Digital Security

БЕЗОПАСНОСТЬ КАК ИСКУССТВО

ЭКСПЕРТНОЕ ЗАКЛЮЧЕНИЕ

по результатам проведения анализа защищённости
сайта bcwallet.io, принадлежащего компании «Blockchain.ru»

Даты проведения работ:
7.02.18 - 16.02.18

Технический менеджер проекта:
А.О. Перцев
Директор департамента аудита:
А.Н. Тюрин

1. Введение

1.1. Общие положения

В настоящем экспертном заключении представлены результаты проведения работ по анализу защищенности сайта bcwallet.io (далее – Система), принадлежащего «Blockchain.ru» (далее – Компания), а также предложены рекомендации по устранению выявленных проблем и повышению уровня защищенности.

1.2. Принятые сокращения

Таблица 1.2–1. Принятые сокращения

Сокращение	Расшифровка
ИБ	Информационная безопасность
ИС	Информационная система
КИС	Корпоративная информационная сеть
МЭ	Межсетевой экран

1.3. Резюме

В соответствии с договором ДСС-КУ-2018/03 специалистами компании «Digital Security» в период с 7.02.18 по 16.02.18 были проведены работы по анализу защищенности сайта bcwallet.io.

Была рассмотрена модель внешнего нарушителя без знаний о Системе.

Проведенные работы показали, что:

1. Имеющийся уровень безопасности Системы можно определить как «высокий».

Основными рекомендациями являются:

1. Устранение выявленных уязвимостей и слабостей Системы.

Далее содержатся подробности и описание выявленных недостатков и связанных с ними рисков информационной безопасности, а также детальные рекомендации по устранению слабостей.

1.4. Область проводимых работ

В область проведения работ по анализу защищенности вошли ресурсы ЛВС Заказчика, включая основные важные бизнес-системы, перечисленные в Таблице 1.4:

Таблица 1.4. Перечень хостов Компании для анализа защищённости

№ п/п	Имя хоста/IP-адрес
1	bcwallet.io

2. Принципы проведения работ

2.1. Угрозы ИБ

На информационные ресурсы Компании могут действовать следующие три угрозы ИБ: угрозы нарушения конфиденциальности, целостности и доступности.

Угроза нарушения конфиденциальности направлена на разглашение информации, имеющей в Компании статус конфиденциальной. При реализации угрозы информация становится известной лицам, которые не должны иметь к ней доступ – ряду сотрудников Компании, клиентам, партнерам, конкурентам, третьим лицам.

Угроза нарушения целостности направлена на модификацию или искажение информации, приводящее к изменению ее структуры или смысла, полному или частичному уничтожению.

Угроза нарушения доступности (угроза отказа в обслуживании) заключается в невозможности получения доступа к информационному ресурсу пользователями информационной системы.

Основным принципом проведения аудита ИБ является проверка возможности реализации указанных угроз, воздействующих на информационные ресурсы Системы, в рамках заданной модели нарушителя.

2.2. Модель нарушителя

В качестве вероятного нарушителя информационной безопасности Системы Компании рассматривается лицо или группа лиц, состоящих или не состоящих в сговоре, которые в результате умышленных или неумышленных действий потенциально могут реализовать угрозы ИБ, осуществить посягательства на информационные ресурсы Системы и нанести ущерб интересам Компании.

В качестве угроз ИБ рассматриваются базовые угрозы нарушения конфиденциальности и целостности информации, а также угроза отказа Системы в обслуживании клиентов Компании.

Умышленно действующий нарушитель может преследовать следующие цели (а также их всевозможные комбинации):

- злонамеренный вызов отказа в обслуживании;
- повышение собственных привилегий;
- несанкционированный доступ к критичной с точки зрения бизнеса информации.

В ходе работы была использована модель внешнего нарушителя.

2.2.1. Внешний нарушитель

При проведении теста на проникновение используются следующие модели внешнего нарушителя:

- внешний нарушитель из сети, не обладающий знаниями о тестируемой Системе и правами в ней.

3. Сценарии атак

3.1. MiTM-атака на пользователя

При использовании слабости 4.2.1. злоумышленник может проводить MiTM-атаку (атака “человек посередине”). Злоумышленник может принудительно заставить браузер пользователя передавать данные через незащищенное соединение (downgrade-атака). При этом необходимо, чтобы злоумышленник и жертва находились в одной сети, например, публичный Wi-Fi. Далее злоумышленник может подменить в ответах от сервера адрес настоящего кошелька на адрес подконтрольного ему, в результате чего жертва может перевести криптовалюту на адрес злоумышленника.

3.2. Восстановление чужой учетной записи

С помощью уязвимости 4.1.1. атакующий может сгенерировать большое количество кодов для восстановления и попытаться совершить атаку перебором. В случае успеха злоумышленник завладеет аккаунтом пользователя.

4. Внешний аудит Системы

4.1. Перечень обнаруженных уязвимостей

4.1.1. Недостаточное количество бит энтропии в токене

Критичность: высокая
Вероятность эксплуатации: низкая
Итоговый риск: средний

Описание:

Приложение генерирует уникальные токены для подтверждения пользователем критичных действий. Однако генерируемый токен недостаточно случайный.

Риск:

При некоторых обстоятельствах атакующий может успешно подобрать токен и выполнить критичное для Системы действие.

Уязвимый ресурс:

- bcwallet.io

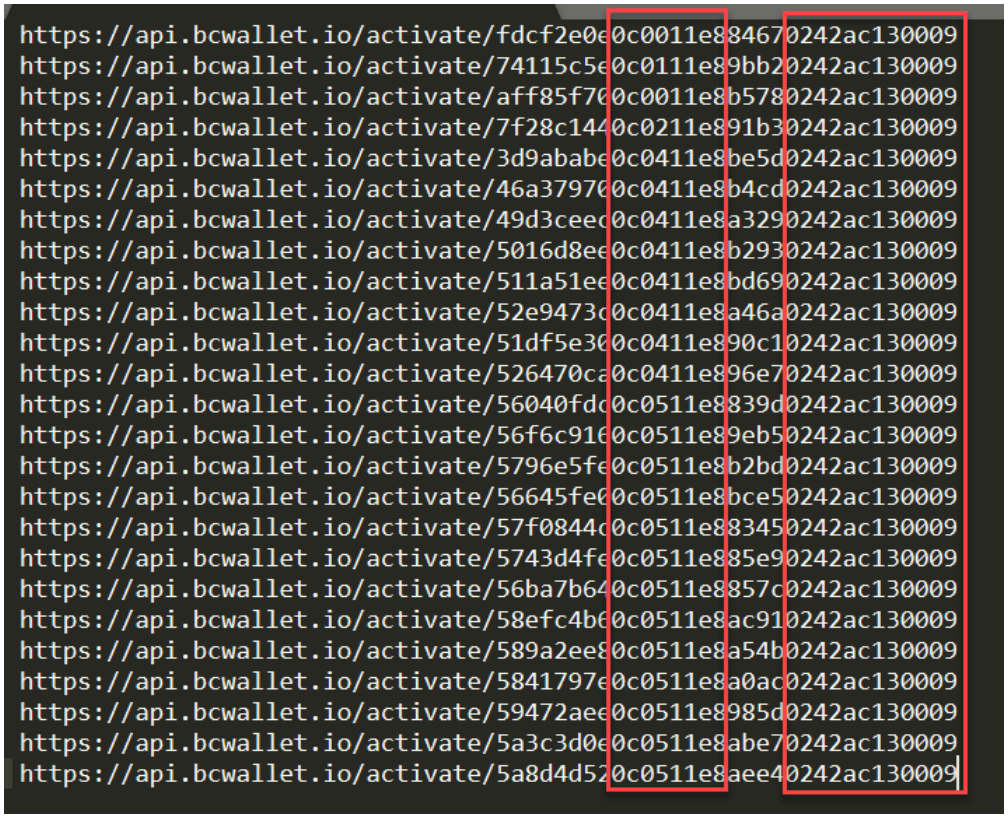
Технические детали:

При восстановлении пароля на указанную почту приходит письмо со ссылкой, содержащей уникальный токен. Количество уникальных байт в токене ≤ 6. Учитывая тот факт, что количество запросов токена на почту жертвы неограниченно, злоумышленник может существенно сократить время перебора.

Рекомендации:

- Увеличить количество бит энтропии в токене.

Рис 4.1.1 – 1. Ссылки для восстановления пароля аккаунта



4.1.2. Некорректное управление сессией

Критичность: средняя
Вероятность эксплуатации: низкая
Итоговый риск: низкий

Описание:

В случае раскрытия идентификатора сессии злоумышленник может неограниченно получать доступ в личный кабинет пользователя.

Риск:

Обладание идентификатором сессии, выданным пользователю при аутентификации, позволяет осуществлять доступ к личной информации после того, как пользователь совершил выход (!) из личного кабинета.

Уязвимый ресурс:

- bcwallet.io

Технические детали:

refresh_token и access_token действительны после осуществления logout.

Рекомендации:

- Удалять сессию пользователя как при истечении определенного времени, так при нажатии им кнопки logout.

4.2. Перечень обнаруженных слабостей

4.2.1. Отсутствие механизма HSTS

Описание:

Злоумышленник может произвести downgrade-атаку, тем самым заставив пользователя использовать незащищенное соединение с web-приложением. В результате этого атакующий сможет активно перехватывать данные, которые пользователь передает web-приложению, например, пароли или cookies.

Риск:

В web-приложении отсутствует механизм HSTS, который позволяет защититься от ряда атак, связанных с активным перехватом трафика.

Уязвимый ресурс:

- bcwallet.io

Технические детали:

Механизм HSTS (HTTP Strict Transport Security) заставляет браузер по умолчанию использовать защищенное TLS-соединение с web-приложением, что значительно усложняет злоумышленнику проведение MiTM-атак (атаки "человек посередине").

Рекомендации:

- Внедрить механизм HSTS. Необходимо добавить в ответ сервера заголовок Strict-Transport-Security: max-age=%срок действия%.

4.2.2. Отсутствие защиты от атак типа clickjacking

Описание:

Web-сервер не использует параметры X-Frame-Options в заголовках ответов web-сервера.

Риск:

Сайт Системы, загруженный во фрейме на стороннем ресурсе злоумышленника, может быть использован для осуществления фишинговых и кликджекинговых атак на пользователей и манипуляций с Системой без их ведома. Например, пользователь будет находиться на сайте злоумышленника и выполнять там какие-то действия (клики мышью, набор текста), при этом сами действия будут отправляться и обрабатываться в Системе, а не сайте злоумышленника (за счёт отображения сайта и Системы на различных слоях).

Уязвимый ресурс:

- bcwallet.io

Технические детали:

X-Frame-Options позволяет определить политику загрузки сайта во фреймы на сторонних ресурсах. Заголовок X-Frame-Options отсутствует в заголовках ответов web-сервера. Возможность атаки сильно зависит от функционала. Защиту следует внедрять, как минимум, для критичных поддоменов/разделов сайта.

Следует отметить, что в данной версии Системы отсутствует функциональность, которую необходимо было бы защищать таким образом. Однако если планируется дальнейшее развитие сайта с внедрением регистрации пользователей и личным кабинетом, то данный заголовок поможет защититься от clickjacking-атак в будущем, в случае, если появится функционал, который можно будет таким образом атаковать.

Рекомендации:

- Добавить во все заголовки ответов от web-сервера заголовок X-Frame-Options со значением ”DENY” или ”SAMEORIGIN”.

4.2.3. Небезопасная конфигурация CORS

Описание:

Злоумышленник может получить доступ к чувствительной информации пользователя.

Риск:

Неправильная конфигурация web-сервера, с включенным механизмом междоменного взаимодействия сайтов CORS (Cross-Origin Resource Sharing), позволяющая получить чувствительную информацию пользователей сайта.

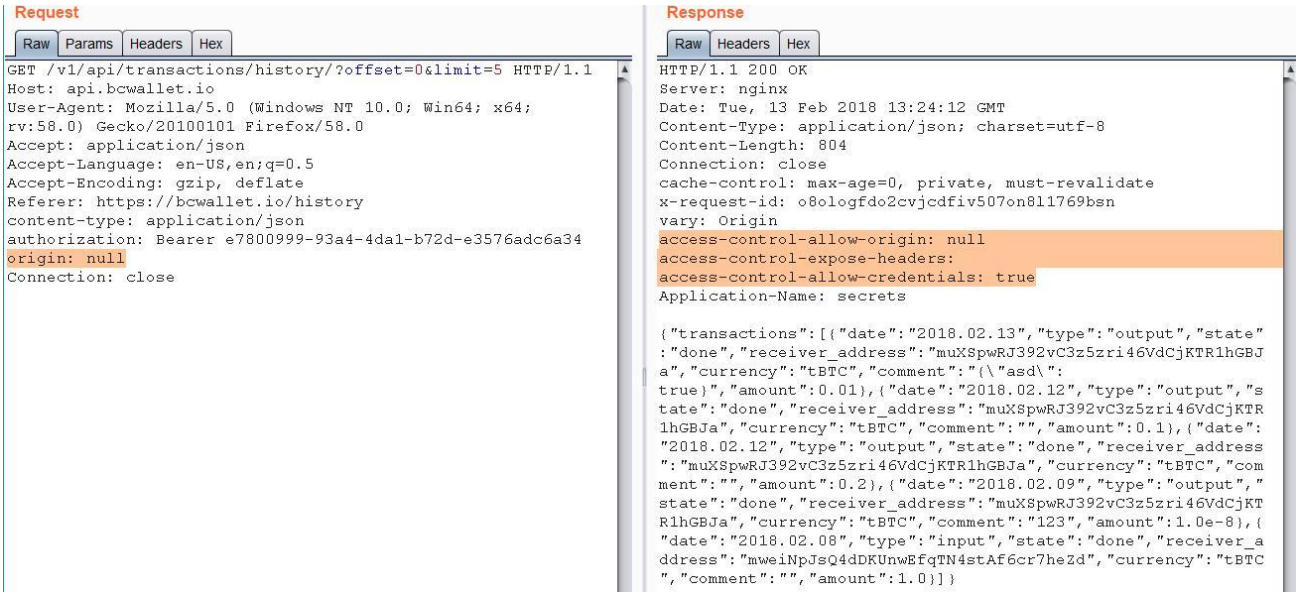
Уязвимый ресурс:

- *.bcwallet.io

Технические детали:

На любой домен (отличный от https://bcwallet.io) в заголовке Origin сервер возвращает null. В связке с заголовком access-control-allow-credentials: true это даёт атакующему потенциальную возможность кроссдоменного чтения чувствительной информации пользователя.

Рис 4.2.3 – 1. Пример получения данных пользователя с Origin, равного null



В данном случае такое поведение не является уязвимостью, так как для авторизации пользователя используется не Cookie, а заголовок Authorization.

Рекомендации:

- Настроить белый список доменов, с которых возможно обращение к целевому домену, и проверять вхождение значения заголовка Origin в этот список.
- Удалить заголовки access-control-allow-credentials и access-control-expose-headers из ответа.

4.2.4. Возможность повторного использования OTP

Описание:

Завладев OTP, атакующий может использовать его повторно для совершения критичных действий от имени жертвы.

Риск:

Приложение позволяет использовать OTP (one time password) повторно для разных или одного и того же действия.

Уязвимый ресурс:

- bcwallet.io

Технические детали:

При любом типе 2FA (через telegram и google authentication) код действителен в течение свой жизни для множества действий.

Рекомендации:

- OTP должен быть привязан к конкретному действию и действовать только один раз.

5. Заключение

В результате анализа сайта “bcwallet.io” специалистами Digital Security была обнаружена уязвимость, которая потенциально могла бы позволить злоумышленнику скомпрометировать аккаунт любого пользователя. Также были выявлены некоторые слабости, исправление которых рекомендуется в целях общего повышения степени защищенности Системы.

Общий уровень защищенности Системы можно охарактеризовать как «высокий».

Приложение 1. Анализ уровня защищенности. Справочная информация

Анализ уровня защищенности

Для анализа уровня защищенности необходимо оценить критичность и вероятность реализации выявленных в ходе аудита уязвимостей. Вероятность реализации определяется доступностью и простотой реализации уязвимости.

Критичность реализации уязвимости

Свойство «критичность реализации» некоторой уязвимости характеризует возможные последствия реализации данной уязвимости с точки зрения угроз нарушения конфиденциальности, целостности и доступности информации, обрабатываемой на уязвимом ресурсе. Описание уровней критичности реализации уязвимостей приведено в Таблице А–1.

Таблица А–1. Уровни критичности уязвимостей

Значение	Нарушение конфиденциальности	Нарушение целостности	Нарушение доступности
Отсутствует	Не происходит	Не происходит	Не происходит
Низкий	Получение нарушителем доступа к некритичной информации в результате эскалации привилегий	Нарушение целостности некритичной информации с правами обычного пользователя	Кратковременный отказ в обслуживании критичного приложения
Средний	Нарушение конфиденциальности критичной информации с правами обычного пользователя	Нарушение целостности критичной информации с правами обычного пользователя	Отказ в обслуживании критичного приложения или кратковременный отказ в обслуживании
Высокий	Нарушение конфиденциальности критичной информации с правами	Нарушение целостности критичной информации с правами	Отказ в обслуживании

	администратора	администратора	

Простота эксплуатации уязвимости

Свойство «простота эксплуатации» некоторой уязвимости определяет, какие аппаратные и программные средства, профессиональные навыки, а также какое количество временных и вычислительных ресурсов, необходимо потенциальному нарушителю для реализации некоторой уязвимости (Таблица А–2).

Таблица А–2. Уровни простоты эксплуатации уязвимости

Значение	Описание
Низкий	Для эксплуатации уязвимости требуется разработка новых программных средств, проведение анализа конфигурации атакуемой системы, выявление и проверка различных возможных путей и условий успешной эксплуатации данной уязвимости, вычислительные мощности или временной резерв. Атакующий должен обладать значительными профессиональными навыками и познаниями в специфичных областях.
Средний	Для эксплуатации уязвимости требуется наличие специальных программных или аппаратных средств, проведение анализа конфигурации атакуемой системы, вычислительные мощности или временной резерв. Атакующему достаточно обладать незначительным объемом профессиональных навыков и познаний для реализации атаки.
Высокий	Для эксплуатации уязвимости не требуется использование специальных аппаратных или программных средств, значительные вычислительные мощности или временной резерв, детальное знание конфигурации атакуемой системы. Атакующему для реализации атаки не требуются специфичные профессиональные навыки и познания.

Доступность уязвимости

Свойство «доступность» некоторой уязвимости определяет, каким классам пользователей доступен уязвимый ресурс (Таблица А–3).

Таблица А–3. Уровни доступности

Значение	Описание
Низкий	Привилегированные пользователи
Средний	Зарегистрированные пользователи
Высокий	Все пользователи

Вероятность эксплуатации уязвимости

Вероятность эксплуатации уязвимости рассчитывается на основе простоты эксплуатации и области доступности уязвимости по таблице А–4.

Таблица А–4. Уровень вероятности эксплуатации

Вероятность эксплуатации		Простота эксплуатации		
		Низкий	Средний	Высокий
Доступность	Низкий	Низкий	Низкий	Средний
	Средний	Низкий	Средний	Высокий
	Высокий	Средний	Высокий	Высокий

Риск уязвимости

Риск уязвимости (по одной из угроз) рассчитывается на основе критичности уязвимости (по одной из угроз) и вероятности эксплуатации уязвимости по таблице А–5.

Таблица А–5. Уровень риска

Риск уязвимости		Вероятность эксплуатации		
		Низкий	Средний	Высокий
Критичность уязвимости	Низкий	Низкий	Низкий	Средний
	Средний	Низкий	Средний	Высокий
	Высокий	Средний	Высокий	Высокий

Приложение 2. Анализ уровня защищенности. Перечень обнаруженных слабостей и уязвимостей

Обнаруженные в ходе работ уязвимости и слабости Системы представлены в таблице Б-1.

Таблица Б-1. Перечень обнаруженных уязвимостей и слабостей Системы

Перечень обнаруженных уязвимостей		
Уязвимость	**Итоговый риск**	**Подробности в пункте**
Недостаточное количество бит энтропии в токене	Средний	4.1.1.
Некорректное управление сессией	Низкий	4.1.2.
Перечень обнаруженных слабостей		
Слабость	**Подробности в пункте**	
Отсутствие механизма HSTS	4.2.1.	
Отсутствие защиты от атак типа clickjacking	4.2.2.	