SQL Injection

**Lỗ hổng SQL injection**

Là một lỗ hổng bảo mật web, cho phép attacker can thiệp vào các câu truy vấn của ứng dụng thực hiện với database của nó; cho phép attacker xem những dữ liệu – thuộc về người dùng hoặc dữ liệu của ứng dụng thường mà họ không thể xem được. Trong nhiều trường hợp, attacker có thể xóa, sửa các dữ liệu và gây ra những thay đổi bất lợi với nhà sản xuất và người sử dụng.

Attacker có thể thực hiện tấn công để xâm nhập vào máy chủ bên dưới hoặc cơ sở hạ tầng back-end hoặc thực hiện tấn công DoS.

**Tại sao lại xảy ra lỗ hổng**

**Các loại SQLi**

SQLi chia thành 3 loại dựa trên phương pháp tấn công và độ thiệt hai là in—band SQLi (cơ bản), inferential SQLi (blind) và out-of-band SQLi.

**In-band SQLi**

Attacker sử dụng cùng 1 kênh giao tiếp để thực hiện tấn công và lấy kết quả. Sự đơn giản và hiệu quả của In-band SQLi khiến nó trở thành 1 trong những kiểu tấn công SQLi phổ biến nhất. Có 2 loại biến thể phụ của kiểu tấn công này:

* Error-based SQLi : attacker thực hiện các hành động khiến cho database tạo ra thông báo lỗi. Attacker có thể sử dụng các dữ liệu được cung cấp bởi những thông báo lỗi để thu thập thông tin về cấu trúc của database.
* Union-based SQLi: kỹ thuật này tận dụng lợi thế của toán tử UNION, toán tử này kết hợp nhiều câu lệnh truy vấn lựa chọn được tạo bởi dtb để nhận được 1 phản hổi HTTP duy nhất. Phản hồi này có thể chứa những dữ liệu mà attacker có thể sử dụng

**Inferential (blind) SQLi**

Attacker gửi các payload chứa dữ liệ đến máy chủ và quan sát phản ứng; hành vi cả máy chủ để tìm hiểu về cấu trúc của nó. Phương pháp này được gọi là blind SQLi bởi vì dữ liệu không chuyển từ dtb của trang web đến attacker, do đó attacker không thể xem thông tin về cuộc tấn công trong băng tần

Blind SQLi dự trên phản hồi và hành vi của máy chủ, vì thế chúng thường chậm hơn để thực thi nhưng có thể gây hại tương tự. Blind SQLi có thể được phân loại như sau:

* Boolean: attacker gửi những câu truy vấn đến dtb nhắc ứng dụng trả về 1 kết quả. Kết quả sẽ khác nhay tùy thuộc vào câu truy vấn đúng hay sai. Dựa trên kết quả, thông tin trong phản hồi HTTP sẽ được thay đổi hoặc không. Sau đó, attacker có thể tìm hiểu thông báo tạo ra kết quả đúng hay sai.
* Time-based: attacker gửi những câu truy vấn SQL tới dtb, những câu truy vấn này làm cho dtb đợi (trong vài giây) trước khi nó có thể phản ứng. Từ thời gian phản hồi của dtb, attacker có thể thấy những câu truy vấn đấy là đúng hay sai. Dựa vào kết quả, 1 phản hồi HTTP sẽ được tạo ra ngay lập tức hoặc sau 1 khoảng thời gian chờ đợi. Do đó, attacker có thể tìm ra liệu rằng thông báo mà họ đã sử dụng được trả về đúng hay sai, mà không cần dựa vào dữ liệu từ dtb.

**Cách khắc phục lỗ hổng**

**Tài liệu tham khảo**

<https://www.imperva.com/learn/application-security/sql-injection-sqli/>