CISC 327 Software Quality Assurance

Lecture "review3"
Review for Mini-Exam #3

- From Lecture 17:
 - Mutation testing
 - Is mutation testing systematic?
 - What is the system (if there is one)?
 - How is mutation testing different from other white-box methods?

- From Lecture 18:
 - Maintenance and continuous testing methods
 - Corrective, perfective, adaptive maintenance

- From Lectures 18–19 (Maintenance, continuous testing, regression testing)
 - Corrective, perfective, adaptive maintenance
 - Regression testing
 - Know the 3 kinds of tests in a regression test suite
 - Know why some regression tests get "retired"

- From Lecture 20
 - Black hat vs. gray hat vs. white hat
 - Data vs. information
 - Three aspects of data: I C A
 - Adversarial vs. Non-adversarial threats

- From Lecture 21
 - CVE CVSS CWE (differences)
 - Buffer overflow:
 - Given a piece of code, and current break point -> draw out stack frame
 - Why it suffers from buffer overflow vulnerability
 - Prevention
 - DEP, ASLR, Canary

```
int read_user_name ()
   char user_name [100];
   int ok = 0;
   scanf("%s", user_name);
   return ok;
void greeting(){
   read_user_name()
```

- From Lecture 22:
 - Given a piece of code, identify SQL injection vulnerability
 - Explain how to launch an attack
 - Recommendation:
 - Blacklisting?
 - IPS/IDS?
 - Whitelisting?
 - Statement template?

Escaping

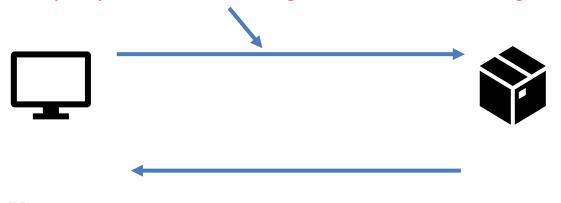
- // create connection
- Connection conn = DriverManager.getConnection(myUrl, "root", "");
- // create the query:
- String query = "SELECT * FROM users WHERE user_id ='" + user_id + "'";
- // create the java statement
- Statement st = conn.createStatement();
- // execute the query, and get a java resultset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

- 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://youronlinebanking.com/error.html?msg=This+is+an+error+message



You encounter an error

This is an error message

```
HTML template
  <!DOCTYPE html>
  <html>
  <body>
  <h2>You encounter an error</h2>
  message_placeholder
  </body>
  </html>
                   Replace
                   'message placeholder' with
                   the actual message
<!DOCTYPE html>
<html>
<body>
<h2>You encounter an error</h2>
This is an error message
</body>
</html>
```