Jesse Kniss

CS-405

Module Two SQL Injection

SQL injection is a common web security vulnerability that allows hackers to interfere with queries made to the database by an application. A SQL injection occurs when a program asks users for an input such as a username/password, and the returned input is a SQL statement that changes the way the program behaves. These attacks can allow hackers to view, modify or delete data that they would not normally have access to. (PortSwigger, 2022).

For this assignment, the attacker tries to gain access to the system by suppling an OR statement into the WHERE clause of the SELECT statement. The attacker’s SQL statement submits a Boolean statement for the condition that tricks the database into seeing WHERE name = “Fred” OR 1 = 1. The part of the statement after the OR statement will always evaluate to true, this unlocks the full database for the hacker to view. To prevent this, a copy of the user SQL statement is created, and validated against the original SQL statement. If the two values do not match, then the application displays an error message and stops the process from continuing.

# Works Cited

PortSwigger. (2022, September 5th). *SQL Injection*. Retrieved from Web Security: https://portswigger.net/web-security/sql-injection

Graphical user interface, text

Description automatically generated