Good essay on how to prevent sql injections

Sociology, Violence

Introduction

Structured Query Language (SQL) injection is a code injection technique used in requesting, deleting and updating information from databases. Therefore, it is one of the main web attack mechanism used by hackers to steal data. This attack allows the hacker to inject SQL commands into allowing them access data in a database, as it takes advantage of improper coding in the web applications. This kind of attack bypasses firewalls and endpoint defenses, because web based forms must allow access to databases so as to give some sort of response.

Impacts of SQL

SQL injections pose a serious threats to database servers in computer networks. With SQL injection attack, a malicious user can insert a series of illegal SQL statements into the pre-defined through some input interface. Also, SQL statements can manipulate SQL statements and make them different from the intended use, and the hacker can gain additional information from the accessed database. SQL injections take advantage of the flaws in web application, hence can inject malicious scripts into the database. Such attacks compromise integrity of the database and the exposure of sensitive/ private information. Sometimes the attacker can be able to execute shell commands and read and write out files from the operating system, and this can be disastrous.

SQL injections can be prevented through firewalls, which act as intrusion detection mechanism, as they prevent defense against full scale attacks. Patching programming languages, databases and servers and operating

systems can also be helpful but not the best way in prevention of attacks. Whitelisting and blacklisting can also be used in the prevention of such attacks. Whitelisting examines a list of permitted characters against each piece of users input, on the other hand, blacklisting removes specific, known malicious characters, hence preventing against SQL injections. SQL can also be prevented by reducing attack surface; this get rids of any database functionality that hackers can use to their advantage.