Cheatography

SQL Injection Attacks: Concepts, Tools, Techniques Cheat Sheet

by ironclad via cheatography.com/36781/cs/11566/

Description

SQL Injection is the act of inserting data into an SQL query through the input data given to an application by a client.

Causes

Lack of input validation

Usage of untrusted code

Lack of adherence to best practices

Server configuration issues

Client-provided information used in query

Structure of an SQL Query

select <col> from <table> where <field> = <value>;

In this case: col, table, field, and value are all places where injection could happen.

Escaping the Intent of the Query

SELECT name, pass FROM users WHERE user_id = "'" + **$id** + "'";

Input	Result
%' or '1'='1	All names and passwords
1' UNION SELECT 1, @@version -- -	A name and MySQL Version
1' UNION SELECT distinct(table_schema),null FROM information_schema.tables	All Schema Information

State of the Art - Latest Techniques

SQL Injection through Ads	Forces compromised server to serve the attacker's ads
Chaining of Attacks	Utilizing techniques such as camel-casing, escape characters and character codes to get around protections
Information Schema	Dumping the Information Schema to learn more about the database
Multi-Line Comments	Using multi-line comments (/**/) to bypass defensive techniques
Obfuscation	Utilizing obfuscation to mask attacks
SQL Union	Using SQL UNION along with attacks above to mask attacks

Successful Attacks May

Modify Database Data

Read Sensitive Information

Execute Operations as an Administrator

Recover Files Present on the Database System

Issue Commands to the Database System's OS

Why?

In many applications, direction access to the database is the easiest means of access. Thus, a simple form-based authentication or web query may be one step away from interacting with a database. With this knowledge in hand, a skilled attacker could use cleverly crafted SQL queries to gain root level access and further attack the network.

Modern Injection Tools

Havij	User-friendly GUI for automatic SQL Injection
sqlmap	Open source penetration testing tool
Google dorks	Advance web searches that are used to fingerprint web servers
BSQL Hacker	Made for Blind SQL Injection
Mole	Provide the tool with a URL and it does the rest

Mitigation Techniques

Input Validation	Make sure all client-supplied information is sanitized
Use Parameterized Queries	Separates the developer's SQL query from client input
Stored Procedures	Store SQL queries in the database itself and only provide sanitized input
Whitelist Input Validation	Only accept the information you want, make sure it doesn't affect query intent
Front-end/Back-end Design	Don't let the application interact directly with the database
Least Privilege	In the event of a compromise, limit the damage
Patch Your Systems	Keep your servers up to date
Logging	Keep a log of all queries, preferable on a remote server