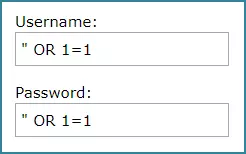
SQL Injection là kỹ thuật của người dùng độc hại nhằm phá hoại cơ sở dữ liệu bằng cách thêm các câu lệnh SQL inject vào trong câu lệnh SQL thông thường thông qua trường nhập liệu trên web. Những câu lệnh Inject có thể thay đổi câu lệnh SQL. Điều đó gây nguy hiểm cho an toàn, bảo mật của hệ thống, đánh cắp các thông tin nhạy cảm và có giá trị đối với doanh nghiệp. Khi cơ sở dữ liệu xuất hiện lỗ hổng, kẻ xấu có thể tấn công bằng 1=1 luôn đúng hoặc = luôn đúng.

Ví dụ:



SELECT \* FROM Users WHERE Name ="" OR 1=1 AND Pass ="" OR 1=1

Để bảo vệ cơ sở dữ liệu trước những cuộc tấn công SQL Injection, ta sử dụng tham số SQL. Tham số SQL là giá trị được thêm vào từ truy vấn SQl ở thời gian thực hiện trong cách thức có thể kiểm soát. Công cụ SQL kiểm tra các thông số, đảm bảo chắc chắn đúng với cột và được thực thi chứ không phải là một phần SQL được thực thi.

Ngoài ra việc cộng thêm chuỗi vào cũng tạo ra lỗ hổng cho cơ sở dữ liệu và kẻ xấu có thể thêm cơ hội tấn công. Do đó nên sử dụng parameter. Nếu như dữ liệu input không hợp pháp thì sẽ tự động báo lỗi mà không cần check.