## **I.SQL Injection là gì?**

- SQL Injection là một kỹ thuật lợi dụng vào các lỗ hổng liên quan đến câu chuyện truy vấn của các ứng dụng. Việc này sẽ được thực hiện bằng cách chèn thêm một đoạn SQL để làm sai lệnh đi các câu truy vấn ban đầu, từ đó sẽ khai thác các dữ liệu từ database.

## **II.Các loại SQL Injection**

- SQL Injection có ba loại: In-band SQLi (Classic), Inferential SQLi (Blind) và Out-of-band SQLi.

### **In-band SQLi**

- Đây là dạng tấn công phổ biến nhất và cũng dễ để khai thác lỗ hổng SQL Injection nhất

- Xảy ra khi hacker có thể tổ chức tấn công và thu thập kết quả trực tiếp trên cùng một kênh liên lạc

-In-Band SQLi chia làm 2 loại chính:

|  |  |
| --- | --- |
| **Error-based SQLi** | **Union-based SQLi** |
| -Hacker  sẽ cài một đoạn mã độc để hệ thống cơ sở dữ liệu báo lỗi. Hacker có thể dùng dữ liệu được cung cấp bởi các thông báo lỗi này để thu thập thông tin về cấu trúc của cơ sở dữ liệu. | Kỹ thuật này lợi dụng toán tử UNION SQL hacker sẽ tiến hành hợp nhất các câu lệnh được tạo ra từ cơ sở dữ liệu để thu được một HTTP response. Trong response sẽ chứa thông tin riêng tư mà kẻ tấn công nhắm đến. |

### **2. Inferential (Blind) SQLi**

- Không giống như In-band SQLi, Inferential SQL Injection tốn nhiều thời gian hơn cho việc tấn công do không có bất kì dữ liệu nào được thực sự trả về thông qua web application và hacker thì không thể theo dõi kết quả trực tiếp như kiểu tấn công In-band.

- Thay vào đó, kẻ tấn công sẽ cố gắng xây dựng lại cấu trúc cơ sở dữ liệu bằng việc gửi đi các payloads, dựa vào kết quả phản hồi của web application và kết quả hành vi của database server.

-Inferential SQLi chia làm 2 loại chính:

|  |  |
| --- | --- |
| Boolean | Time-based |
| Hacker gửi một truy vấn SQL đến Server, làm ứng dụng trả về một kết quả. Kết quả có thể là True hay False. Tuỳ thuộc kết quả trả về của câu truy vấn mà HTTP reponse có thể thay đổi, hoặc giữ nguyên | Cách thức tấn công này cũng tương tự như Boolean. Thay vì đợi cơ sở dữ liệu đưa ra đáp án, hacker sẽ dùng những câu lệnh truy vấn làm server ngừng hoạt động trong vài giây trước khi phản hồi. Thời gian phản hồi (ngay lập tức hay trễ theo khoảng thời gian được set) cho phép kẻ tấn công suy đoán kết quả truy vấn là TRUE hay FALSE |

### **2.3Out-of-band SQLi**

- Out-of-band SQLi không phải dạng tấn công phổ biến, chủ yếu bởi vì nó phụ thuộc vào các tính năng được bật trên Database Server được sở dụng bởi Web Application.

-Kiểu tấn công này xảy ra khi hacker không thể trực tiếp tấn công và thu thập kết quả trực tiếp trên cùng một kênh (In-band SQLi), và đặc biệt là việc phản hồi từ server là không ổn định.

-Kiểu tấn công này phụ thuộc vào khả năng server thực hiện các request DNS hoặc HTTP để chuyển dữ liệu cho kẻ tấn công

## **III.Sự nguy hiểm của SQL Injection**

- Hack tài khoản cá nhân của người khác.

- Ăn cắp hoặc sao chép dữ liệu của trang web hoặc hệ thống.

- Thay đổi dữ liệu nhạy cảm của hệ thống.

- Xóa dữ liệu nhạy cảm và quan trọng của hệ thống.

- Người dùng có thể đăng nhập vào ứng dụng với tư cách người dùng khác, ngay cả với tư cách quản trị viên.

- Người dùng có thể xem thông tin cá nhân thuộc về những người dùng khác, ví dụ chi tiết hồ sơ của người dùng khác, chi tiết giao dịch của họ,...

- Người dùng có thể sửa đổi cấu trúc của cơ sở dữ liệu, thậm chí xóa các bảng trong cơ sở dữ liệu ứng dụng.

- Người dùng có thể kiểm soát máy chủ cơ sở dữ liệu và thực thi lệnh theo ý muốn.

## **IV.Các cách ngăn chặn SQL Injection**

### **1.Input Validation (Xác thực đầu vào)**

Quá trình xác thực nhằm xác minh xem loại input do người dùng gửi có hợp lệ hay không. Xác thực đầu vào đảm bảo đó là kiểu, độ dài, định dạng… được chấp nhận. Chỉ các giá trị qua được xác thực mới có thể được xử lý. Nó giúp chống lại mọi lệnh được chèn vào trong chuỗi input.

### **Parametrized queries (Tham số hóa truy vấn)**

Các truy vấn tham số hóa là một phương tiện pre-compile lệnh SQL. Sau đó bạn có thể cung cấp các tham số để câu lệnh được thực thi.

Phương pháp này giúp Cơ sở dữ liệu có thể nhận ra mã và phân biệt nó với dữ liệu đầu vào.

Input của người dùng được trích dẫn tự động, và kiểu mã hóa này giúp giảm thiểu tấn công SQL injection

### **Stored Procedures**

Các stored procedures (SP) yêu cầu developer nhóm một hay nhiều lệnh SQL thành một đơn vị logic để có thể tạo một kế hoạch thực thi. Các lần thực thi tiếp theo cho phép các lệnh được tham số hóa tự động. Nói một cách đơn giản, nó là một loại code có thể được lưu trữ để sử dụng sau này

### **Sử dụng Escaping**

Luôn sử dụng các hàm character-escaping cho input do user cung cấp, được cấp bởi mỗi hệ thống quản lý Cơ sở dữ liệu (DBMS). Việc này giúp đảm bảo DBMS không bao giờ nhầm lẫn nó với lệnh SQL do developer cung cấp