
STOP | THINK | CONNECT
www.stopthinkconnect.org
So you're telling me a Nigerian prince really didn't leave me any money?
STOP. THINK. CONNECT. When in doubt, throw it out!
Avoid clicking on suspicious emails, links & social media posts - even if you know the source.

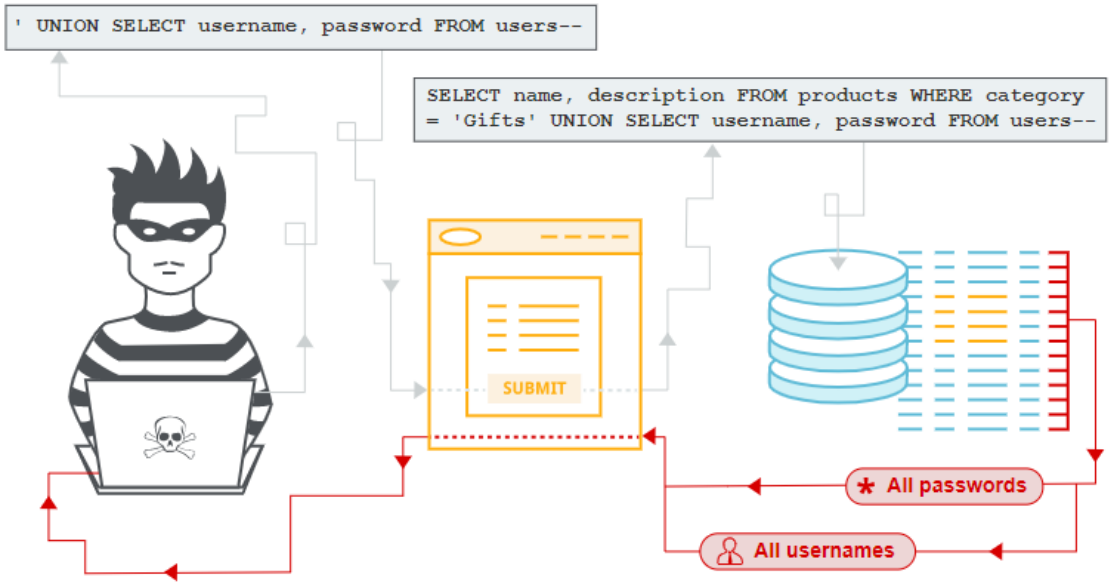
Module 2-8

Data Security

Objectives

- SQL Injection Attack
- Prepared statements
- Hashing
- Salt
- Encryption

SQL Injection attacks



SQL Injection attacks

- Makes it possible to execute malicious SQL statements
  - SQL statements control database server
  - Attackers can bypass authentication and authorization
  - Can add modify and delete records in a database

Preventing SQL Injection

- Parameterized Queries
- Input Validation
- Limit Database User Privileges

The following code is vulnerable to SQL injection because the user input is concatenated directly into the query:

```
String query = "SELECT * FROM products WHERE category = '"+ input + "'";
Statement statement = connection.createStatement();
ResultSet resultSet = statement.executeQuery(query);
```

This code can be easily rewritten in a way that prevents the user input from interfering with the query structure:

```
PreparedStatement statement = connection.prepareStatement("SELECT * FROM products WHERE
category = ?");
statement.setString(1, input);
ResultSet resultSet = statement.executeQuery();
```

Protecting sensitive data

- How many stories have we heard regarding data breaches divulging sensitive information??
- Data stored in a database hacked
- To stop this, we need to have data stored in a database in such a way that it is not readable by unauthorized parties
- Data can be protected by either hashing or encryption

Hashing

- Using an algorithm to map data of any size to a fixed length.
    - Called a hash code or hash value
    - Many different algorithms (MD2, MD4, MD5, SHA, SHA1, SHA2)
- Is a one-way function
    - Technically it is possible to reverse-hash, would require immense computing power therefore unfeasible
- Meant to verify that a file or piece of data has not been altered

```
hash("password") = 2cf24dba5fb0a30e26e83b2ac5b9e29e1b161e5c1fa7425e7
```

Hashing

- Hashed output of the same string will be the same.
- Hashed data conforms to algorithm in terms of storage size
- The stronger hash function used, the more storage required, the slower the performance but minimal change of has collision
- Humans are predictable, passwords tend to be memorable keywords, phrases, or numbers
- Hackers create a “rainbow” table of possible passwords and run this through while trying to hack in
    - Salt

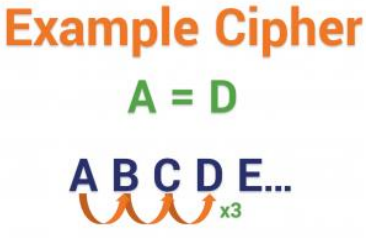
SALT

- Unique value added to end of password to create a different value.
- Adds layer of security to hashing process
    - Helps protect against brute force
- Because salt is unique, produced hash of same password will not be the same.

```
hash(salt . "hello") = 58756879c05c68dfac9866712fad6a93f8146f337a78t
hash(salt . "hello") = c0e81794384491161f1777c232bc6bd9ec38f616560b1
```

Encryption

- Most effective way to achieve data security
- Practice of scrambling information
    - Needs a key to unscramble
- Two-way function



Plaintext: Don't be a jerk

Becomes:

Ciphertext: Grqwehdmhun

Encryption algorithms

- Shift ciphers
- Substitution ciphers
- Transposition ciphers
- Polyalphabetic ciphers
- Nomenclature ciphers

Modern encryption algorithms

- Asymmetric Encryption
  - Public key example – 1 key encrypts, 1 key decrypts
  - Used in SSL/TLS transfer of data
- Symmetric Encryption
  - Closer to form of private key encryption
  - Each party has a key that encrypts and decrypts
  - After asymmetric encryption in SSL handshake, browser and server communicate with symmetric key that is passed along

Digital certificate

- Public key certificate
- Used for encryption and authentication
- Certificate authority (CA) is trusted third-party that provide certificate
    - Prevents attacker from impersonating a server

Man in the Middle Attack

- Attacker intercepts communications between two parties
    - Either to eavesdrop
    - Modify traffic
- Oldest form of cyber attacks
- Not as common as ransomware or phishing, still threat
- Encryption protocols (SSL/TLS) are best way to help protect against

Let’s Code!