

Forum:[Hack Forums](#)

Thread: [SQL Injection - An Explanation and Guide](#)

Koyote - February 1, 2023, 1:53 am

What is SQL Injection?

SQL injection is a type of security vulnerability that allows an attacker to inject malicious code into a web application's SQL (Structured Query Language) statement. This allows the attacker to manipulate the underlying database, potentially exposing sensitive information or allowing unauthorised access to the system.

SQL injection attacks can occur when a web app takes user inputted data and incorporates it into an SQL statement without properly validating or sanitising it. This can allow an attacker to craft a malicious input that causes the SQL statement to behave in unintended ways, such as bypassing authentication or revealing sensitive data.

How do you Perform SQL Injection?

1. Identify the target: Find a web application that is vulnerable to SQL injection, either through manual testing or using a tool like sqlmap or Havij.

2. Craft a malicious payload: Construct an SQL statement that will be injected into the web application, using special characters or other techniques to manipulate the statement and expose sensitive information or gain unauthorized access.

3. Inject the payload: Inject the malicious SQL statement into the web application by sending it as part of a user input field, such as a search query or login form.

4. Monitor the results: Observe the results of the injection, looking for evidence of a successful attack, such as error messages that reveal sensitive information or successful logins to restricted areas of the web application.

What SQL Injection Tools are Available?

sqlmap: An open-source tool for automatically detecting and exploiting SQL injection vulnerabilities in web applications.

Havij: A proprietary tool for automated SQL injection that supports multiple injection techniques and includes features such as loadable plugins and a user-friendly graphical interface.

Burp Suite: A comprehensive suite of tools for web application security testing, including a module for performing SQL injection attacks.

OWASP ZAP: An open-source web application security scanner that includes a module for performing SQL injection attacks.

SQLNinja: An open-source tool for performing SQL injection attacks against Microsoft SQL Server databases.

paragram - February 21, 2023, 1:53 pm

I've always wanted to learn about SQL injections but never had the time, thanks for sharing this small bit of info.

JustGuys - December 27, 2023, 6:38 pm

thank you for this explantion really needed this