
SQL
injection

AGENDA

- What is an SQL Injection vulnerability
- An example of SQL Injection
- An analysis of how it works
- impact of SQL injection
- SQL injection mitigation

What Does Sql Injection Mean

- First, there is a software defect
- That defect results in a security vulnerability (or just vulnerability)
- A vulnerability is a weakness for certain types of attacks on the security of the application
- One of the possible attack types is an SQL Injection
- So, if you have a vulnerability that permits SQL Injection attacks, you have an SQL Injection vulnerability
- Why are we talking about this before we know more about security?

The SQL Injection Attack

- SQL is “Structured Query Language”
- It is a standardized language for accessing databases
- Examples
    - select name from employee where ssn=‘123456789’
    - select name, ssn, dob from employee where ssn=‘123456789’ and id=‘31042’
    - select code,name from products where code =‘536’ union select code,name from sales where code > ‘500
- Every programming language implements SQL functionality in its own way

SQL Injection Example DB

Account			
Name	Account	UserID	Password
joi	1234	joi	mypass
Tom M	6787	dorry	tommy
Alex T	6574	hosty	fullfun
Homy H	5432	hommy	gothommy

SQL Injection Example ……

- Assume that the select statement implemented is:
- $acct is the variable containing the account number input by the user (PHP style naming)
- This is a typical usage of a select statement to look up a value

Enter your account number	3215
Your balance	

- Results in:

res = select CBalance from Balances where Acct='3215'

SQL Injection Example …

• If the code block is:

```
res = select CBalance from Balances where Acct=‘$acct’ if res
PrintHTML (res)
```

• Then the application will print whatever is in res.

• The attacker will have valuable information for further attacks, such as issuing a transaction against the account number discovered

An Example Program

• Command line form –
http://www.cs.montana.edu/courses/csci476/code/sqli_ex1_mysql.py –
http://www.cs.montana.edu/courses/csci476/code/sqli_ex1_outputWeb form –
http://www.cs.montana.edu/courses/csci476/code/sqli_form.html –
http://www.cs.montana.edu/courses/csci476/code/sqli_submit.php

impact of SQL injection

- **Data Breach**: Attackers can access sensitive information like personal data, passwords, and credit card details.
- **Data Corruption**: Malicious SQL queries can modify, delete, or corrupt important data.
- **Unauthorized Access**: Attackers might escalate privileges, gaining admin access and controlling the system.
- **Service Disruption**: SQL injection can degrade performance or cause system downtime.
- **Reputation Damage**: Data breaches can damage an organization’s reputation and customer trust.
- **Financial Loss**: Companies may face fines, lawsuits, and loss of revenue due to the breach.

SQL injection mitigation

- **Use Parameterized Queries**: Ensure all SQL queries use parameters instead of directly including user input.
- **Input Validation**: Validate and sanitize all user inputs to prevent malicious data.
- **Least Privilege**: Limit database account privileges to only what's necessary for the application.
- **Error Handling**: Avoid exposing detailed error messages to users.
- **Regular Security Audits**: Continuously test and review applications for vulnerabilities

Thank you