


# SQL Injection

Jaroslav Hlaváč

# About me

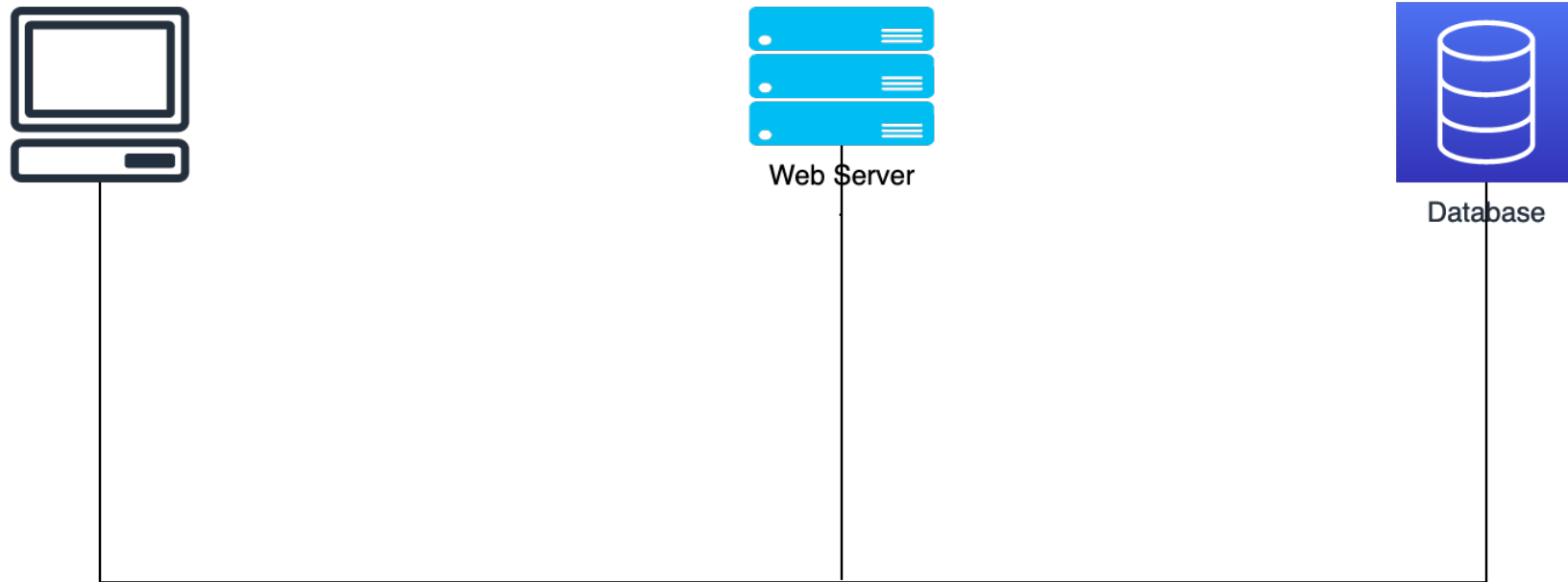
- teaching you for 2 weeks
- PhD student at MFF UK – Behavioural modelling of network entities
- Data Scientist at  Cisco

# Homework

- <https://github.com/fel-communication-security/sql-injection>
- Write me an email with detailed description not only some commands semi-copied from the internet.
- Deadline: ???
- BONUS: who finishes by midnight gets a bonus point 😊

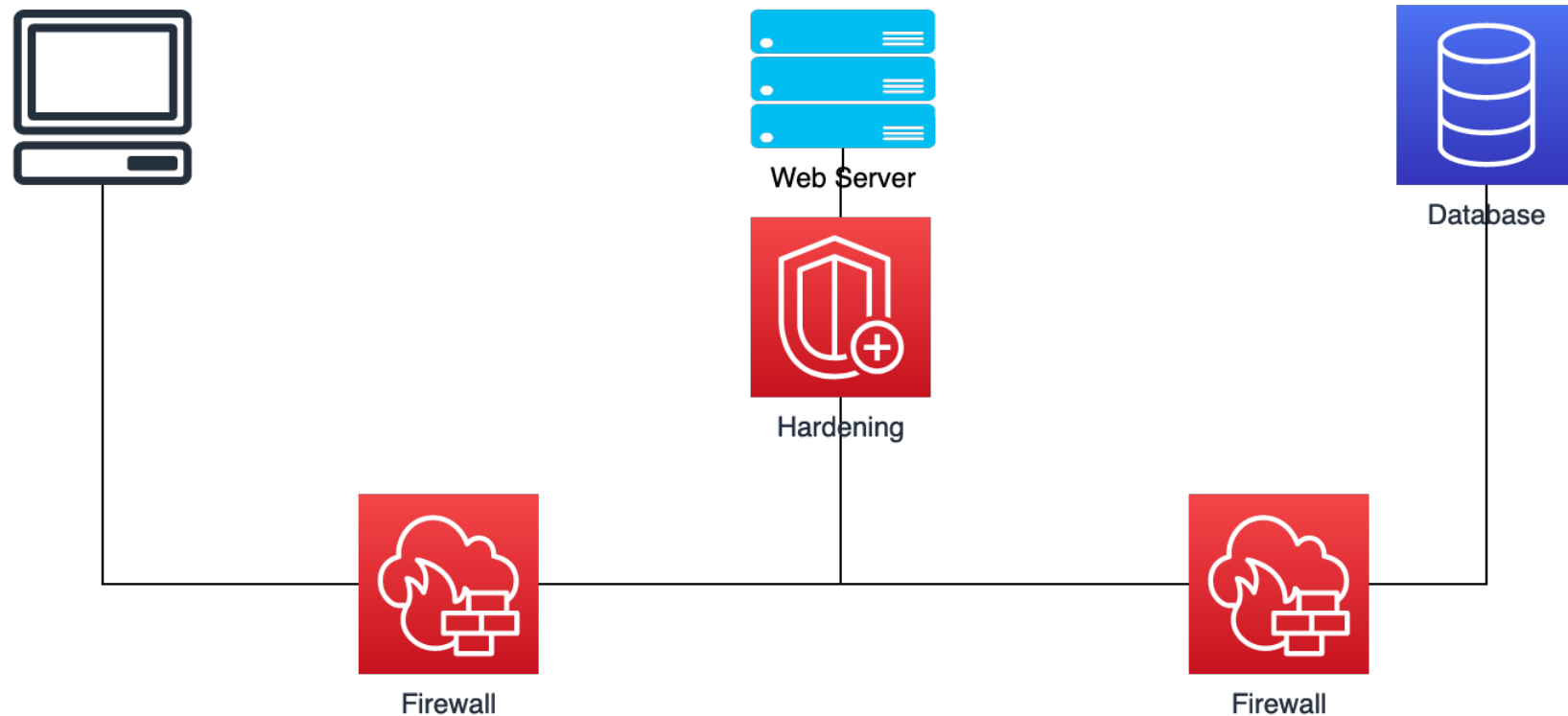
# Basics of Web Application Security

- How does basic web app look like?



# Basics of Web Application Security

- How does basic web app look like?



# SQL Injection

- OWASP definition: A [SQL injection](#) attack consists of insertion or “injection” of a SQL query via the input data from the client to the application.
- Exploiting mistakes in code access the database:
  - read
  - delete
  - modify
  - ...

# SQL Injection

- OWASP definition: A [SQL injection](#) attack consists of insertion or “injection” of a SQL query via the input data from the client to the application.
- Exploiting mistakes in code access the database:
  - read (SELECT)
  - delete
  - modify
  - ...

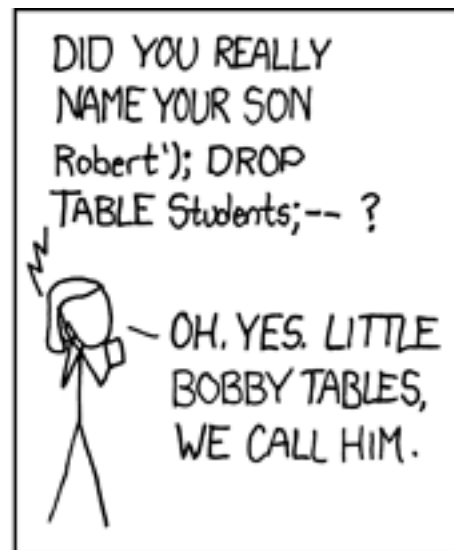
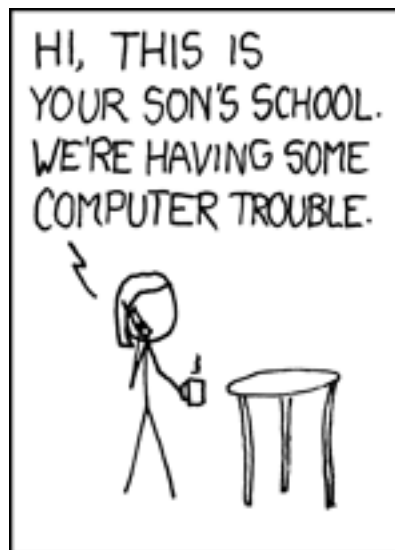
# SQL Injection

- OWASP definition: A [SQL injection](#) attack consists of insertion or “injection” of a SQL query via the input data from the client to the application.
- Exploiting mistakes in code access the database:
  - read (SELECT)
  - delete (DROP)
  - modify
  - ...



# SQL Injection

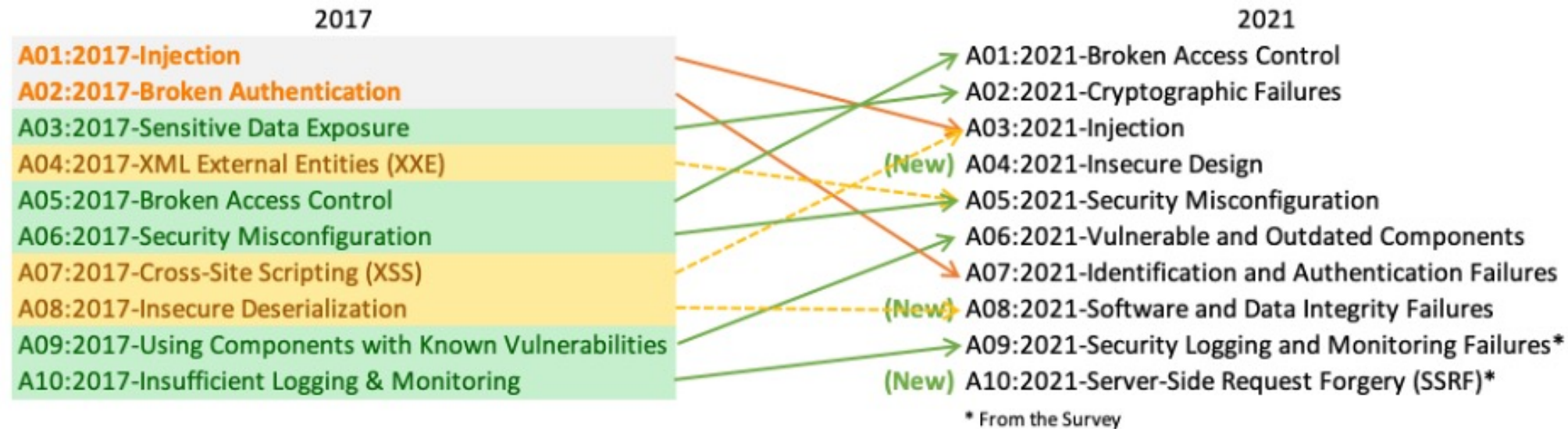
- OWASP definition: A [SQL injection](#) attack consists of insertion or “injection” of a SQL query via the input data from the client to the application.
- Exploiting mistakes in code access the database:
  - read (SELECT)
  - delete (DROP)
  - modify (UPDATE)
  - ...



# Motivation

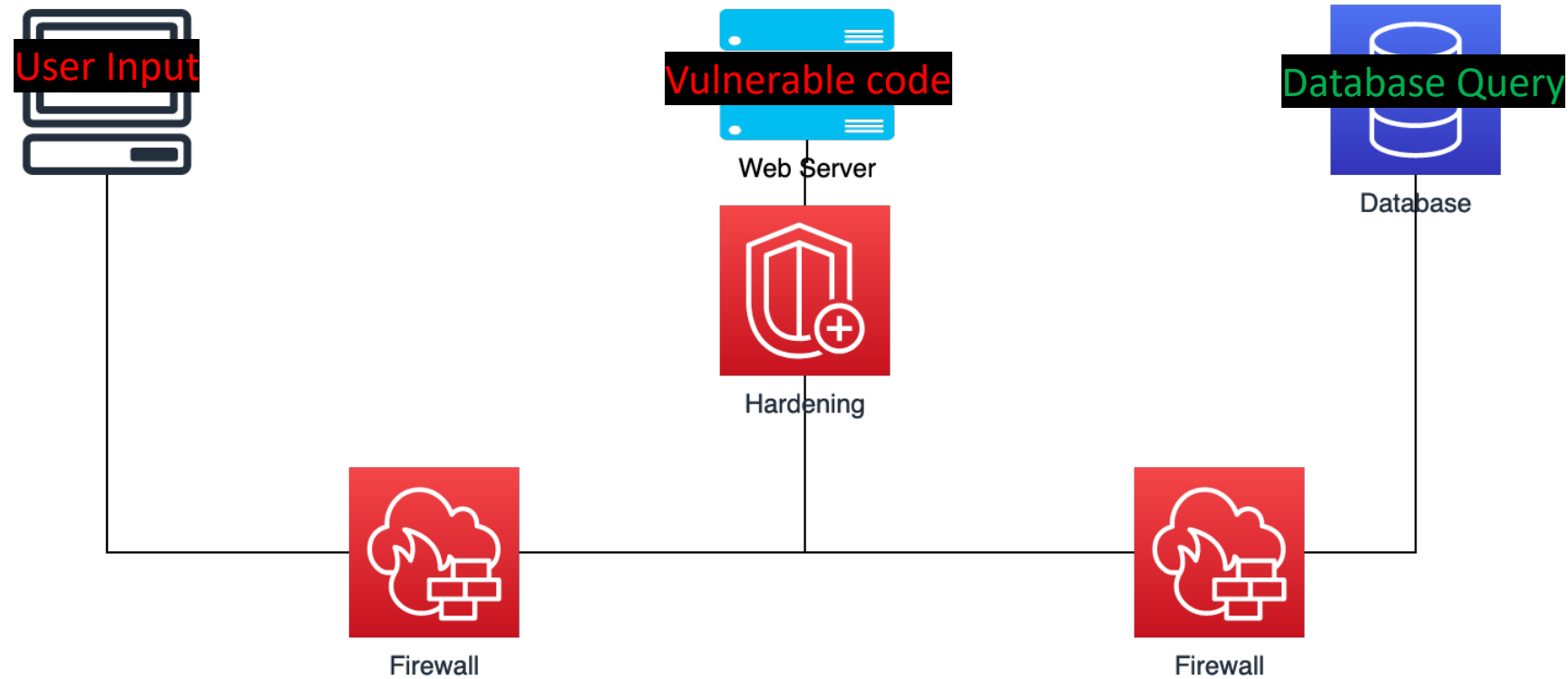
- First public discussion ~ 1998
- Still relevant [today!](#)
- Tesla (2014) – website vulnerable to SQL Injection exposed by researchers
- Cisco (2018) – license manager software injection enabled to gain shell, patched ofc.
- Fortnite (2019) - vulnerability that could lead to all users shown

# OWASP TOP 10



# Overview

- User input is taken and inserted into code
- User can affect what the app does



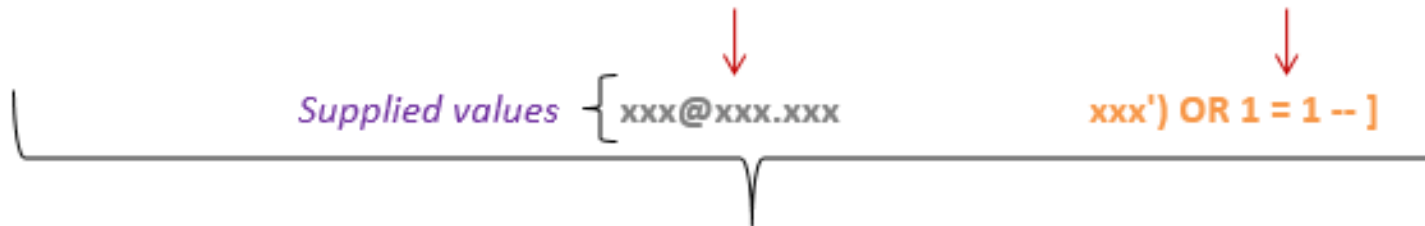
# Secure?

```
String query = "SELECT account_balance FROM user_data WHERE user_name = "  
               + request.getParameter("customerName");  
try {  
    Statement statement = connection.createStatement( ... );  
    ResultSet results = statement.executeQuery( query );  
}
```

# Basic Query Explained

```
SELECT * FROM users WHERE email = '$email' AND password = md5('$password');
```

*Supplied values* { `xxx@xxx.xxx`      `xxx') OR 1 = 1 -- ]` }



```
SELECT * FROM users WHERE email = 'xxx@xxx.xxx' AND password = md5('xxx') OR 1 = 1 -- ]');
```

```
SELECT * FROM users WHERE FALSE AND FALSE OR TRUE
```

```
SELECT * FROM users WHERE FALSE OR TRUE
```

```
SELECT * FROM users WHERE TRUE
```

# Examples

- <https://www.hacksplaining.com/lessons>
- <https://vm-thijs.ewi.utwente.nl/ctf/sql>



# Mitigation

- Sanitizing the input
- Prevent raw input from reaching the database
  - Prepared statements
  - Stored procedures
  - Allow-list
- Do not show errors from database to the user
  - Blind SQL Injection

# Prepared Statements

```
// This should REALLY be validated too
String custname = request.getParameter("customerName");
// Perform input validation to detect attacks
String query = "SELECT account_balance FROM user_data WHERE user_name = ? ";
PreparedStatement pstmt = connection.prepareStatement( query );
pstmt.setString( 1, custname);
ResultSet results = pstmt.executeQuery( );
```

# Stored Procedures

```
// This should REALLY be validated
String custname = request.getParameter("customerName");
try {
    CallableStatement cs = connection.prepareCall("{call sp_getAccountBalance(?)}");
    cs.setString(1, custname);
    ResultSet results = cs.executeQuery();
    // ... result set handling
} catch (SQLException se) {
    // ... logging and error handling
}
```

!!! Depends on how **sp\_getAccountBalance** is written, but generally safer !!!

# Allow-list

[illegible]

Now go and do the homework! Today!

[kbe.felk.cvut.cz](http://kbe.felk.cvut.cz)