SQL Injection Attack & Basic Research

SQL Basics: SQL Tutorial (tutorialspoint.com)

SQL Injection Attack Introduction: https://portswigger.net/web-security/sql-injection

SQL Injection

An SQL injection attack is a web security vulnerability that allows an attacker to interfere with the queries that an application makes to its database. When successful, an attacker can view data that is not supposed to be visible. Sometimes, the attacker is also able to change or delete the data.

SQL injection attacks are often responsible for denial of service attacks.

SQL Injection Examples:

- **Retrieving hidden data-** where you can modify an SQL query to return additional results.
- **Subverting application logic-** where you can change a query to interfere with the application's logic.
- **UNION attacks-** where you can retrieve data from different database tables.
- **Examining the database-** where you can extract information about the version and structure of the database.
- **Blind SQL injection-** where the results of a query you control are not returned in the application's responses.

Example in Websites:

Website

https://insecure-website.com/products?category=Gifts

Injection attack:

https://insecure-website.com/products?category=Gifts'--

This changes the SQL query:

```
SELECT * FROM products WHERE category = 'Gifts' AND released = 1
```

To

```
SELECT * FROM products WHERE category = 'Gifts'--' AND released = 1
```