SQL Injection

Introduction

SQL injection attack is to insert malicious SQL query or add statement into the input parameters of the application, and then parse and execute the attack in the background SQL server. It is one of the most common means for hackers to attack the database at present.

Methods

* Guess the background database, this is the most use of the way to steal sensitive information site.
* Bypass authentication, column such as bypass verification login site background.
* Injection can use database stored procedures for weight lifting and other operations

UNION injection attack

The SQL UNION operator

The result set used to merge two or more SELECT statements; the internal SELECT statements must have the same number of columns.And have similar data types.

The default UNION operator picks different values, and if duplicate values are allowed, UNION ALL is used

UNION SELECT EXPLANATION:

A joint query with two previous and subsequent query statements that must contain the same column.

Applicable conditions: there are direct data display bits on the page.

Basic steps:

Look for injection point

Use the ORDER BY command to determine the number of columns in the dataset.

UNION SELECT 1,2,3,4...To determine which column the display bit is in. (Note: the query before UNION needs to return null value)

Gets the current database name, table name, column name, all data.