1 vấn đề trong tài liệu:

A04 - Insecure Design

1. Mô tả

Thiết kế không an toàn là một phạm vi rộng mô tả cho các điểm yếu khác nhau, được hiểu là “thiết kế thiếu kiểm soát hoặc không hiệu quả" . Sai sót trong thiết kế và sai sót trong triển khai có nguyên nhân và khắc phục khác nhau.

Thiết kế an toàn là một văn hóa và phương pháp đánh giá liên tục các mối đe dọa và đảm bảo rằng mã (code) được thiết kế và thử nghiệm đầy đủ để ngăn chặn các phương pháp tấn công đã biết.

Vòng đời phát triển an toàn

Hãy liên hệ, trao đổi với các chuyên gia bảo mật của bạn từ khi bắt đầu một dự án phần mềm cho đến khi kết thúc dự án và cả trong quá trình bảo trì phần mềm.

2. Phương pháp ngăn chặn:

Thiết lập và sử dụng vòng đời phát triển an toàn cùng với các chuyên gia ATTT để giúp đánh giá và thiết kế các biện pháp kiểm soát liên quan đến quyền riêng tư và bảo mật.
Thiết lập và sử dụng thư viện các mẫu thiết kế an toàn.
Sử dụng mô hình mối đe dọa đối với các xác thực quan trọng, kiểm soát truy cập, logic nghiệp vụ và các luồng chính.
Tích hợp kiểm tra tính hợp lý của dữ liệu (từ frontend đến backend).
Viết các bài kiểm tra để kiểm tra các luồng quan trọng.
Tách các phần của hệ thống và các lớp mạng tùy thuộc vào nhu cầu hoạt động của ứng dụng.
Phân tách người dùng một cách chặt chẽ theo thiết kế ở tất cả các tầng.
Hạn chế tài nguyên được sử dụng của người dùng hoặc dịch vụ.

3. Các kịch bản tấn công:

Kịch bản 1: Quy trình khôi phục thông tin xác thực thông qua “câu hỏi và câu trả lời” là không đáng tin cậy. Thiết kế như vậy nên được loại bỏ và thay thế bằng một thiết kế an toàn hơn.
Kịch bản 2: Trang web thương mại điện tử của một chuỗi bán lẻ không có biện pháp bảo vệ chống lại các bot tự động mua thẻ video cao cấp được giảm giá để bán lại ở các trang web khác.
Các quy tắc thiết kế về logic để chống bot cần được xem xét kỹ lưỡng, ví dụ các giao dịch mua được thực hiện quá nhanh trong vòng vài giây, cần từ chối các giao dịch này

Ý niệm blockchain

Đó là danh sách các khối dữ liệu được liên kết với nhau bằng dấu thời gian.
Mỗi blockchain chứa hàm băm (hash) dữ liệu của nó được nới với hàm băm của blockchain trước đó.
Block 1:
Hash (dữ liệu 1)
Block 2:
Hash(Hash1 + Hash(dữ liệu 2))
Block 3:
Hash(hash2 + hash(dữ liệu 3))
Blockchain đại diện cho cơ sở dữ liệu chỉ ghi:

• tính bất biến của nó được đảm bảo bởi một số lượng lớn máy tính ‘ngang hàng’ có bản sao của chuỗi khối
• Nó có thể được sử dụng như một sổ cái, có thể truy cập rộng rãi vì nó được phân phối.
• Bất kỳ máy tính ngang hàng nào cũng có thể thêm một khối mới vào chuỗi và sau khi cập nhật giá trị băm của nó, có thể phân phối phiên bản mới hơn cho tất cả các máy ngang hàng.
• Khi các khối được tạo ra đồng thời, chuỗi khối sẽ liên tục phân nhánh
• Mỗi blockchain có một thuật toán để chấm điểm các phiên bản khác nhau và chỉ giữ lại phiên bản có điểm cao nhất
• Do đó, bất cứ khi nào hai đồng nghiệp phát hiện ra các chuỗi khối khác nhau, rõ ràng họ sẽ chỉ giữ lại một phiên bản.
• Các đồng nghiệp đã chèn khối vào chuỗi khối bị từ chối phải chèn lại khối đó vào chuỗi khối tham chiếu mới
• Có động cơ mở rộng một chuỗi khác mới hơn thay vì cố gắng thay thế nó. Điều này đạt được bằng cách yêu cầu nỗ lực tính toán (nghiêm túc) để mở rộng.
Blockchain
• cho phép có hệ thống phân tán mà không cơ quan nào có thể kiểm soát/thao túng
• triển khai và thực thi thuật toán (hợp đồng) đã được thiết kế trong chuỗi
• gần như không thể có chuyện blockchain có thể bị làm giả
Nhiều ví dụ về tiềm năng sử dụng ...
• Phiếu bầu điện tử, truy xuất nguồn gốc hàng hóa, hợp đồng mua bán, hồ sơ bản quyền, quản lý quyền kỹ thuật số, hồ sơ tiết kiệm năng lượng, bằng cấp điện tử,...
• Chuỗi khối trở thành cơ sở dữ liệu đáng tin cậy với các quy trình được xác định cho phép các thực thể ngang hàng tin cậy lẫn nhau
• Khắc phục được nhiều điểm yếu của phương pháp công chứng tập trung đó là:
• có thể bị hack
• có thể không hiệu quả trong việc xử lý giao dịch và làm chậm hoạt động kinh doanh
• có thể phân biệt đối xử
• có thể lấy % giá trị giao dịch không hợp lý để cung cấp ít dịch vụ
• có thể lấy cắp thông tin, lo ngại về quyền riêng tư

Chữ ký điện tử

Chúng ta cần một cách để đảm bảo tính toàn vẹn của dữ liệu nếu kẻ tấn
công có thể sửa đổi cả dữ liệu và hàm băm.Chữ ký số giải quyết được vấn đề này.
Chữ ký số là hàm băm của dữ liệu được mã hóa bằng khóa riêng của người ký.
Chữ ký điện tử là gửi: dữ liệu + Encryption(Hash(dữ liệu))
Encryption có 2 khóa: khóa người gửi và khóa người nhận
Chữ ký số giải quyết vấn đề toàn vẹn ban đầu và ngăn chặn mọi nỗ
lực giả mạo. Bởi vì kẻ tấn công cần biết về khóa riêng của người ký để tạo lại chữ
ký số.
Tài liệu được ký kỹ thuật số KHÔNG được mã hóa.
• Bất kỳ ai có quyền truy cập vào tài liệu đều có thể đọc nó
• Không cần biết về bất kỳ phím nào để đọc tài liệu
• Bất kỳ ai cũng có thể xác minh tính toàn vẹn và tính xác thực của tài liệu
• Cần có kiến thức về khóa công khai của người ký để xác minh
• Nếu tài liệu được sửa đổi thì cần phải ký lại
• Cần có kiến thức về khóa riêng
• Thứ tự phát triển từ checksum ---> digital signature --> blockchain

Rủi ro khi lộ thông tin vị trí

Tạo điều kiện thuận lợi cho việc theo dõi vật lý, tống tiền, tiết lộ những bí mật sâu sắc và hơn thế nữa. Chỉ với dữ liệu vị trí, không khó để phát hiện nhà hoặc nơi làm việc của một cá nhân và sau đó tìm chi tiết nhận dạng bằng cách sử dụng địa chỉ được suy luận và thông tin có sẵn công khai.Ngoài ra, nhà phát triển ứng dụng có thể lưu trữ dữ liệu vị trí nội bộ hoặc bán cho nhà mô giới dữ liệu. Tin tặc, nhà

quảng cáo và thậm chí một số cơ quan chính phủ nhất định có thể khai thác thông tin này, xâm phạm quyền riêng tư của chúng ta và khiến chúng ta dễ bị tổn thương trước các mối đe dọa trực tuyến khác nhau.