**PHÂN TÍCH YÊU CẦU BẢO MẬT TỪ SRS**

Thứ 3, ngày 5 tháng 3 năm 2024

Thời gian: 8h00 am

1. Mã Hóa Dữ Liệu:

• Yêu cầu: Tất cả dữ liệu người dùng phải được mã hóa và lưu trữ một cách an toàn.

• Phân Tích: Đảm bảo rằng thông tin cá nhân của người dùng, bao gồm thông tin đăng nhập, mật khẩu và dữ liệu khác, được mã hóa khi lưu trữ trong cơ sở dữ liệu.

2. Xác Thực và Ủy Quyền:

• Yêu cầu: Hệ thống phải có cơ chế xác thực và ủy quyền mạnh mẽ để đảm bảo chỉ người dùng có quyền mới có thể truy cập và sửa đổi dữ liệu.

• Phân Tích: Cung cấp cơ chế xác thực bằng cách sử dụng mã thông báo (token) hoặc phiên làm việc (session) cùng với việc sử dụng một cơ chế ủy quyền để kiểm soát quyền truy cập của người dùng vào các phần của ứng dụng.

3. Bảo Mật Dữ Liệu:

• Yêu cầu: Đảm bảo dữ liệu người dùng được lưu trữ một cách an toàn.

• Phân Tích: Sử dụng các biện pháp bảo mật như mã hóa dữ liệu, kiểm tra ràng buộc SQL, và cập nhật thường xuyên để bảo vệ hệ thống khỏi các lỗ hổng bảo mật potentional.

Người tạo

Nguyễn Minh Diện

**THIẾT KẾ CƠ CHẾ BẢO MẬT**

Thứ 3, ngày 5 tháng 3 năm 2024

Thời gian: 8h00 am

1. Mã Hóa Dữ Liệu:

• Sử dụng thuật toán mã hóa mạnh mẽ như AES (Advanced Encryption Standard) để mã hóa thông tin nhạy cảm như mật khẩu trước khi lưu trữ vào cơ sở dữ liệu.

2. Xác Thực và Ủy Quyền:

• Thiết kế một cơ chế xác thực sử dụng JWT (JSON Web Tokens) hoặc OAuth2 để xác thực người dùng.

• Áp dụng một cơ chế ủy quyền để kiểm soát quyền truy cập của người dùng vào các tài nguyên và chức năng trong ứng dụng.

3. Bảo Mật Dữ Liệu:

• Sử dụng kỹ thuật mã hóa dữ liệu ở cả ở mức truyền dữ liệu và lưu trữ dữ liệu.

• Triển khai kiểm tra ràng buộc SQL để ngăn chặn các cuộc tấn công SQL Injection.

• Thực hiện các biện pháp bảo mật phần mềm như cập nhật định kỳ để đảm bảo hệ thống luôn bảo vệ khỏi các lỗ hổng mới được phát hiện.

Người tạo

Nguyễn Minh Diện