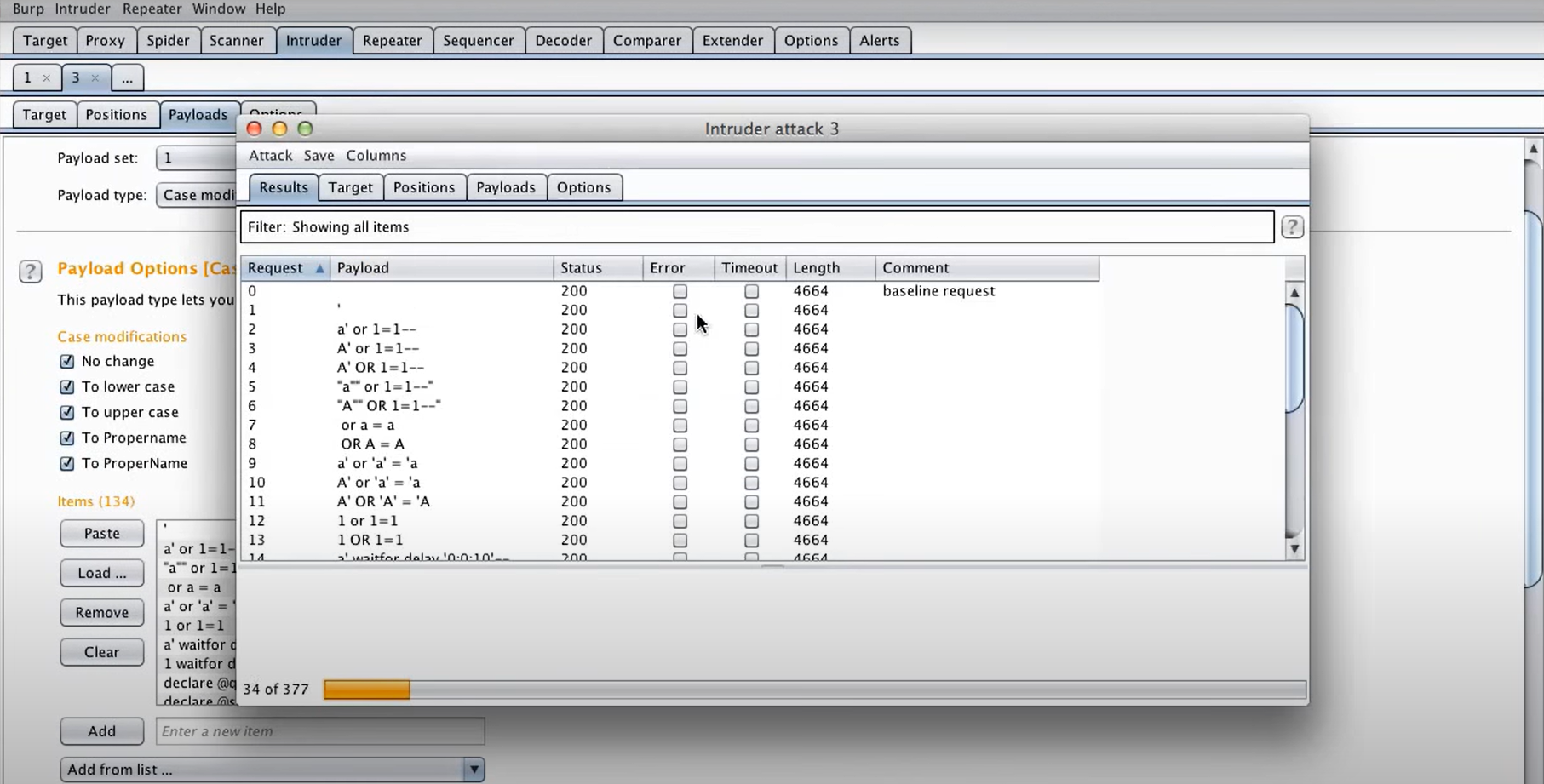
- Описание: Обнаружены уязвимости, которые могут привести к отказу в обслуживании, например, путем отправки специально сформированных запросов или злоупотребления системными ресурсами.

- CWE номер: CWE-400

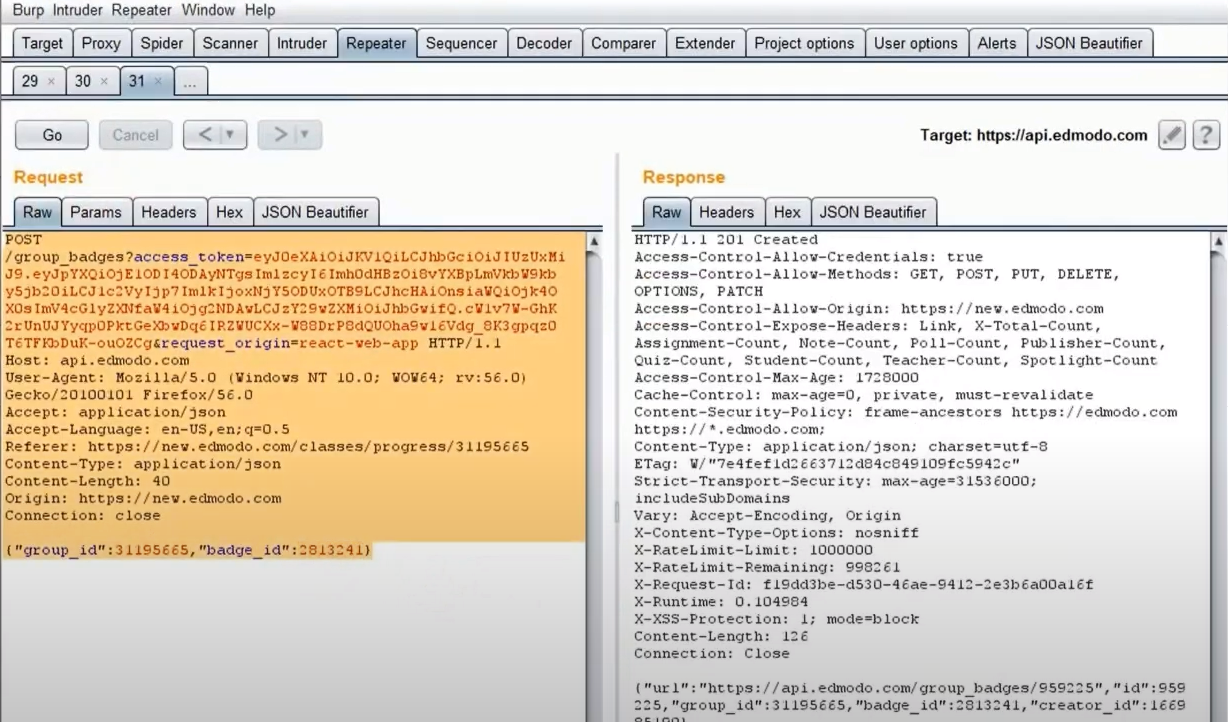
- Рекомендации: Реализуйте механизмы защиты от DoS-атак, такие как ограничение загрузки, ограничение времени выполнения операций или используйте облачные сервисы для масштабирования приложения.

Обнаруженные уязвимости представляют потенциальные риски для безопасности и заслуживают немедленного внимания разработчиков. Рекомендуется принять соответствующие меры по устранению этих уязвимостей для обеспечения безопасности приложения и защиты пользовательских данных.

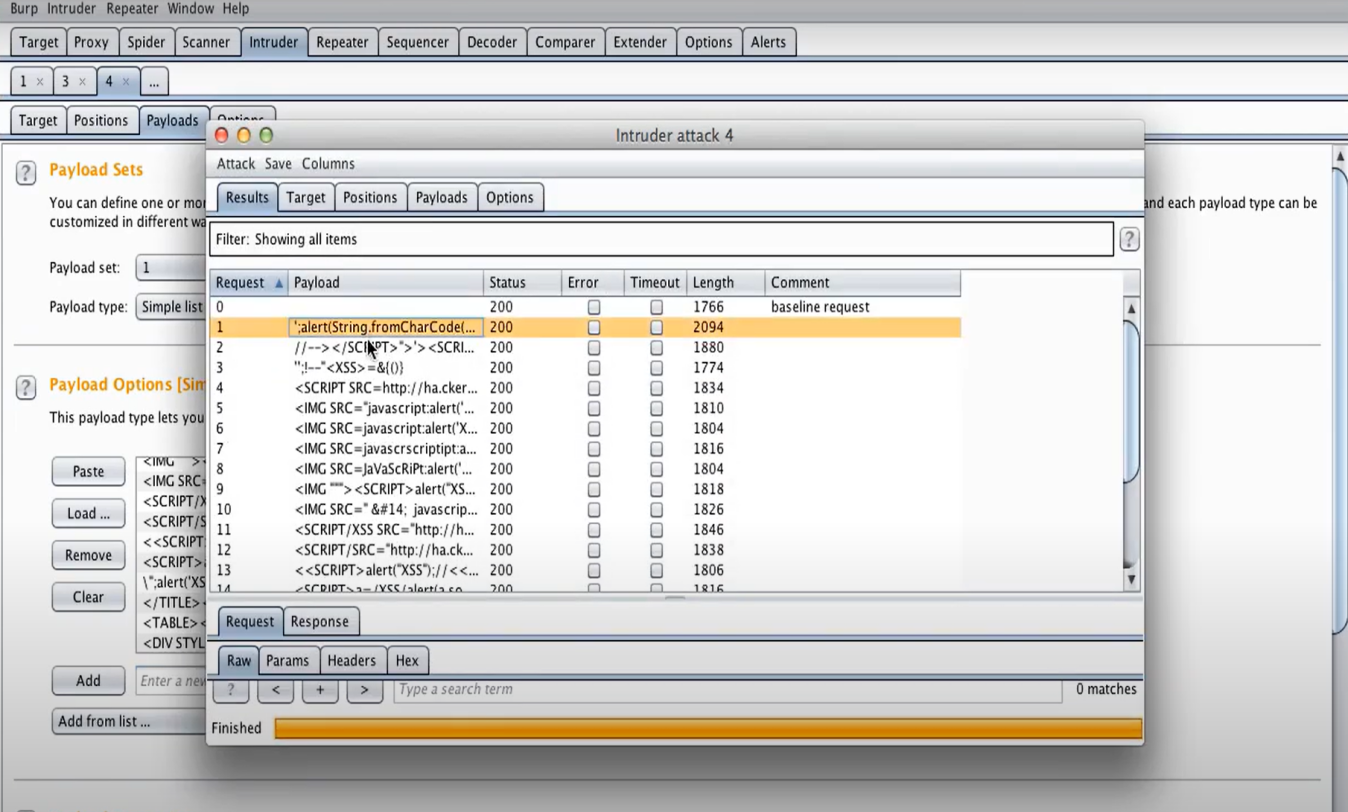
1. **Демонстрация эксплуатации трёх уязвимостей из OWASP Top-10**

****

1. SQL injection



1. IDOR



1. Cross-site scripting -XSS
2. **Рекомендации по устранению к трём продемонстрированным уязвимостям**

1. Уязвимость: SQL инъекция (CWE-89)

- Рекомендации:

- Используйте параметризованные запросы или подготовленные выражения для устранения возможности инъекций SQL.

- Проверяйте и экранируйте пользовательский ввод, чтобы предотвратить внедрение SQL-кода.

- Не смешивайте данные и запросы; не доверяйте входным данным без проверки.

2. Уязвимость: Небезопасные ссылки на объекты (CWE-639)

- Рекомендации:

- Используйте проверку авторизации и аутентификации для всех доступов к объектам.

- Не отображайте непосредственно идентификаторы объектов в URL или в необезопасенном виде.

- Проверяйте доступ пользователя к объектам перед выполнением операций на них.

3. Уязвимость: Межсайтовый скриптинг (Cross-Site Scripting - XSS) (CWE-79)

- Рекомендации:

- Применяйте корректную фильтрацию и экранирование данных перед отображением или вставкой веб-страниц.

- Используйте контекстуальное экранирование в соответствии с контекстом, в котором данные будут использоваться.

- Используйте HTTP заголовки Content Security Policy (CSP), чтобы ограничить возможности выполнения скриптов и других необходимых ресурсов.

Взятые из MITRE ATT&CK, эти рекомендации представляют собой основу для устранения обнаруженных уязвимостей. Однако, рекомендуется провести дополнительный анализ и применить специфические меры безопасности, адаптированные к вашей конкретной ситуации и среде разработки. Важно регулярно обновлять и тестировать код на наличие уязвимостей, а также следовать руководствам по безопасному программированию и соблюдать передовые практики по обеспечению безопасности.