FORGE

The Arkansas Cyber Defense Center

SQL Injection Attack

An attack in which the perpetrator uses a vulnerability to interfere with queries in an application's database, which allows the attacker to view data they are not normally able to see.

Why be aware of this attack?

If your business uses online applications, there is a chance you are open to this attack. The result of a successful SQL injection attack can result in unauthorized access to sensitive data (passwords, personal health information, personal identifiable information, financial information, etc.).

Tactics of an SQL injection attack:

- Subverting application logic to gain access to information
- Examining a database to gain more information about its structure
- UNION attacks to retrieve data from different database tables

Prevention tips:

This type of attack is more complicated than others, and the prevention is complicated as well. It is best to leave prevention strategy to a cyber security professional. For example, one strategy for preventing an SQL injection attack is by using parameterized queries instead of string concatenation within a query. The average application user does not know what this means, and therefore, professional advice should be sought.

POWERED BY SBA U.S. Small Business Administration

REPORT A CYBER INCIDENT:

forge.institute/acdc

501-239-9599