УДК 621.9.048.7

БЕЗОПАСНОСТЬ И КОНФИДЕНЦИАЛЬНОСТЬ ДАННЫХ В МЕДИЦИНСКИХ ПРИЛОЖЕНИЯХ: ЛУЧШИЕ ПРАКТИКИ И ТЕХНОЛОГИИ НА RUBY

[1]Соколовская А. Ю., [2]Макареня С. Н.
[1]Белорусский национальный технический университет,
Минск, Беларусь, nastya_kiulo@mail.ru,
[2]Белорусский национальный технический университет,
Минск, Беларусь, makar_sn@mail.ru

Аннотация. В статье рассматриваются методы защиты медицинских приложений от киберугроз, включая использование HTTPS, регулярное обновление идентификаторов сессии, хранение минимума данных в CookieStore, применение мер защиты от CSRF, валидацию входных данных, ограничение доступа к файлам и проверку загружаемых файлов. Авторы подчеркивают важность этих мер для укрепления безопасности и подчеркивают комплексный подход, включая аудиты безопасности, обучение персонала и отслеживание новых угроз.

Ключевые слова: киберугроза, безопасность, конфиденциальность, HTTPS, CookieStore, CSRF.

Abstract. The article discusses methods for protecting healthcare applications from cyber threats, including using HTTPS, regularly updating session IDs, storing minimal data in the CookieStore, applying CSRF protection measures, validating input data, restricting access to files, and verifying downloaded files. The authors emphasize the importance of these measures to strengthen security and emphasize a comprehensive approach, including security audits, staff training, and monitoring for emerging threats.

Key words: cyber threat, security, privacy, HTTPS, CookieStore, CSRF.

Введение.

В эпоху цифровизации и быстрого развития технологий, медицинская индустрия активно интегрирует в свою работу разнообразные IT-решения. Однако вместе с новыми возможностями приходят и новые риски.

Медицинские данные относятся к категории особо чувствительной информации. Они включают в себя историю болезней, результаты анализов, персональные данные пациентов и многие другие сведения, которые подлежат строгой конфиденциальности. Несанкционированный доступ к такой информации может привести не только к нарушению приватности, но и к серьезным последствиям в виде медицинских ошибок, мошенничеству или даже шантажу.

При этом медицинская сфера становится все более привлекательной для злоумышленников. По данным исследований, медицинские данные стоят на черном рынке значительно дороже, чем кредитная карта или личные данные. Это делает медицинские приложения основной мишенью для атак.

Ruby – это современный интерпретируемый язык программирования, который отличается высокой простотой синтаксиса и читаемостью кода. Он является объектно-ориентированным языком с динамической типизацией, что позволяет разработчикам создавать гибкие и модульные приложения. В контексте конференции о безопасности и конфиденциальности данных в медицинских приложениях, Ruby может быть использован для разработки надежных и безопасных приложений благодаря своей простоте и богатой экосистеме инструментов и библиотек.

Безопасность данных в медицинских приложениях имеет первостепенное значение не только с точки зрения юридической ответственности и репутации медицинской организации, но и с точки зрения благосостояния и доверия пациентов. Неспособность обеспечить должный уровень безопасности может привести к потере доверия со стороны пациентов, судебным искам и серьезным финансовым потерям.

Обеспечение безопасности данных в медицинских приложениях – это не просто техническая задача, но и вопрос этики, ответственности и заботы о пациентах. Разработчикам, IT-специалистам и всем, кто причастен к созданию и эксплуатации медицинских приложений, необходимо постоянно совершенствовать свои навыки и использовать лучшие практики для обеспечения максимальной безопасности.

Обзор текущей ситуации с угрозами безопасности.

Современный мир IT пронизан сложной сетью угроз безопасности, и медицинская сфера – не исключение. Несмотря на все технологические прорывы, угрозы безопасности продолжают эволюционировать, становясь все более изощренными и опасными. Наиболее распространенные угрозы включают недостаточную защиту данных, которая может привести к утечкам чувствительных медицинских данных, и недостаточную аутентификацию, и авторизацию, что может позволить злоумышленникам получить доступ к этой ценной информации. Кроме того, недостаточная защита от вредоносного программного обеспечения может представлять риск в виде вирусов и вредоносных программ-вымогателей. И наконец, отсутствие обновлений и поддержки приложений может создать уязвимости и сделать приложения более подверженными атакам. Ниже приведены наиболее распространенные угрозы:

1. Угон сессии (Session Hijacking). Это тип атаки, при котором злоумышленник узнает идентификатор сессии жертвы и использует его для получения доступа к ее учетной записи. Такие атаки часто возможны из-за утечек идентификатора сессии, например, через нешифрованные соединения.

2. Атаки повторного воспроизведения для сессий CookieStore. CookieStore в Ruby on Rails сохраняет данные сессии прямо в cookie. Если злоумышленник сможет перехватить это cookie, он может прочитать или даже подменить информацию внутри, если она не зашифрована.

3. Фиксация сессии (Session Fixation). При такой атаке злоумышленник заставляет жертву использовать идентификатор сессии, который ему известен. Затем, зная идентификатор сессии, атакующий может угнать сессию.

4. Межсайтовая подделка запроса (CSRF). Это когда злоумышленник заставляет жертву выполнить нежелательное действие на сайте, на котором она аутентифицирована, без ее знания или согласия. Обычно это достигается путем маскировки вредоносного действия под что-то безобидное.

5. Уязвимости, связанные с перенаправлениями и файлами. Неправильно реализованные перенаправления могут позволить злоумышленникам отправлять пользователей на вредоносные сайты. Уязвимости, связанные с файлами, включают такие риски, как загрузка произвольных файлов злоумышленником или чтение файлов сервера, которые не должны быть доступны.

Для защиты от возникающих угроз безопасности в медицинской отрасли можно использовать следующие способы защиты:

1. Использование зашифрованного соединения (HTTPS) для передачи идентификаторов сессии. HTTPS (HTTP Secure) использует SSL/TLS протоколы для шифрования данных, передаваемых между клиентом и сервером. Это предотвращает «прослушивание» данных третьими лицами и гарантирует, что данные, передаваемые между сервером и клиентом, не будут перехвачены или изменены.

2. Регулярное обновление идентификаторов сессии. Путем регулярного обновления идентификаторов сессии можно уменьшить риск угонов сессии. Если идентификатор сессии обновляется с каждым запросом, у злоумышленника будет меньше времени на его использование.

3. Хранение минимума данных в CookieStore или использование сервернова хранения сессий. Сессии CookieStore хранят все данные прямо в куки, что делает их уязвимыми для атак. Хранение минимального количества данных или переход к серверному хранению (например, с использованием Redis или базы данных) может уменьшить риски.

4. Применение мер защиты от CSRF, такие как встроенные механизмы защиты в Rails. Rails предоставляет встроенные средства для борьбы с CSRF-атаками. Один из методов – это использование токенов, которые генерируются и проверяются сервером при каждом изменяющем состояние запросе.

5. Валидация и проверка всех входящих данных, особенно URL для перенаправлений. Непроверенные входные данные могут быть источником многих угроз безопасности, включая инъекции кода и межсайтовые скрипты (XSS). Проверка и очистка данных, особенно тех, которые используются для перенаправлений, может предотвратить многие атаки.

6. Ограничение доступа к файлам на сервере, и проверка загружаемых файлов на наличие вредоносного контента. Злоумышленники могут попытаться загрузить вредоносные файлы на сервер или получить доступ к чувствительной информации. Убедитесь, что у вас есть строгие правила доступа к файлам и директориям на сервере, и используйте программное обеспечение для сканирования файлов на наличие вирусов и другого вредоносного ПО.

Придерживаясь этих рекомендаций, можно значительно укрепить безопасность веб-приложений и минимизировать риски для пользователей.

Обеспечение безопасности в медицинских приложениях требует комплексного подхода, включающего в себя как технические, так и организационные

меры. В свете постоянно меняющегося ландшафта угроз необходимо не только разрабатывать безопасные приложения, но и регулярно проводить аудиты безопасности, обучать персонал и следить за новыми угрозами.

Разработка безопасных медицинских приложений на Ruby – это сложная и ответственная задача. Медицинские данные чрезвычайно чувствительны, и нарушения в области безопасности могут иметь серьезные последствия как для пациентов, так и для медицинских учреждений.