Ministry of Higher Education and Scientific Research

University of Babylon

College of Information Technology

Department of Information Security

Study: Morning

Sql Injection Testing

A Graduate Project Submitted to the department of Information Security of the College of Information Technology, University of Babylon, in Partial Fulfillment of the Requirements for the Bachelor's degree in the Information Security of Information Technology.

By:

Rose Azher Jaber Alkufashi

Supervised by:

Dr. Moayad Najm Abdullah

2023-2024

Abstract

The SQL Injection vulnerability is one of the easiest vulnerabilities that is widespread and easy to exploit. It is usually the target of many ethical hacking testers. It is a vulnerability that exists in the database layer of the system affected by it. It may be formed due to the lack of a filtering system for the inputs to the base from the included symbols and special characters. Within query sentences in the SQL language, the hacker can inject the input fields with commands and query sentences that return a desired value or secret data within the database. The vulnerability is discovered by passing one of these letters or special symbols and receiving an error message or specific suspicious behavior that indicates… The database treated the entry as a programming command that resulted in this error and not a textual entry that was searched for within the database.

The best way to prevent SQL Injections is to use safe programming functions that make SQL Injections impossible: parameterized queries (prepared statements) and stored procedures. Every major programming language currently has such safe functions and every developer should only use such safe functions to work with the database.

Therefore, a successful SQL Injection attack can have very serious consequences. Attackers can use SQL Injections to find the credentials of other users in the database. They can then impersonate these users. The impersonated user may be a database administrator with all database privileges.