**Требования по информационной безопасности**

**для автоматизированной системы «test\_system\_nlmk»**

|  |  |
| --- | --- |
| **Код** | **Формулировка требования** |
|  | **Архитектура и Дизайн** |
| AR1 | Сторонние компоненты и библиотеки, используемые для разработки приложения должны быть описаны в документации. Использование компонентов с известными уязвимостями должно быть исключено. |
| AR2 | Для работы в одном приложении внутренних и внешних пользователей должны использоваться различные инстансы приложения. |
| AR3 | Для взаимодействия с другими приложениями и компонентами должны использоваться учетные записи, обладающие минимально необходимыми полномочиями. |
| AR4 | Все данные загружаемые в систему должны быть получены из довернных источников. Если исользуются данные из недоверенных источников(например, сторонние Java скрипты) они должны запускаться в iFrame с параметром Sandboxing |
| AR8 | Реализован механизм принудительных обновлений мобильного приложения |
| AR6 | Проверки безопасности должны быть реализованы как на клиентской части приложения так и на бэкенде |
| AR5 | Необходимо использовать правила для линтера, направленные на проверку безопасности кода |
|  | **Технические. Защита клиентской части** |
| RE4 | Приложение обнаруживает и реагирует на наличие на устройстве широко используемых инструментов и фреймворков для реверс инжиниринга |
| RE6 | Приложение обнаруживает и реагирует на изменение своего кода и данных в его области оперативной памяти |
|  | **Технические. Взаимодействие с ОС** |
| PI8 | Десериализация объектов, если она есть, реализована с использованием безопасного API сериализации. |
|  | **Процессные** |
| PR3 | После формирования требований по защите информации должна быть проведена встреча по их обсуждению |
| PR4 | Должно быть проведено моделирование угроз |
| PR6 | Для приложения должен быть проведен анализ защищенности. Для проведения работе необходимо: выделить бюджет, предоставить учетные записи, схему стенда, стабильно работающий стенд и реквизиты доступа в систему учета ошибок. |
| PR5 | До развертывания приложения в продуктовой среде должно быть проведено тестирование приложения на предмет выполнения требований по защите информации |
| PR8 | Перед переводом в продуктовый контур должно быть проведено как тестирование нового приложение, так и систем, доработанных для интеграции с ним. |
| PR7 | Должен быть проведен статический анализ приложения. Для внешней разработки - предоставлены результаты данного анализа. |
|  | **Технические. Управление сессиями** |
| SM11 | Если в приложении используется управление сессиями с сохранением состояния(stateful), то бэкэнд использует случайным образом сгенерированные идентификаторы сессии для аутентификации клиентских запросов. При этом учетные записи пользователей не пересылаются |
| SM12 | Если используется аутентификация без сохранения состояния(stateless), сервер предоставляет токен, подписанный с использованием безопасного криптоалгоритма. Долны выполняться базовые требования к работе с токенами. |
| SM13 | Бэкенд удаляет существующую сессию, когда пользователь выходит из системы |
| SM1 | Session IDs, передающиеся с помощью cookies должны настроены с использованием флагов безопасности(http only, secure, path) |
| SM2 | Session ID должен быть сменен при аутентификации, повторной аутентификации или смене привилегий учетной записи. |
| SM3 | Функциональность по принудительному завершению сессии пользователем(Logout) должна быть доступна на каждой странице приложения |
| SM4 | В приложении должен быть реализован настраиваемый механизм конфигурирования абсолютного времени жизни сессий пользователей |
| SM5 | В приложении должен быть реализован настраиваемый механизм конфигурирования времени жизни сессий пользователей в случае неактивности |
| SM6 | Session ID должен быть связана с параметрами подключения пользователя (например с user agent / типом устройства/данными геолокации) |
| SM7 | Параметр, определяющий количество конкурентных сессий для одного пользователя должен быть настраиваемым на стороне приложения |
| SM8 | Пользователю должна быть предоставлена возможность просмотра и завершения всех активных сессий |
| SM9 | Необходимо ограничивать максимальное количество одновременных запросов к серверу |
| SM10 | В случае отсутствия в приложении механизма управления жизненным циклом токенов в приложении должны поддерживать чёрные списки JWT-токенов |
|  | **Технические. Идентификация и аутентификация** |
| AU14 | Для выполнения критичных операций в приложении(регистрация и восстановление аккаунта) не должен использоваться небезопасные каналы взаимодействия (e-mail или колл-центр). |
| AU10 | Подтверждение финансовых операций должно осуществляться с использованием одноразовых паролей |
| AU1 | Все интерфейсы и ресурсы приложения должны быть доступны только после успешного прохождения аутентификации |
| AU2 | В качестве Single Sign-On провайдера может быть использован только корпоративный каталог пользователей |
| AU13 | Приложение информирует пользователей о всех важных действиях с их учетной записью. Пользователи могут просматривать список устройств, просматривать дополнительную информацию (IP-адрес, местоположение и т.д.), и блокировать конкретные устройства. |
| AU12 | В приложении реализована и применяется двухфакторная аутентификация. Второй фактор может использоваться только на этапе выполнения критичных функций в приложении. |
| AU3 | В приложении должны быть реализованы механизмы, позволяющие противодействовать атакам, связанным с перебором паролей пользователей |
| AU4 | Перед проведением критичных с точки зрения безопасности операций(например, смены пароля, проведение финанисовой операции, изменения способа аутентификации) должна осуществляться повторная аутентификация пользователей |
| AU5 | В приложении должен быть реализован настраиваемый механизм конфигурирования параметров сложности паролей пользователей |
| AU6 | В приложении должен быть реализован настраиваемый механизм конфигурирования времени жизни паролей пользователей |
| AU7 | Должно осуществляться уведомление пользователя в случае выявления попыток входа в приложения(как успешных, так и не успешных) из необычного окружения |
| AU8 | Должно осуществляться уведомление пользователя в случае смены его пароля в приложении |
| AU9 | Процедура восстановления забытого пароля не должна отличаться по стойкости от процедуры его первичного получения |
|  | **Технические. Разграничение доступа** |
| AC1 | Механизмы разграничения доступа должны быть реализованы на стороне сервера и использовать только надежные реализации |
| AC2 | Разграничение доступа должно быть реализовано в соответсвии с матрицей ролей |
| AC3 | Пользователям должны быть предоставлены только минимально необходимые полномочия, необходимые для реализации бизнес-процесса. |
| AC4 | В приложение должны быть настроены лимиты на выполняемые операций и функций(максимальное количество просмотров карточек клиентов в час, количество отправляемых по почте уведомлений в день и т.д.) |
| AC5 | Для запуска Node.js не должен использоваться пользователь, обладающий root-привилегиями |
|  | **Технические. Валидация входных данных** |
| IV4 | Должны быть реализованы механизмы противодействия атакам типа Cross-Site Request Forgery |
| IV1 | Для валидации данных должен использоваться только согласованный и проверенный на предмет соответствия требованиям по безопасности набор библиотек |
| IV2 | Конфиденциальная информация никогда не должна передаваться методом GET |
| IV3 | Параметры валидации должны в явном виде определять допустимые значения для данных. Все, не советующие правилам данные не должны обрабатываться в приложении. |
| IV5 | Должны быть реализованы механизмы противодействия атакам типа Clickjacking |
| IV6 | Редиректы не должны содержать не проверенных данных |
| IV7 | В случае реализации в приложении функциональности по загрузке файлов необходимо осуществлять валидацию контента, включая проверку на наличие во вложении вредоносного кода |
| IV8 | Должны быть реализованы механизмы противодействия атакам типа переполнение буффера( Buffer overflow) |
| IV9 | В случае если для работы приложения обязательно использование небезопасного кода его выполнение должно осуществляться в песочнице |
|  | **Технические. Валидация вывода** |
| OE1 | Для валидации данных, передаваемых в любые интерфейсы должен использоваться только согласованный и проверенный на предмет соответствия требованиям по безопасности набор практик |
| OE2 | Неэкранированные данные не должны передаваться в HTTP заголовки |
| OE3 | Неэкранированные данные не должны записываться в журналы аудита |
| OE4 | Неэкранированные данные не должны передаваться в качестве параметров для системных команд операционной системы |
|  | **Технические. Криптография и генерация случайных чисел** |
| CR10 | При реализации взаимной аутентификации с помощью сертификатов приложение верифицирует серверные X.509 сертификаты во время установления защищённого соединения. Принимаются только сертификаты, подписанные доверенными удостоверяющими центрами |
| CR9 | Данные, передаваемые по сети от клиентской части к приложения до бэкэнда шифруются с использованием протокола TLS |
| CR8 | Приложение не переиспользует один и тот же ключ для различных целей |
| CR7 | В приложение не используются устаревшие и слабые криптографические протоколы и алгоритмы. |
| CR1 | Криптографические библиотеки должны применяться в приложении для достижения описаных в документации целей и должны быть настроены в соответствии с задокументированными требованиями по безопасности |
| CR2 | Применение средств криптографической защиты должно осуществляться с учетом утвержденной политики по управлению ключевой информацией |
| CR3 | Для хранения паролей в приложении должно использоваться хэширование с солью |
| CR4 | Для генерации случайных чисел должен использоваться согласованный и проверенный на предмет соответствия требованиям по безопасности набор методов |
| CR5 | Для обработки паролей не должен использоваться стандартный модуль Node.js crypto. Вместо него необходимо применять Bcrypt |
|  | **Технические. Обработка ошибок** |
| EH3 | Логика обработки ошибок, связанных с реализаций функций безопасности по-умолчанию должна предполагать блокирование доступа. |
| EH1 | В случае возникновения ошибок в работе приложения, содержащаяся в описании ошибки информация не должна содержать чувствительных данных, которые могут быть использованы злоумышленником |
| EH2 | Файл Robots.txt не должен содержать чувствительной информации |
|  | **Технические. Журналирование** |
| LO1 | Все имеющие отношение к информационной безопасности и описанные в документации параметры должны журналироваться при изменении. |
| LO2 | Все имеющие отношение к безопасности события, содержащиеся в журналах аудита должны содержать всю необходимую информацию для их интерпретации |
| LO3 | В приложении не должны журналироваться данные, которые могут помочь злоумышленнику для реализации атаки (например: идентификаторы клиентских сессий, коды, персональные данные, отладочные сообщения и т.д). Отладочный код и скрытые настройки удалены из приложения. |
|  | **Технические. Защита данных** |
| DP6 | Конфиденциальные данные не должны передаваться третьей стороне, кроме случаев если это часть бизнес функциональности приложения |
| DP10 | Конфиденциальные данные не сохраняются в бэкапы, создаваемые операционной системой |
| DP1 | Чувствительная информация, сохраненная в кэше системы должна быть защищена от неавторизованного доступа и очищена сразу же после достижения целей обработки |
| DP2 | Пароли, используемые для подключения к компонентам приложения и другим приложениям не должны храниться в открытом виде |
| DP8 | Чувствительные данные недоступны через механизмы межпроцессного взаимодействия (IPC). |
| DP5 | Для хранения чувствительных данных, таких как персональные данные, аутентификационная информация и криптографические ключи должно использоваться хранилище для конфиденциальной информации предоставляемое платформой(Android, iOS). |
| DP12 | Приложение хранит чувствительные данные в памяти только на время необходимое для обработки и полностью удаляет их из памяти после завершения работы с ними. |
| DP3 | Пароли никогда не должны храниться в клиентской части приложения |
| DP4 | Чувствительные данные передаваемые клиентской части приложения должны быть защищены от кэширования за счет использования соответствующих HTTP заголовков |
|  | **Технические. Безопасность подключений** |
| CS1 | Передача информации между компонентами приложения и другими приложениями должна осуществляться только по защищенным протоколам |
| CS2 | В приложении должна быть реализована Content Security Policy |
| CS3 | Для обеспечения безопасности приложения должны быть корректно настроены относящиеся к безопасности HTTP заголовки |
|  | **Технические. Общие требования и документирование** |
| CO1 | В документации на приложения должны быть перечислены все используемые криптографические библиотеки, цели и способы их применения, а так же их настройки по безопасности |
| CO2 | В документации на приложение должны быть перечислены все имеющие отношение к информационной безопасности параметры |
|  | **Технические. Качество кода и безопасность сборки** |
| CQ5 | Используются все стандартные функции безопасности, предоставляемые инструментами для разработки (такие как обфускация, минификация байт-кода, защита стека, поддержка PIE и ARC). |