

# CISC 327

# Software Quality Assurance

Review for Mini-Exam #4

# Likely topics/questions on mini-exam #3

- From Lecture 20
  - Black hat vs. gray hat vs. white hat
  - Data vs. information
  - Three aspects of data: CIA

# Likely topics/questions on mini-exam #3

- From Lecture 22:
  - Given a piece of code, identify SQL injection vulnerability
  - Explain **SQL injection payload**
  - Recommendation:
    - Blacklisting?
    - IPS/IDS?
    - Whitelisting?
    - Statement template?

# Escaping

- `// create connection`
- `Connection conn = DriverManager.getConnection(myUrl, "root", "");`
- `// create the query:`
- `String query = "SELECT * FROM users WHERE user_id ='" + user_id + "'";`
- `// create the java statement`
- `Statement st = conn.createStatement();`
- `// execute the query, and get a java resultset`
- `ResultSet rs = st.executeQuery(query);`

*Given a payload, explain the purpose.*

# Likely topics/questions on mini-exam #3

- From Lecture 23:
  - Given a web page and its backend logics, identify XSS
  - Describe steps to launch a reflected XSS
  - Difference between Phishing and XSS

# XSS - Example

- Error Page:
  - A single HTML page with JavaScript to display different error message on demand.
  - One doesn't want to create a dedicated page for all possible errors.

<http://youonlinebanking.com/error.html?msg=This+is+an+error+message>

