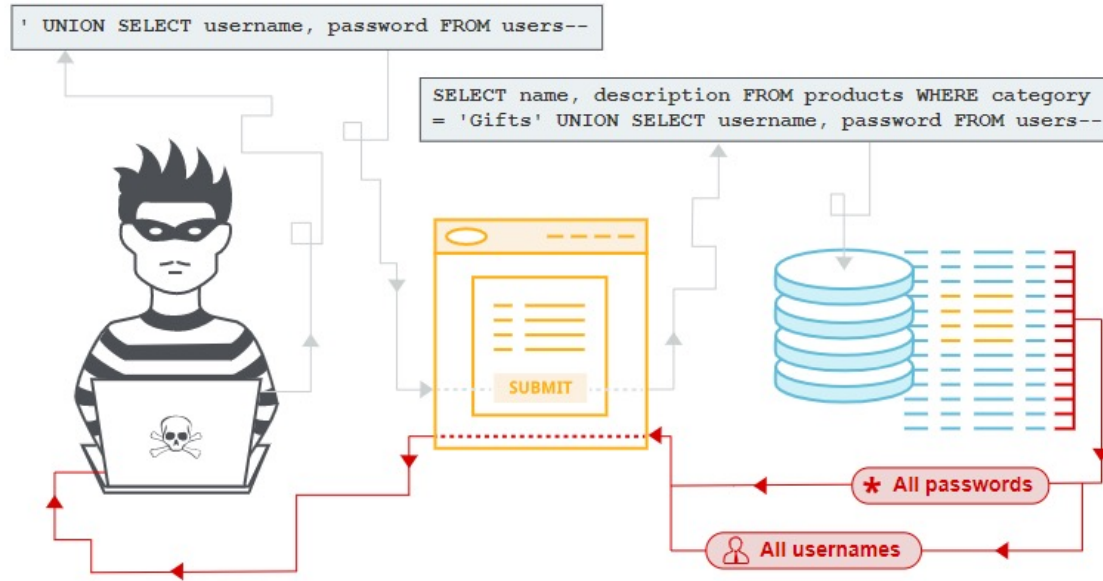# Module 2-8

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

Preventing SQL Injection

- Parameterized Queries

```
String userId = {get data from end user};
String sqlQuery = "select * from tbluser where userId = " + userId;
```

If this is executed with a userId of 132, it will look like this:
SELECT * FROM tbluser WHERE userId=132;

A hacker can alter a user request to send SQL code where the userId says 2 or 1=1;
This will cause the sqlQuery to read:
SELECT * FROM tbluser WHERE userId=2 or 1=1;

Because 1=1 is always true, it will return all data from the table!

Preventing SQL Injection

- Input Validation

Preventing SQL Injection

- Limit Database User Privileges

Preventing SQL Injection

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 chance of having 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("hello")                     = 2cf24dba5fb0a30e26e83b2ac5b9e29e1b161e5c1fa7425e73043362938b9824
hash("hello" + "QxLUF1bgIAdeQX")  = 9e209040c863f84a31e719795b2577523954739fe5ed3b58a75cff2127075ed1
hash("hello" + "bv5PehSMfV11Cd")  = d1d3ec2e6f20fd420d50e2642992841d8338a314b8ea157c9e18477aaef226ab
hash("hello" + "YYLmfY6IehjZMQ")  = a49670c3c18b9e079b9cfaf51634f563dc8ae3070db2c4a8544305df1b60f007
```

Encryption

- Most effective way to achieve data security
- Practice of scrambling information

  - Needs a key to unscramble

- Two-way function
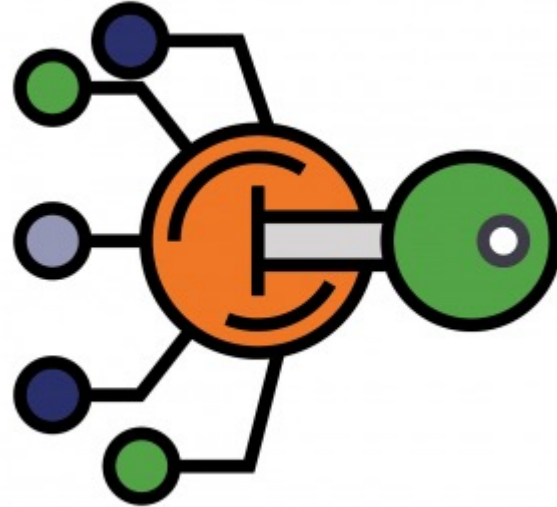
Example Cipher

A = D

A B C D E... x3

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
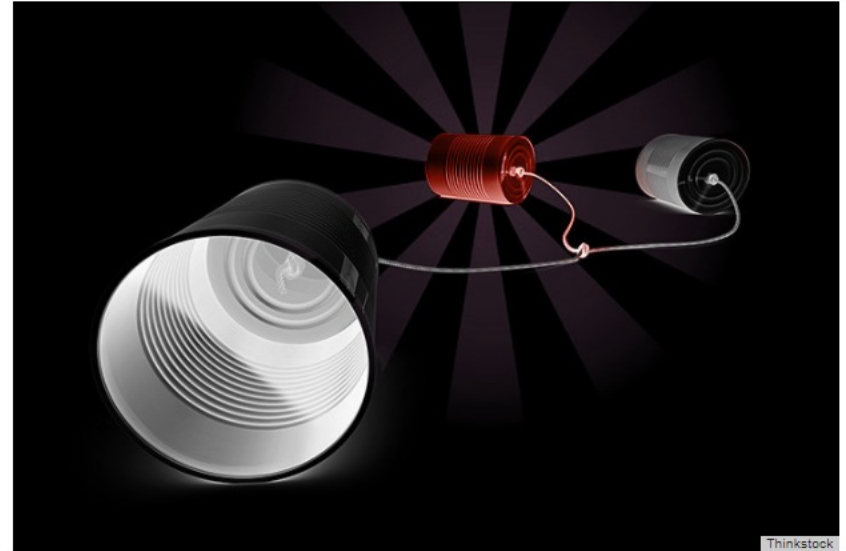
- Symmetric Encryption

  - 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

Thinkstock

Let's Code!