Ahmed ELMALOUL

16030441006 mis

Report

Introduction:

SQL, or Structured Query Language, is a computer language for managing databases. This includes discovering data quickly, updating it, and deleting it. Several websites, such as e-commerce sites and investment firms, have large databases that store information about millions of customers, and they manage such databases using SQL.

When someone log it into a website that maintains information about them, for example, it may utilize SQL to seek up their usernames in a table and then retrieve related account information. If you make a change to your account (for example, your mailing address), SQL would overwrite each old address in the database and replace it with the new one.

These databases frequently contain sensitive personal data such as phone numbers, email and mailing addresses, as well as credit card and social security numbers (Although very sensitive data must be encrypted rather than stored in plaintext, this is not always the case). Just authorized users should have access to particular database information. Individual users may usually view their own information on a website, whereas a website administrator may have entry to every users' information.

Considering data must be kept someplace, nearly every system & website nowadays uses a database. Because sensitive data is kept in the database, the security of the system is endangered. When data from a personal website or blog is taken, the impact is minor compared to data stolen from its financial system.

Because the primary goal of this assault is to get access to the system's database, the repercussions of this attack can be quite damaging.

SQL injection is a type of code injection that has the potential to seriously damage your database.

SQL injection is amongst one the top frequent web hacking tactics.

SQL injection is that when malicious software is injected into SQL statements through web page inputs.

 SQL injection with Web Pages,

, SQL injection take place, whenever you request a user for information, such as his username/use id, but rather than a name/id, the user provides you a SQL statement that you unintentionally perform in your database

History

During 1998, the very first published discussions regarding SQL injection began to appear; for instance, 1998 article in Phrack Magazine.

Form,

The Open web Application Security Project named SQL injection (SQLI) as one of the top ten web application vulnerabilities in 2007 and 2010.   On the OWASP top ten list in 2013, SQLI was ranked number one.  SQL injection can be divided into four types:

Classic SQLI

Blind or Inference SQL injection

Database management system-specific SQLI

Compounded SQLI

SQL injection + insufficient authentication

SQL injection + DDoS attacks

SQL injection + DNS hijacking

SQL injection + XSS

Characteristics of an SQL injection attack;

By integrating user input to SQL queries, SQL injection attacks seek to leverage web application vulnerabilities. If effective, those attacks can use the legitimate web application connection to run malicious SQL instructions. SQL injection attacks can be difficult to detect since specific steps of an attack, when evaluated apart from the others, may appear to be legitimate.

**Risk Factors**

The platform affected can be:

* Language: SQL
* Platform: Any (requires interaction with a SQL database)

Prerequisites;

basic SQL and PHP.

SQL Injection potentially led to the following outcomes:

* The user might change the database's structure or even destroy tables from the database application.
* The user could take control of the database server and execute commands on it at will.
* The user could take control of the database server and execute commands on it at will.
* Modifying any sensitive information in the system.
* Hacking into someone else's account.

Critical information on the system is being deleted.