TÌM HIỂU VỀ LỖI BẢO MẬT

ĐỐI TƯỢNG THAM CHIẾU THIẾU AN TOÀN

Họ tê:Trương Văn trang

MSSV:12020392

1. Tìm hiểu sơ lược về lỗi bảo mật đối tượng tham chiếu thiếu an toàn
2. Các đối tượng nguy hiểm  
   Hãy xem xét các loại người dùng khác nhau trong hệ thống của bạn. Liệu có người dùng nào chỉ có một phần quyền truy cập đến các loại dữ liệu trong hệ thống ?
3. Khả năng tấn công  
   Kẻ tấn công, là một người dùng trong hệ thống, có thể thay đổi một tham số ứng với một đối tượng hệ thống nào đó mà hắn không có quyền truy cập đến. Liệu việc truy cập có thành công hay không?
4. Sự phổ biến  
   Ứng dụng thường xuyên sử dụng trực tiếp tên hoặc khóa của một đối tượng khi xây dựng các trang web. Các ứng dụng thường không kiểm tra nếu người dùng này thật sự có quyền truy cập hay không. Đây chính là mấu chốt dẫn đến lỗi các đối tượng tham chiếu. Người kiểm tra có thể dễ dàng thay đổi các giá trị tham số để phát hiện ra lỗ hổng này, phân tích mã nguồn có thể giúp ta nhanh chóng phát hiện quyền truy cập có được xem xét cẩn thận hay không.
5. Sự nguy hiểm nếu có thể khai thác  
   Lỗi như thế có thể giúp kẻ tấn công nắm quyền toàn bộ những dữ liệu có thể được liên kết bởi các tham biến. Trừ khi không gian truy cập rời rạc, kẻ tấn công có thể truy cập tất cả các loại dữ liệu như thế.
6. Cách phát hiện ra lỗi bảo mật  
   Cách tốt nhất để biết xem một ứng dụng có bị lỗi này hay không là kiểm tra nếu tất cả các đối tượng tham chiếu có được bảo vệ hợp lí không. Để đạt được điều này, xem xét :
   1. Đối với các liên kết trực tiếp tới các dữ liệu cần bảo vệ, ứng dụng cần phải kiểm tra xem người dùng đang yêu cầu có được cho phép quyền truy cập đến dữ liệu đó hay không
   2. Nếu liên kết là một tham biến gián tiếp, việc chuyển biến đến dữ liệu trực tiếp phải được giới hạn bởi những giá trị cho phép đối với người dùng hiện tại
   3. Kiểm tra mã nguồn của ứng dụng có thể nhanh chóng phát hiện nếu một trong 2 phương pháp trên không được thiết kế cẩn thận. Chạy kiểm tra cũng có thể hiệu quả trong việc phát hiện những đối tượng không an toàn. Những công cụ tự động thường không thể tìm ra lỗi này vì rất khó để xác định cái nào cần bảo vệ và như thế nào là an toàn / thiếu an toàn
7. Làm cách nào để ngăn chặn ?  
   Việc ngăn chặn lỗi đối tượng tham chiếu thiếu an toàn yêu cầu xác định một cách bảo vệ các đối tượng mà người dùng có thể truy cập ( số/tên của đối tượng ).
   1. Sử dụng mỗi liên kết đối tượng cho từng người dùng hoặc phiên làm việc. Việc này có thể ngăn chặn kẻ tấn công nhắm đến các dữ liệu không được bảo vệ. Ví dụ, thay vì sử dụng khóa cơ sở dữ liệu, một danh sách 6 dữ liệu được cho phép đối với người dùng hiện tại có thể được đánh số từ 1 đến 6 để xác định lựa chọn nào người dùng muốn truy cập.
   2. Kiểm tra truy cập. Đối với mỗi tham chiếu trực tiếp từ một nguồn không xác thực phải được kiểm tra điều khiển để chắc chắn rằng người dùng được quyền truy cập đến đối tượng yêu cầu