**ACCESS CONTROL VULNERABILITIES AND PRIVILEGE ESCALATION**

**BÀI 1: KIỂM SOÁT TRUY CẬP LÀ GÌ ?**

Kiểm soát truy cập là việc áp dụng các ràng buộc đối với người hoặc cái gì được phép thực hiện hành động hoặc truy cập tài nguyên. Trong bối cảnh của các ứng dụng web, kiểm soát truy cập phụ thuộc vào xác thực và quản lý phiên:

* Xác thực xác nhận người dùng chính là người mà họ khai báo.
* Quản lý phiên xác định những yêu cầu HTTP tiếp theo nào đang được thực hiện bởi cùng một người dùng.
* Kiểm soát truy cập xác định liệu người dùng có được phép thực hiện hành động mà họ đang cố gắng thực hiện hay không.

Kiểm soát truy cập bị hỏng là phổ biến và thường gây ra lỗ hổng bảo mật nghiêm trọng. Thiết kế và quản lý kiểm soát truy cập là một vấn đề phức tạp và năng động, áp dụng các ràng buộc về mặt kinh doanh, tổ chức và pháp lý vào việc triển khai kỹ thuật. Các quyết định thiết kế kiểm soát truy cập phải do con người đưa ra nên khả năng xảy ra lỗi là rất cao.

\* KIỂM SOÁT TRUY CẬP THEO CHIỀU DỌC

Kiểm soát truy cập theo chiều dọc là cơ chế hạn chế quyền truy cập vào chức năng nhạy cảm đối với những loại người dùng cụ thể.

Với các biện pháp kiểm soát truy cập theo chiều dọc, các loại người dùng khác nhau có thể truy cập vào các chức năng ứng dụng khác nhau. Ví dụ, người quản trị có thể sửa đổi hoặc xóa bất kỳ tài khoản nào của người dùng, trong khi người dùng thông thường không có quyền truy cập vào các hành động này. Các biện pháp kiểm soát truy cập theo chiều dọc có thể là các triển khai chi tiết hơn của các mô hình bảo mật được thiết kế để thực thi các chính sách kinh doanh như phân tách nhiệm vụ và đặc quyền tối thiểu.

\* KIỂM SOÁT TRUY CẬP THEO CHIỀU NGANG

Kiểm soát truy cập theo chiều ngang là cơ chế hạn chế quyền truy cập vào tài nguyên cho những người dùng cụ thể.

Với kiểm soát truy cập theo chiều ngang, những người dùng khác nhau có thể truy cập vào một tập hợp con các tài nguyên cùng loại. Ví dụ, một ứng dụng ngân hàng sẽ cho phép người dùng xem các giao dịch và thực hiện thanh toán từ tài khoản của họ, nhưng không phải tài khoản của bất kỳ người dùng nào khác.

\* KIỂM SOÁT TRUY CẬP PHỤ THUỘC VÀO NGỮ CẢNH

Kiểm soát truy cập theo ngữ cảnh hạn chế quyền truy cập vào chức năng và tài nguyên dựa trên trạng thái của ứng dụng hoặc tương tác của người dùng với ứng dụng.

Kiểm soát truy cập theo ngữ cảnh ngăn người dùng thực hiện hành động theo thứ tự sai. Ví dụ, một trang web bán lẻ có thể ngăn người dùng sửa đổi nội dung giỏ hàng của họ sau khi họ đã thanh toán.

\* VÍ DỤ VỀ ACCESS BROKEN

Lỗ hổng kiểm soát truy cập xảy ra khi người dùng có thể truy cập tài nguyên hoặc thực hiện các hành động mà họ không được phép thực hiện.

- TĂNG ĐẶC QUYỀN THEO CHIỀU DỌC

Nếu người dùng có thể truy cập vào chức năng mà họ không được phép truy cập thì đây là leo thang đặc quyền theo chiều dọc. Ví dụ, nếu người dùng không phải là quản trị viên có thể truy cập vào trang quản trị nơi họ có thể xóa tài khoản người dùng thì đây là leo thang đặc quyền theo chiều dọc.

- CHỨC NĂNG KHÔNG ĐƯỢC BẢO VỆ

Về cơ bản nhất, leo thang đặc quyền theo chiều dọc phát sinh khi một ứng dụng không thực thi bất kỳ biện pháp bảo vệ nào cho chức năng nhạy cảm. Ví dụ, các chức năng quản trị có thể được liên kết từ trang chào mừng của quản trị viên nhưng không phải từ trang chào mừng của người dùng. Tuy nhiên, người dùng có thể truy cập các chức năng quản trị bằng cách duyệt đến URL quản trị có liên quan.

Ví dụ: một trang web có thể lưu trữ chức năng nhạy cảm tại URL sau:

<https://insecure-website.com/admin>

Điều này có thể được truy cập bởi bất kỳ người dùng nào, không chỉ những người dùng quản trị có liên kết đến chức năng trong giao diện người dùng của họ. Trong một số trường hợp, URL quản trị có thể được tiết lộ ở các vị trí khác, chẳng hạn như tệp robots.txt:

<https://insecure-website.com/robots.txt>

Ngay cả khi URL không được tiết lộ ở bất kỳ đâu, kẻ tấn công vẫn có thể sử dụng danh sách từ để tìm ra vị trí của chức năng nhạy cảm.

Trong một số trường hợp, chức năng nhạy cảm được che giấu bằng cách cung cấp cho nó một URL ít dự đoán hơn. Đây là một ví dụ về cái gọi là "bảo mật bằng sự mơ hồ". Tuy nhiên, việc ẩn chức năng nhạy cảm không cung cấp khả năng kiểm soát truy cập hiệu quả vì người dùng có thể phát hiện ra URL bị che giấu theo một số cách.

Hãy tưởng tượng một ứng dụng lưu trữ các chức năng quản trị tại URL sau:

<https://insecure-website.com/administrator-panel-yb556>

Kẻ tấn công có thể không đoán được trực tiếp điều này. Tuy nhiên, ứng dụng vẫn có thể rò rỉ URL cho người dùng. URL có thể được tiết lộ trong JavaScript xây dựng giao diện người dùng dựa trên vai trò của người dùng:

<script>

var isAdmin = false;

if (isAdmin) {

...

var adminPanelTag = document.createElement('a');

adminPanelTag.setAttribute('href', 'https://insecure-website.com/administrator-panel-yb556');

adminPanelTag.innerText = 'Admin panel';

...

}

</script>

Tập lệnh này thêm liên kết đến UI của người dùng nếu họ là người dùng quản trị. Tuy nhiên, tập lệnh chứa URL sẽ hiển thị cho tất cả người dùng bất kể vai trò của họ.

- PHƯƠNG PHÁP KIỂM TRA TRUY CẬP DỰA TRÊN THAM SỐ

Một số ứng dụng xác định quyền truy cập hoặc vai trò của người dùng khi đăng nhập, sau đó lưu trữ thông tin này ở vị trí do người dùng kiểm soát. Có thể là:

* A hidden field.
* A cookie.
* A preset query string parameter.

Ứng dụng đưa ra quyết định kiểm soát truy cập dựa trên giá trị được gửi. Ví dụ:

https://insecure-website.com/login/home.jsp?admin=true

<https://insecure-website.com/login/home.jsp?role=1>

Cách tiếp cận này không an toàn vì người dùng có thể sửa đổi giá trị và truy cập vào chức năng mà họ không được phép, chẳng hạn như chức năng quản trị.

- KIỂM SOÁT TRUY CẬP BỊ HỎNG DO CẤU HÌNH NỀN TẢNG KHÔNG ĐÚNG

Một số ứng dụng thực thi kiểm soát truy cập ở lớp nền tảng. Chúng thực hiện điều này bằng cách hạn chế quyền truy cập vào các URL và phương thức HTTP cụ thể dựa trên vai trò của người dùng. Ví dụ: một ứng dụng có thể định cấu hình quy tắc như sau:

DENY: POST, /admin/deleteUser, managers

Quy tắc này từ chối quyền truy cập vào POST phương thức trên URL /admin/deleteUser, đối với người dùng trong nhóm quản lý. Nhiều thứ có thể xảy ra sai sót trong tình huống này, dẫn đến việc bỏ qua kiểm soát truy cập.

Một số khung ứng dụng hỗ trợ nhiều tiêu đề HTTP không chuẩn có thể được sử dụng để ghi đè URL trong yêu cầu gốc, chẳng hạn như X-Original-URL và X-Rewrite-URL. Nếu một trang web sử dụng các điều khiển giao diện người dùng nghiêm ngặt để hạn chế quyền truy cập dựa trên URL, nhưng ứng dụng cho phép ghi đè URL thông qua tiêu đề yêu cầu, thì có thể bỏ qua các điều khiển truy cập bằng cách sử dụng một yêu cầu như sau:

POST / HTTP/1.1

X-Original-URL: /admin/deleteUser

...

\* Note:

X-Original-URL:

Header này chứa URL gốc mà client đã yêu cầu. Nó được gửi khi có sự thay đổi URL, ví dụ như khi reverse proxy chuyển hướng một yêu cầu đến một URL khác.

Mục đích của X-Original-URL là để giữ thông tin về URL ban đầu mà client yêu cầu, trước khi có bất kỳ sự thay đổi hoặc rewrite nào xảy ra trong quá trình xử lý của server.

X-Rewrite-URL:

Header này được sử dụng trong trường hợp URL bị rewrite (thay đổi) trong quá trình xử lý bởi server. URL này có thể là một đường dẫn mới mà server sẽ trả về cho client, hoặc là URL mà server xử lý sau khi có sự thay đổi từ reverse proxy.

Nó thường được sử dụng trong các tình huống mà yêu cầu gốc cần phải được điều chỉnh, chẳng hạn như khi có quy tắc rewrite URL trong cấu hình của server hoặc proxy.

Ví dụ:

Một request từ client có thể yêu cầu URL example.com/old-path, nhưng vì một quy tắc rewrite trong server hoặc proxy, server có thể chuyển hướng yêu cầu này đến example.com/new-path.

Khi đó:

X-Original-URL sẽ lưu example.com/old-path.

X-Rewrite-URL sẽ lưu example.com/new-path.

Điều này giúp các hệ thống hoặc các dịch vụ bên ngoài có thể hiểu được lịch sử thay đổi URL và giúp các hệ thống xử lý yêu cầu một cách chính xác.

Một cuộc tấn công thay thế liên quan đến phương thức HTTP được sử dụng trong yêu cầu. Các điều khiển giao diện người dùng được mô tả trong các phần trước hạn chế quyền truy cập dựa trên URL và phương thức HTTP. Một số trang web chấp nhận các phương thức yêu cầu HTTP khác nhau khi thực hiện một hành động. Nếu kẻ tấn công có thể sử dụng phương thức GET (hoặc phương thức khác) để thực hiện các hành động trên một URL bị hạn chế, chúng có thể bỏ qua quyền kiểm soát truy cập được triển khai ở lớp nền tảng.

- KIỂM SOÁT TRUY CẬP BỊ HỎNG DO SỰ KHÔNG KHỚP URL

Các trang web có thể khác nhau về mức độ nghiêm ngặt khi khớp đường dẫn của yêu cầu đến với điểm cuối đã xác định. Ví dụ: chúng có thể chấp nhận chữ hoa không nhất quán, do đó yêu cầu đến /ADMIN/DELETEUSER vẫn có thể được ánh xạ đến điểm cuối /admin/deleteUser. Nếu cơ chế kiểm soát truy cập ít chấp nhận hơn, nó có thể coi đây là hai điểm cuối khác nhau và không thực thi đúng các hạn chế do đó.

Những sự khác biệt tương tự có thể phát sinh nếu các nhà phát triển sử dụng khung Spring đã bật tùy chọn useSuffixPatternMatch. Điều này cho phép các đường dẫn có phần mở rộng tệp tùy ý được ánh xạ đến điểm cuối tương đương không có phần mở rộng tệp. Nói cách khác, yêu cầu đến /admin/deleteUser.anything vẫn sẽ khớp với mẫu /admin/deleteUser. Trước Spring 5.3, tùy chọn này được bật theo mặc định.

Trên các hệ thống khác, bạn có thể gặp phải sự khác biệt về việc /admin/deleteUser và /admin/deleteUser/ có được coi là các điểm cuối riêng biệt hay không. Trong trường hợp này, bạn có thể bỏ qua các biện pháp kiểm soát truy cập bằng cách thêm dấu gạch chéo vào đường dẫn.

- LEO THANG ĐẶC QUYỀN THEO CHIỀU NGANG

Việc leo thang đặc quyền theo chiều ngang xảy ra nếu người dùng có thể truy cập vào các tài nguyên thuộc về người dùng khác, thay vì tài nguyên của riêng họ cùng loại. Ví dụ: nếu một nhân viên có thể truy cập vào hồ sơ của những nhân viên khác cũng như hồ sơ của riêng họ, thì đây là leo thang đặc quyền theo chiều ngang.

Các cuộc tấn công leo thang đặc quyền theo chiều ngang có thể sử dụng các loại phương pháp khai thác tương tự như leo thang đặc quyền theo chiều dọc. Ví dụ: người dùng có thể truy cập vào trang tài khoản của riêng họ bằng URL sau:

https://insecure-website.com/myaccount?id=123

Nếu kẻ tấn công sửa đổi giá trị tham số id thành giá trị của người dùng khác, chúng có thể truy cập vào trang tài khoản của người dùng khác và dữ liệu cũng như chức năng liên quan.

Lưu ý:

Đây là ví dụ về lỗ hổng tham chiếu đối tượng trực tiếp không an toàn (IDOR). Loại lỗ hổng này phát sinh khi các giá trị tham số của bộ điều khiển người dùng được sử dụng để truy cập trực tiếp vào tài nguyên hoặc chức năng.

Trong một số ứng dụng, tham số có thể khai thác không có giá trị dự đoán được. Ví dụ, thay vì một số tăng dần, một ứng dụng có thể sử dụng mã định danh duy nhất toàn cầu (GUID) để xác định người dùng. Điều này có thể ngăn chặn kẻ tấn công đoán hoặc dự đoán mã định danh của người dùng khác. Tuy nhiên, các GUID thuộc về những người dùng khác có thể được tiết lộ ở nơi khác trong ứng dụng nơi người dùng được tham chiếu, chẳng hạn như tin nhắn hoặc đánh giá của người dùng.

Trong một số trường hợp, ứng dụng phát hiện khi người dùng không được phép truy cập tài nguyên và trả về chuyển hướng đến trang đăng nhập. Tuy nhiên, phản hồi chứa chuyển hướng vẫn có thể bao gồm một số dữ liệu nhạy cảm thuộc về người dùng mục tiêu, do đó cuộc tấn công vẫn thành công.

- LEO THANG ĐẶC QUYỀN THEO CHIỀU NGANG SANG CHIỀU DỌC

Thông thường, một cuộc tấn công leo thang đặc quyền theo chiều ngang có thể được chuyển thành một cuộc leo thang đặc quyền theo chiều dọc, bằng cách xâm phạm một người dùng có đặc quyền cao hơn. Ví dụ, một cuộc leo thang theo chiều ngang có thể cho phép kẻ tấn công đặt lại hoặc lấy được mật khẩu của người dùng khác. Nếu kẻ tấn công nhắm mục tiêu vào một người dùng quản trị và xâm phạm tài khoản của họ, thì họ có thể giành được quyền truy cập quản trị và do đó thực hiện leo thang đặc quyền theo chiều dọc.

Kẻ tấn công có thể truy cập vào trang tài khoản của người dùng khác bằng cách sử dụng kỹ thuật can thiệp tham số đã được mô tả cho cuộc leo thang đặc quyền theo chiều ngang:

https://insecure-website.com/myaccount?id=456

Nếu người dùng mục tiêu là quản trị viên ứng dụng, thì kẻ tấn công sẽ có quyền truy cập vào trang tài khoản quản trị. Trang này có thể tiết lộ mật khẩu của quản trị viên hoặc cung cấp phương tiện để thay đổi mật khẩu hoặc có thể cung cấp quyền truy cập trực tiếp vào chức năng có đặc quyền.

- THAM CHIẾU ĐỐI TƯỢNG TRỰC TIẾP KHÔNG AN TOÀN

Tham chiếu đối tượng trực tiếp không an toàn (IDOR) là một tiểu thể loại của lỗ hổng kiểm soát truy cập. IDOR xảy ra nếu một ứng dụng sử dụng dữ liệu đầu vào do người dùng cung cấp để truy cập trực tiếp vào các đối tượng và kẻ tấn công có thể sửa đổi dữ liệu đầu vào để có được quyền truy cập trái phép. Nó đã trở nên phổ biến khi xuất hiện trong Top Ten của OWASP 2007. Đây chỉ là một ví dụ về nhiều lỗi triển khai có thể cung cấp phương tiện để vượt qua các biện pháp kiểm soát truy cập.

- LỖ HỔNG KIỂM SOÁT TRUY CẬP TRONG QUY TRÌNH NHIỀU BƯỚC

Nhiều trang web triển khai các chức năng quan trọng qua một loạt các bước. Điều này thường xảy ra khi:

* Cần nắm bắt nhiều đầu vào hoặc tùy chọn khác nhau.
* Người dùng cần xem xét và xác nhận thông tin chi tiết trước khi thực hiện hành động.

Ví dụ: chức năng quản trị để cập nhật thông tin chi tiết về người dùng có thể bao gồm các bước sau:

* Tải biểu mẫu có chứa thông tin chi tiết về một người dùng cụ thể.
* Gửi các thay đổi.
* Xem xét các thay đổi và xác nhận.

Đôi khi, một trang web sẽ triển khai các biện pháp kiểm soát truy cập nghiêm ngặt đối với một số bước này nhưng lại bỏ qua các bước khác. Hãy tưởng tượng một trang web mà các biện pháp kiểm soát truy cập được áp dụng chính xác cho bước đầu tiên và bước thứ hai nhưng không áp dụng cho bước thứ ba. Trang web cho rằng người dùng sẽ chỉ đạt đến bước 3 nếu họ đã hoàn thành các bước đầu tiên, được kiểm soát đúng cách. Kẻ tấn công có thể truy cập trái phép vào chức năng bằng cách bỏ qua hai bước đầu tiên và trực tiếp gửi yêu cầu cho bước thứ ba với các tham số bắt buộc.

- KIỂM SOÁT TRUY CẬP DỰA TRÊN NGƯỜI REFERER

Một số trang web dựa trên tiêu đề Referer được gửi trong yêu cầu HTTP để kiểm soát quyền truy cập. Tiêu đề Referer có thể được thêm vào các yêu cầu của trình duyệt để chỉ ra trang nào đã khởi tạo yêu cầu.

Ví dụ: một ứng dụng thực thi mạnh mẽ quyền kiểm soát quyền truy cập đối với trang quản trị chính tại /admin, nhưng đối với các trang phụ như /admin/deleteUser chỉ kiểm tra tiêu đề Referer. Nếu tiêu đề Referer chứa URL chính /admin, thì yêu cầu được phép.

Trong trường hợp này, tiêu đề Referer có thể bị kẻ tấn công kiểm soát hoàn toàn. Điều này có nghĩa là chúng có thể tạo ra các yêu cầu trực tiếp đến các trang phụ nhạy cảm bằng cách cung cấp tiêu đề Referer bắt buộc và có được quyền truy cập trái phép.

- KIỂM SOÁT TRUY CẬP DỰA TRÊN LOCATION:

Một số trang web thực thi kiểm soát truy cập dựa trên vị trí địa lý của người dùng. Ví dụ, điều này có thể áp dụng cho các ứng dụng ngân hàng hoặc dịch vụ truyền thông nơi luật pháp tiểu bang hoặc hạn chế kinh doanh áp dụng. Các kiểm soát truy cập này thường có thể bị bỏ qua bằng cách sử dụng proxy web, VPN hoặc thao tác các cơ chế định vị địa lý phía máy khách.

\* CÁCH NGĂN CHẶN LỖ HỔNG KIỂM SOÁT TRUY CẬP

Có thể ngăn ngừa các lỗ hổng kiểm soát truy cập bằng cách áp dụng phương pháp phòng thủ chuyên sâu và các nguyên tắc sau:

* Không bao giờ chỉ dựa vào việc che giấu để kiểm soát truy cập.
* Trừ khi tài nguyên được dự định để truy cập công khai, hãy từ chối truy cập theo mặc định.
* Bất cứ khi nào có thể, hãy sử dụng một cơ chế duy nhất trên toàn ứng dụng để thực thi kiểm soát truy cập.
* Ở cấp độ mã, hãy bắt buộc các nhà phát triển khai báo quyền truy cập được phép cho từng tài nguyên và từ chối truy cập theo mặc định.
* Kiểm tra và thử nghiệm kỹ lưỡng các biện pháp kiểm soát truy cập để đảm bảo chúng hoạt động như thiết kế.