**1 SQL Injection**

* Khái niệm:

SQL injection (SQLi) là một lỗ hổng bảo mật web cho phép kẻ tấn công can thiệp vào các truy vấn mà ứng dụng thực hiện đối với cơ sở dữ liệu của ứng dụng. Điều này có thể cho phép kẻ tấn công xem dữ liệu mà thông thường chúng không thể truy xuất được. Dữ liệu này có thể bao gồm dữ liệu thuộc về người dùng khác hoặc bất kỳ dữ liệu nào khác mà ứng dụng có thể truy cập. Trong nhiều trường hợp, kẻ tấn công có thể sửa đổi hoặc xóa dữ liệu này, gây ra những thay đổi liên tục đối với nội dung hoặc hành vi của ứng dụng.

Trong một số trường hợp, kẻ tấn công có thể leo thang tấn công SQL injection để xâm phạm máy chủ cơ sở hoặc cơ sở hạ tầng phụ trợ khác. Nó cũng có thể cho phép chúng thực hiện các cuộc tấn công từ chối dịch vụ.

* Cách phát hiện lỗ hổng SQL injection

Bạn có thể phát hiện SQL injection theo cách thủ công bằng cách sử dụng một tập hợp các bài kiểm tra có hệ thống đối với mọi điểm vào trong ứng dụng. Để thực hiện việc này, bạn thường sẽ gửi:

* Ký tự dấu nháy đơn 'và tìm kiếm lỗi hoặc các bất thường khác.
* Một số cú pháp SQL cụ thể đánh giá theo giá trị cơ sở (gốc) của điểm nhập và một giá trị khác, đồng thời tìm kiếm sự khác biệt có hệ thống trong phản hồi của ứng dụng.
* Các điều kiện Boolean như OR 1=1và OR 1=2, và tìm kiếm sự khác biệt trong phản hồi của ứng dụng.
* Tải trọng được thiết kế để kích hoạt độ trễ thời gian khi được thực hiện trong truy vấn SQL và tìm kiếm sự khác biệt về thời gian phản hồi.
* Tải trọng OAST được thiết kế để kích hoạt tương tác mạng ngoài băng tần khi được thực hiện trong truy vấn SQL và giám sát mọi tương tác phát sinh.

Lỗ hổng SQL injection có thể xảy ra ở bất kỳ vị trí nào trong truy vấn và trong các loại truy vấn khác nhau. Một số vị trí phổ biến khác mà SQL injection phát sinh là:

* Trong UPDATE các câu lệnh, trong các giá trị được cập nhật hoặc WHERE mệnh đề.
* Trong INSERT các câu lệnh, bên trong các giá trị được chèn vào.
* Trong SELECT các câu lệnh, bên trong tên bảng hoặc cột.
* Trong SELECT các câu lệnh, trong ORDER BY mệnh đề.

Blind SQL Injection

Tiêm SQL mù xảy ra khi một ứng dụng dễ bị tấn công bởi SQL injection, nhưng phản hồi HTTP của nó lại không chứa kết quả của truy vấn SQL có liên quan hoặc thông tin chi tiết về bất kỳ lỗi cơ sở dữ liệu nào.

Nhiều kỹ thuật như UNION tấn công không hiệu quả với lỗ hổng blind SQL injection. Điều này là do chúng dựa vào khả năng xem kết quả của truy vấn được tiêm trong phản hồi của ứng dụng. Vẫn có thể khai thác blind SQL injection để truy cập dữ liệu trái phép, nhưng phải sử dụng các kỹ thuật khác nhau.

* Các cách khai thác:
* Khai thác SQL injection mù bằng cách kích hoạt phản hồi có điều kiện.
* Tiêm SQL dựa trên lỗi

+ Khai thác lỗi SQL injection mù bằng cách kích hoạt lỗi có điều kiện.

+ Trích xuất dữ liệu nhạy cảm thông qua các thông báo lỗi SQL chi tiết.

* Khai thác lỗi SQL injection mù bằng cách kích hoạt độ trễ thời gian
* Khai thác SQL injection mù bằng kỹ thuật out-of-band (OAST)
* Tiêm SQL trong các bối cảnh khác nhau
* Tiêm SQL bậc hai

**CVE-2024-48813**

**Firmware info:**

Tên ứng dụng: Taskmatic

Loại lỗ hổng: SQL Injection

Phiên bản xây dựng: Taskmatic 1.0

Liên kết tải xuống: <https://www.sourcecodester.com/download-code?nid=17217&title=PHP+Task+Management+System+Free+Download>

**Description and Impact**

Lỗ hổng tiêm SQL trong employee-management-system-php-and-mysql-free-download.html taskmatic 1.0 cho phép kẻ tấn công từ xa thực thi mã tùy ý thông qua tham số admin\_id của thành phần /update-employee.php.

**Steps to reprocedure**

* Đăng nhập vào cổng thông tin.
* Sử dụng brute suite để chặn bắt gói tin ‘GET /update-employee.php?admin\_id=’.
* Truyền payload vào để khai thác.

**POC:**

**A screenshot of a computer

Description automatically generated**

Quan sát thấy rằng lệnh inject xuất hiện bên trong một chuỗi được trích dẫn đơn.

**A screenshot of a computer

Description automatically generated**

Gửi yêu cầu. Xác nhận thấy không còn nhận được lỗi nữa. Điều này cho thấy rằng truy vấn hiện đã hợp lệ về mặt cú pháp.

**A screenshot of a computer

Description automatically generated**

**A screenshot of a computer

Description automatically generated**

Sử dụng SQL Map để khai thác lỗ hổng SQL trên:

**A computer screen shot of a program

Description automatically generated**

**A screenshot of a computer program

Description automatically generated**

**A screenshot of a computer program

Description automatically generated**

**A screenshot of a computer

Description automatically generated**