LTAT.05.003
Software Engineering

Lecture 10:
Verification & Validation (Testing) II

Dietmar Pfahl
email: dietmar.pfahl@ut.ee

Fall 2019
Schedule of Lectures

Week 01: Introduction to SE
Week 02: Requirements Engineering I
Week 03: Requirements Engineering II
Week 04: Analysis
Week 05: Development Infrastructure
Week 06: Continuous Development and Integration
Week 07: Architecture and Design I
Week 08: Architecture and Design II

Week 09: Verification and Validation I
Week 10: Verification and Validation II
Week 11: Refactoring (and TDD)
Week 12: Agile/Lean Methods
Week 13: Agile Methods in Industry
Week 14: Course wrap-up, review and exam preparation
Week 15: Reserve time slot (no lecture scheduled as of today)
Structure of Lecture 10

• Testing Basics
• Testing Levels
• Testing Methods
• Testing Types
• Testing Artefacts
• Metrics
Recap from last week … (Terminology)

• **Failure** is an event caused by an **error**, **error** is a state of the program caused by a **fault** in the code

  • **Fault** – wrong/missing statement in code (resulting in error)
  • **Error** – incorrect program state (may result in a failure)
  • **Failure** – inability to perform its required functions (correctly)
  • **Defect (?)** – Bug ?

• **Debugging** / Fault localization – localizing, repairing, re-testing.
• **Test Case**, Test Script, Test Oracle, Test Verdict, …
• **Incident**, Issue
Recap from last week … (Terminology)

- **Failure** is an event caused by an error, error is a state of the program caused by a **fault** in the code

- **Fault** – wrong/missing statement in code (resulting in error)
- **Error** – incorrect program state (may result in a failure)
- **Failure** – inability to perform its required functions (correctly)
- **Defect (?)** – Bug ?

- **Debugging / Fault localization**
- **Test Case**, Test Script, Test Oracle, Test Verdict, ...
- **Incident, Issue**

“*I fixed the bug!*”

“*Here comes my bug report*”
Recap from last week … (Test Levels)

- Actual Needs and Constraints
- System Specifications
- Subsystem Design/Specs
- Unit/Component Specs
- System Test
- Integration Test
- Module Test
- Analysis / Review
- User Acceptance (alpha, beta test)
- Delivered Package

User review of external behavior as it is determined or becomes visible
Recap from last week … (Unit Test)

For CalculatorApp:

```java
@Test
void additionTest() {
    System.out.println("inside additionTest");
    assertAll(
        () -> assertEquals(2, calc.add(1, 1), "Doesn't add two positive numbers properly"),
        () -> assertEquals(0, calc.add(-1, 1), "Doesn't add a negative and a positive number properly"),
        () -> assertNotNull(calc, "The calc variable should be initialized")
    );
}

@Test
void divisionTest() {
    System.out.println("inside divisionTest");
    assertThrows(ArithmeticException.class, () -> calc.divide(2, 0));
}
```

Why not check this:
(-1) + (-1)
0 + 0
???

Why not check this:
2 / 1
1 / 2
-1 / 0
???
Black-Box versus White-Box Testing

External/user view:
- Check conformance with specification -> function coverage
- Abstraction from details:
  - Source code not needed
- Scales up:
  - Different techniques at different levels of granularity

Internal/developer view:
- Allows tester to be confident about code coverage
- Based on control and data flow:
  - Easier debugging
- Does not scale up:
  - Most useful at unit & integration testing levels, as well as regression testing

USE

BOTH!
Black-Box versus White-Box Testing

Gray-Box Testing

Combines black-box and white-box testing; typically, the focus is on input/output testing (black-box view) which is informed by structural information of the code (white-box view).

Example: The tester knows that certain constraints on the input are checked by the unit under test.

Application, e.g., in regression testing: apply (or update) black-box test cases only where code has been changed;

Most useful at unit & integration testing levels, as well as regression testing

Different techniques at different levels of granularity

USE

BOTH!
Black-Box vs. White-Box
Black-Box vs. White-Box

Specification-based Testing: Test against specification

Goal of BBT: Tries to check whether specified functionality is available and working correctly
Black-Box vs. White-Box

Specification-based Testing: Test against specification

System

Specification

Implementation

Goal of BBT: Tries to check whether specified functionality is available and working correctly

Unexpected functionality: Cannot be (directly) revealed by black-box techniques
Black-Box vs. White-Box

System

Specification

Implementation

Structural Testing: Test against implementation

Goal of WBT: Tries to check, whether the Implementation is working correctly (there is no dead code, it’s maintainable, etc.); useful for debugging;
Black-Box vs. White-Box

System

Specification

Implementation

Structural Testing: Test against implementation

Goal of WBT: Tries to check, whether the Implementation is working correctly (there is no dead code, it's maintainable, etc.); useful for debugging;

Missing functionality: Cannot be (directly) revealed by white-box techniques
Black-Box vs. White-Box

Specification-based Testing:
Test against specification

Structural Testing:
Test against implementation

System

Specification

Implementation

Missing functionality:
Cannot be (directly) revealed by white-box techniques

Unexpected functionality:
Cannot be (directly) revealed by black-box techniques
How do Black-Box and White-Box Testing relate to one another?

- Develop an initial Test suite using BB techniques
- Analyze the parts of the code uncovered by BB test suite
- Enhance the Test suite using WB techniques
- Apply BB coverage criteria to enhance it
- Apply WB coverage criteria to enhance it
Black Box Testing (BBT)

- BBT, also known as Behavioral Testing, is a software testing method in which the internal structure/design/implementation of the item being tested is not known to the tester.
  - These tests can be functional or non-functional

Aims to detect these types of issues:
- Incorrect or missing functions
- (User) Interface problems
- Problems in data structures or external database access
- Behavior or performance problems
- Initialization and termination problems
BBT Techniques

Following are some techniques that can be used for designing black box tests:

- **Equivalence Class Partitioning**
- **Boundary Value Analysis**
BBT Techniques

Following are some techniques that can be used for designing black box tests

• *Equivalence Class Partitioning*: It is a software test design technique that involves dividing input values into valid and invalid partitions and selecting representative values from each partition as test data. The partitions must cover the whole input value space and the partitions must be disjoint.

• *Boundary Value Analysis*: It is a software test design technique that involves determination of boundaries for input values and selecting values that are at the boundaries and just inside/outside of the boundaries as test data.
### Example

Assume a 'magic' Function M

**Spec:**
The program accepts integers x & y
The program calculates sum = x + y
The program displays the result 'sum'

M (x, y) → sum = x + y
with x, y: int (32 bit)

Exhaustive (positive) testing: ?
Example

Assume a ’magic’ Function M

Spec:
The program accepts integers x & y
The program calculates sum = x + y
The program displays the result ‘sum’

M (x, y) → sum = x + y
with x, y: int (32 bit)

Exhaustive (positive) testing:
$2^{32} \times 2^{32}$
= $2^{64} \sim 1.8\times10^{19}$ test cases (input data + expected output)
Equivalence Class Partitioning (ECP)

Input: x & y | Output: sum

Classes

C1: InputX: ?
C2: InputY: ?
C3: OutputSum: ?
Equivalence Class Partitioning (ECP)

Input: x & y | Output: sum

Classes

C1: InputX: [MinInt, MaxInt]
C2: InputY: [MinInt, MaxInt]
C3: OutputSum: [MinInt, MaxInt]
Equivalence Class Partitioning (ECP)

Input: x & y | Output: sum

Classes

C1: InputX: [MinInt, MaxInt]
C2: InputY: [MinInt, MaxInt]
C3: OutputSum: [MinInt, MaxInt]

Is that all?
Equivalence Class Partitioning (ECP)

Input: x & y | Output: sum

Classes

C1: InputX: [MinInt, MaxInt]
C2: InputY: [MinInt, MaxInt]
C3: OutputSum: [MinInt, MaxInt]

C4: InputX: notInt
C5: InputY: notInt
C6: OutputSum: exception
Equivalence Class Partitioning (ECP)

Input: x & y | Output: sum

Classes

C1: InputX: [MinInt, MaxInt]
C2: InputY: [MinInt, MaxInt]
C3: OutputSum: [MinInt, MaxInt]
C4: InputX: notInt
C5: InputY: notInt
C6: OutputSum: exception

Test Cases

Data: x, y, sum

TC1: 0, 0 -> 0
TC2: notInt, 0 -> WrongInputException
TC3: 0, notInt -> WrongInputException

It's good practice to check for the effect of each invalid input class independently.

minimal, TCs cover all classes
Equivalence Class Partitioning (ECP)

Input: x & y | Output: sum

Test Cases

Data: x, y, sum

TC1: 0, 0 -> 0
TC2: notInt, 0 -> WrongInputException
TC3: 0, notInt -> WrongInputException

Classes covered:

C1, C2, C3
C4, C2, C6
C1, C5, C6

minimal,
TCs cover all classes
Boundary Value Analysis (BVA)

Input: x & y | Output: sum

Classes

C1: InputX: [MinInt, MaxInt]
C2: InputY: [MinInt, MaxInt]
C3: OutputSum: [MinInt, MaxInt]
C4: InputX: notInt
C5: InputY: notInt
C6: OutputSum: exception

Test Cases

Data: x, y, sum

TC1: 0, 0 -> 0
TC2: notInt, 0 -> WrongInputException
TC3: 0, notInt -> WrongInputException
TC4: MinInt, MinInt -> ArithmeticException
TC5: MaxInt, MaxInt -> ArithmeticException
TC6: MaxInt/2, MaxInt/2 -> MaxInt
TC7: MinInt/2, MinInt/2 -> MinInt
Other BBT Methods

- Cause Effect Graphing (CEG)
- Combinatorial Testing
- Fuzzing
- Exploratory Testing
- Model-driven Testing
- ...

Spring 2020: “Software Testing” course
BBT – Advantages & Disadvantages

Advantages
• Tests are done from a user’s point of view and will help in exposing discrepancies in the specifications.
• Tester need not know programming languages or how the software has been implemented.
• Tests can be conducted by a body independent from the developers, allowing for an objective perspective and the avoidance of developer-bias.
• Test cases can be designed as soon as the specifications are complete.

Disadvantages
• Only a small number of possible inputs can be tested and many program paths will be left untested.
• Without clear specifications, which is the situation in many projects, test cases will be difficult to design.
• Tests can be redundant if the software designer/developer has already run a test case.
• Ever wondered why a soothsayer closes the eyes when foretelling events? So is almost the case in Black Box Testing.
White Box Testing (WBT)

• WBT, also known as Clear Box Testing, Open Box Testing, Glass Box Testing, Transparent Box Testing, Code-Based Testing or Structural Testing) is a testing method the internal structure/design/implementation of the item being tested is known to the tester.

• The tester chooses inputs to exercise paths through the code and determines the appropriate outputs. Programming know-how and the implementation knowledge is essential.

Aims to detect these types of issues:
- Control flow issues
- Data flow issues
- Algorithms
Example

Assume a ’magic’ Function M

M (x, y) \rightarrow \text{sum} = x + y
with x, y: \text{int (32 bit)}

Possible approaches:
- Execute each statement
- Execute paths based on:
  - Control-flow (decisions, conditions, loops, independent paths, etc.)
  - Data-flow (definition and usage of variables)
- Read (review) code

White Box

... 

if ( x - 100 <= 0 ) {
    if ( y - 100 <= 0 ) {
        if ( x + y - 200 == 0 ) {
            \text{crash(); }}
    }
}

\text{print}(x + y);

How many statements covered with BBT suite?
Example

Assume a ‘magic’ Function M

\[ M(x, y) \rightarrow \text{sum} = x + y \]

with \( x, y: \text{int (32 bit)} \)

TC1: 0, 0 -> 0

White Box

... 
if ( \( x - 100 \leq 0 \) ) {
  if ( \( y - 100 \leq 0 \) ) {
    if ( \( x + y - 200 \equiv 0 \) ) {
      \text{crash();} \}
  }
}
print(\( x + y \));

How many statements covered with BBT suite?
Example

Assume a ’magic’ Function $M$

$M(x, y) \rightarrow \text{sum} = x + y$
with $x, y$: int (32 bit)

TC1: 0, 0 -> 0

White Box

... 
if ( $x - 100 \leq 0$ ) {
    if ( $y - 100 \leq 0$ ) {
        if ( $x + y - 200 \equiv 0$ ) {
            crash();
        }
    }
}
print($x + y$);

How many statements covered with BBT suite?

$\rightarrow 80\%$
Example

Assume a 'magic' Function M

\[ M(x, y) \rightarrow \text{sum} = x + y \]
with \( x, y: \text{int (32 bit)} \)

TC1: 0, 0 -> 0
TC2: notInt, 0 -> WrongInputException
TC3: 0, notInt -> WrongInputException
TC4: MinInt, MinInt -> ArithmeticException
TC5: MaxInt, MaxInt -> ArithmeticException
TC6: MaxInt/2, MaxInt/2 -> MaxInt
TC7: MinInt/2, MinInt/2 -> MinInt

White Box

... 
if ( x - 100 <= 0 ) {
    if ( y - 100 <= 0 ) {
        if ( x + y - 200 == 0 ) {
            crash(); }}}
print(x + y);

How many statements covered with BBT suite?

\[ \rightarrow 80\% \]
Control-Flow Testing: Statement Coverage

- If we try to cover all statements, we must find input data such that all three if-statements are ‘true’:

Traverse code and combine conditions:
(x<=100) and (y<=100) and (x+y=200) ->
(200-y<=100) and (y<=100) ->
(y>=100) and (y<=100) ->
y = 100 ->
x = 100 ->

White Box

\[
\begin{align*}
\text{\ldots} \\
\text{if ( x - 100 } \leq 0 \) } \{ \\
\quad \text{if ( y - 100 } \leq 0 \) } \{ \\
\qquad \text{if ( x + y - 200 } = 0 \) } \{ \\
\qquad\qquad \text{crash(); } \}}
\}
\]
print(x + y);
Control-Flow Testing: Statement Coverage

Assume a magic Function $M$

$M(x, y) \rightarrow \text{sum} = x + y$
with $x, y$: int (32 bit)

TC1: $M(0, 0) \rightarrow 0$
TC2: $M(100, 100) \rightarrow \text{crash()}$

1st if = true: $x \leq 100$
2nd if = true: $y \leq 100$
3rd if = true: $x + y = 200$

$\rightarrow$ 100% Statement Coverage

White Box

\[
\begin{align*}
... \\
\text{if ( } x - 100 \leq 0 \text{ ) } \{ \\
\quad \text{if ( } y - 100 \leq 0 \text{ ) } \{ \\
\quad\quad \text{if ( } x + y - 200 == 0 \text{ ) } \{ \\
\quad\quad\quad \text{crash(); } \} \} \}
\end{align*}
\]

print($x + y$);
Control-Flow Testing: Branch Coverage

• If we try to cover all branches, we must find input data such that all three if-statements are once evaluated to 'true' and once to 'false':

TC1: M(0, 0) -> 0
TC2: M(100, 100) -> crash()

How much branch coverage?
Control-Flow Testing: Branch Coverage

Assume a 'magic' Function M

TC1: M(0, 0) -> 0
TC2: M(100, 100) -> crash()

-> 66% Branch (or Decision) Coverage

TC1: if1 = true / if2 = true / if3 = false
TC2: if1 = true / if2 = true / if3 = true

Missing: if1=false and if2=false -> 2 additional TCs needed
Other WBT Methods

- Data Flow Testing
- Mutation Testing
- Symbolic Execution
- ...

Spring 2020: “Software Testing” course
WBT – Advantages & Disadvantages

Advantages
• Testing can be commenced at an earlier stage. One need not wait for the GUI to be available.
• Testing is more thorough, with the possibility of covering most paths.

Disadvantages
• Since tests can be very complex, highly skilled resources are required, with thorough knowledge of programming and implementation.
• Test script maintenance can be a burden if the implementation changes too frequently.
Other Testing Methods
Other Testing Methods

Gray Box Testing
• Combines BBT and WBT

Ad-hoc Testing (also known as Monkey Testing)
• A testing method without planning (and usually without documentation)
• The tests are conducted informally and randomly without any specified expected results
• Success relies highly on skills and creativity of the testers
• If automated → Random Testing (e.g., randoop)

Agile Testing
• Context: Test-Driven Development (TDD) and Behavior Driven Development (BDD)
• Exploratory Testing
TDD and BDD

- Developer TDD => Unit Tests

Acceptance TDD => Acceptance Tests
also called:
Behavior-driven testing (BDD)
TDD

1. Write a test
2. See it fail
3. Make it run

Add a developer test
- [Pass]
- [Fail]
  - Run the developer tests
  - Make a little change
  - [Pass, Functionality incomplete]
  - [Pass, Functionality complete]

JUnit
Test class name:
org.jboss.dmr2.crimeportal.CrimePortalTest

Runs: 3/3 Errors: 0 Failures: 0

Run

- X Failures
- Test Hierarchy

Finished: 4,008 seconds
TDD

1. Write a test
2. See it fail
3. Make it run
4. Make it right (refactor)
BDD

Acceptance TDD =>
Acceptance Tests
also called:
Behavior-driven testing (BDD)
TDD and BDD

- Developer TDD => Unit Tests

Acceptance TDD => Acceptance Tests
also called: Behavior-driven testing (BDD)
Exploratory Testing

- Not the same as ‘random testing’ or ‘monkey testing’
- Always worth doing (on top of “regular” / automated testing)
- Can trigger failures that systematic techniques miss
- Consider
  - ”What is the craziest thing we can do?”
  - Intuition / Experience / Brainstorming
  - Past failures / Lists in literature
- Tools
  - http://www.softwaretestinghelp.com/tools/top-17-exploratory-testing-tools/
Structure of Lecture 10

- Testing Basics
- Testing Levels
- Testing Methods
- Testing Types
- Testing Artefacts
- Metrics
Overview of Testing Types

- Smoke Testing
- Functional Testing
- Usability Testing
- Security Testing
- Performance Testing
- Regression Testing
- Compliance Testing
Smoke Testing

- Smoke Testing, also known as “Build Verification Testing”, is a type of software testing that covers most of the major functions of the software but none of them in depth.
- The results of this testing is used to decide if a build is stable enough to proceed with further testing.
  - If the smoke test passes, go ahead with further testing.
  - If it fails, halt further tests and ask for a new build with the required fixes.
  - If an application is badly broken, detailed testing might be a waste of time and effort.
Functional Testing

• Functional Testing is a type of software testing whereby the system is tested against the functional requirements/specifications.
• This type of testing is not concerned with how processing occurs, but rather, with the results of processing.

• Functional testing is normally performed during the levels of System and Acceptance Testing
• During functional testing, BBT techniques are used

• Typically, functional testing involves the following steps:
  1. Identify functions that the software is expected to perform
  2. Create input data based on the function’s specifications
  3. Determine the output based on the function’s specifications
  4. Execute the test case
  5. Compare the actual and expected outputs
Usability Testing

• Usability Testing is a type of testing done from an end-user’s perspective to determine if the system is easily usable.

• Usability Testing is normally performed during System and Acceptance Testing levels.

• Tips:
  • Understand who the users of the system are.
  • Understand what their business needs are.
  • Try to mimic their behavior.
Usability Test Types + Environment

Rubin’s Types of Usability Tests (Rubin, 1994, p. 31-46)

Exploratory test – early product development

Assessment test – most typical, either early or midway in the product development

Validation test – confirmation of product’s usability

Comparison test – compare two or more designs; can be used with other three types of tests
Usability Testing – Comparison A versus B
Usability Testing – Example of a Test Task

Let’s say a user needs to print a Financial Update Report, every 30 minutes, and he/she has to go through the following steps:
1. Login to the system
2. Click Reports
3. From the groups of reports, select Financial Reports
4. From the list of financial reports, select Financial Update Report
5. Specify the following parameters
   • Date Range, Time Zone, Departments, Units
6. Click Generate Report
7. Click Print
8. Select an option
   • Print as PDF
   • Print for Real

Good or Bad Usability?
Testing Usability Requirements

<table>
<thead>
<tr>
<th>Problem counts</th>
</tr>
</thead>
<tbody>
<tr>
<td>R1: At most 1 of 5 novices shall encounter critical problems during tasks Q and R. At most 5 medium problems on list.</td>
</tr>
<tr>
<td>Task time</td>
</tr>
<tr>
<td>R2: Novice users shall perform tasks Q and R in 15 minutes. Experienced users tasks Q, R, S in 2 minutes.</td>
</tr>
<tr>
<td>Keystroke counts</td>
</tr>
<tr>
<td>R3: Recording breakfast shall be possible with 5 keystrokes per guest. No mouse.</td>
</tr>
<tr>
<td>Opinion poll</td>
</tr>
<tr>
<td>R4: 80% of users shall find system easy to learn. 60% shall recommend system to others.</td>
</tr>
<tr>
<td>Score for understanding</td>
</tr>
<tr>
<td>R5: Show 5 users 10 common error messages, e.g. Amount too large. Ask for the cause. 80% of the answers shall be correct.</td>
</tr>
</tbody>
</table>

How to test:
- Define several (typical) usage scenarios involving tasks Q and R
- Select test users and classify as 'novice' and 'experienced'
- Let 5 (or better 10, 15) novices perform the scenarios
- Observe what problems they encounter
- Classify and count observed problems
Usability Testing – What? How?

• **Test Focus**
  • **Understandability**
    • Easy to understand?
  • **Ease of learning**
    • Easy to learn?
  • **Operability**
    • Matches purpose & environment of operation?
    • Ergonomics: color, font, sound,...
  • **Communicativeness**
    • In accordance with psychological characteristics of user?

• **Test Environments**
  • Free form tasks
  • Procedure scripts
  • Paper screens
  • Mock-ups
  • Field trial
Heuristic Evaluation by Inspection

List of 10 Heuristics according to (Nielsen, 2005):

<table>
<thead>
<tr>
<th></th>
<th>Visibility of system status</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Match between the system and the real world</td>
</tr>
<tr>
<td>3</td>
<td>User control and freedom</td>
</tr>
<tr>
<td>4</td>
<td>Consistency and standards</td>
</tr>
<tr>
<td>5</td>
<td>Error prevention</td>
</tr>
<tr>
<td>6</td>
<td>Recognition rather than recall</td>
</tr>
<tr>
<td>7</td>
<td>Flexibility and efficiency of use</td>
</tr>
<tr>
<td>8</td>
<td>Aesthetic and minimalist design</td>
</tr>
<tr>
<td>9</td>
<td>Help users recognize, diagnose, and recover from errors</td>
</tr>
<tr>
<td>10</td>
<td>Help and documentation</td>
</tr>
</tbody>
</table>

List violations of heuristics:

Rank by severity: 0...4
0: positive (or neutral) aspect of system
...
4: major, catastrophic aspect of system


Security Testing

- Security Testing is a type of software testing that intends to uncover vulnerabilities of the system and determine that its data and resources are protected from possible intruders.

- 4 Focus Areas:
  - **Network security:** This involves looking for vulnerabilities in the network infrastructure (resources and policies).
  - **System software security:** This involves assessing weaknesses in the various software (operating system, database system, and other software) the application depends on.
  - **Client-side application security:** This deals with ensuring that the client (browser or any such tool) cannot be manipulated.
  - **Server-side application security:** This involves making sure that the server code and its technologies are robust enough to fend off any intrusion.
Security Testing

Example of a basic security test:
• Log into the web application.
• Log out of the web application.
• Click the BACK button of the browser (Check if you are asked to log in again or if you are provided the logged-in application.)

• Most types of security testing involve complex steps and out-of-the-box thinking but, sometimes, it is simple tests like the one above that help expose the most severe security risks.
The Open Web Application Security Project (OWASP) is a great resource for software security professionals. Be sure to check out the Testing Guide: https://www.owasp.org/index.php/Category:OWASP_Testing_Project

OWASP Top 10 security threats for 2013 were:
• Injection
• Broken Authentication and Session Management
• Cross-Site Scripting (XSS)
• Insecure Direct Object References
• Security Misconfiguration
• Sensitive Data Exposure
• Missing Function Level Access Control
• Cross-Site Request Forgery (CSRF)
• Using Known Vulnerable Components
• Unvalidated Redirects and Forwards
How to avoid SQL injection vulnerability?

Instead of:

```java
String query = "SELECT * FROM Users WHERE Username= "+ request.getParameter("username")
+ "AND Password= "
+ request.getParameter("password");

try {
    Statement statement = connection.createStatement();
    ResultSet results = statement.executeQuery(query);
}
```

Which might result in a SQL query string like this:

```sql
SELECT * FROM Users WHERE Username='1' OR '1' = '1' AND
Password='1' OR '1' = '1'
```
How to avoid SQL injection vulnerability?

Use java ‘prepared statement’:

```java
String username = request.getParameter("username");
String password = request.getParameter("password");
// perform input validation to detect attacks

String query = "SELECT * FROM Users WHERE Username= ? AND Password= ?";

PreparedStatement pstmt = connection.prepareStatement(query);
pstmt.setString(1, username);
pstmt.setString(2, password);

ResultSet results = pstmt.executeQuery();
```

Example with Hibernate Query Language (HQL) can be found here:
https://www.owasp.org/index.php/SQL_Injection_Prevention_Cheat_Sheet
Performance Testing

• Performance Testing is a type of software testing that intends to determine how a system performs in terms of responsiveness and stability under a certain load.

Types:
• Load Testing is a type of performance testing conducted to evaluate the behavior of a system at increasing workload.
• Stress Testing is a type of performance testing conducted to evaluate the behavior of a system at or beyond the limits of its anticipated workload.
• Endurance Testing is a type of performance testing conducted to evaluate the behavior of a system when a significant workload is given continuously.
• Spike Testing is a type of performance testing conducted to evaluate the behavior of a system when the load is suddenly and substantially increased.
Regression Testing

- Regression testing is a type of software testing that intends to ensure that changes (enhancements or defect fixes) to the software have not adversely affected it.

How much?
- In an ideal case, a full regression test is desirable but oftentimes there are time/resource constraints. In such cases, it is essential to do an impact analysis of the changes to identify areas of the software that have the highest probability of being affected by the change and that have the highest impact to users in case of malfunction and focus testing around those areas.
Regression Testing – Retest All

• Assumption:
  • Changes may introduce faults anywhere in the code

• BUT: expensive, prohibitive for large systems

• Reuse existing test suite
  • Add new tests as needed
  • Remove obsolete tests

[Skoglund, Runeson, ISESE05]
Regression Testing – Selective Testing

- Conduct impact analysis
  - Only code impacted by change needs to be retested
  - Select tests that exercise such code

- Add new tests if needed
- Remove obsolete tests
Compliance Testing

- Compliance Testing, also known as conformance testing, regulation testing, standards testing, is a type of testing to determine the compliance of a system with internal or external standards.

Checklist:

<table>
<thead>
<tr>
<th>Lorem ipsum dolor sit amet</th>
<th>✓</th>
</tr>
</thead>
<tbody>
<tr>
<td>consectetur adipiscing elit</td>
<td>✓</td>
</tr>
<tr>
<td>sed do eiusmod tempor incididunt ut labore et dolore magna aliqua</td>
<td>✓</td>
</tr>
<tr>
<td>Ut enim ad minim veniam</td>
<td>✗</td>
</tr>
<tr>
<td>quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat</td>
<td>✓</td>
</tr>
</tbody>
</table>
Structure of Lecture 10

• Testing Basics
• Testing Levels
• Testing Methods
• Testing Types
• Testing Artefacts
• Metrics
Test Documentation

IEEE 829-2008: Standard for Software and System Test Documentation

FIG. 7.4
Test Plan

A Software Test Plan is a document describing the testing scope and activities. It is the basis for formally testing any software/product in a project.

One can have the following types of test plans:

- **Master Test Plan**: A single high-level test plan for a project/product that unifies all other test plans.
- **Testing Level Specific Test Plans**:
  - Unit Test Plan
  - Integration Test Plan
  - System Test Plan
  - Acceptance Test Plan
- **Testing Type Specific Test Plans**: Plans for major types of testing like Performance Test Plan and Security Test Plan
# Test Case – Template

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Test Suite ID</td>
<td>The ID of the test suite to which this test case belongs.</td>
</tr>
<tr>
<td>Test Case ID</td>
<td>The ID of the test case.</td>
</tr>
<tr>
<td>Test Case Summary</td>
<td>The summary / objective of the test case.</td>
</tr>
<tr>
<td>Related Requirement</td>
<td>The ID of the requirement this test case relates/traces to.</td>
</tr>
<tr>
<td>Prerequisites</td>
<td>Any prerequisites or preconditions that must be fulfilled prior to executing the test.</td>
</tr>
<tr>
<td>Test Procedure</td>
<td>Step-by-step procedure to execute the test.</td>
</tr>
<tr>
<td>Test Data</td>
<td>The test data, or links to the test data, that are to be used while conducting the test.</td>
</tr>
<tr>
<td>Expected Result</td>
<td>The expected result of the test.</td>
</tr>
<tr>
<td>Actual Result</td>
<td>The actual result of the test; to be filled after executing the test.</td>
</tr>
<tr>
<td>Status</td>
<td>Pass or Fail. Other statuses can be ‘Not Executed’ if testing is not performed and ‘Blocked’ if testing is blocked.</td>
</tr>
<tr>
<td>Remarks</td>
<td>Any comments on the test case or test execution.</td>
</tr>
<tr>
<td>Created By</td>
<td>The name of the author of the test case.</td>
</tr>
<tr>
<td>Date of Creation</td>
<td>The date of creation of the test case.</td>
</tr>
<tr>
<td>Executed By</td>
<td>The name of the person who executed the test.</td>
</tr>
<tr>
<td>Date of Execution</td>
<td>The date of execution of the test.</td>
</tr>
<tr>
<td>Test Environment</td>
<td>The environment (Hardware/Software/Network) in which the test was executed.</td>
</tr>
</tbody>
</table>
Test Case – Example

Test Suite ID: TS001
Test Case ID: TC001
Test Case Summary: To verify that clicking the Generate Coin button generates coins.
Related Requirement: RS001
Prerequisites: User is authorized; Coin balance is available.
Test Procedure:
1. Select the coin denomination in the Denomination field.
2. Enter the number of coins in the Quantity field.
3. Click Generate Coin.
Test Data:
Denominations: 0.05, 0.10, 0.25, 0.50, 1, 2, 5
Quantities: 0, 1, 5, 10, 20
Expected Result:
Coin of the specified denomination should be produced if the specified Quantity is valid (1, 5)
A message ‘Please enter a valid quantity between 1 and 10’ should be displayed if the specified quantity is invalid.
Actual Result:
If the specified quantity is valid, the result is as expected.
If the specified quantity is invalid, nothing happens; the expected message is not displayed
Status: Fail
Remarks: This is a sample test case.
Created By: John Doe
Date of Creation: 01/14/2020
Executed By: Jane Roe
Date of Execution: 02/16/2020
Test Environment: OS: Windows Y, Browser: Chrome N
Incident/Issue Report

- In most companies, an issue reporting tool is used and the elements of a report can vary. However, in general, an issue report can consist of the following elements.
Structure of Lecture 10

- Testing Basics
- Testing Levels
- Testing Methods
- Testing Types
- Testing Artefacts
- Metrics
Code Coverage

- The relative amount of covered items with regards to a coverage criterion, e.g., statement, branch, condition, ...

\[
\begin{align*}
\text{statement\_coverage} &= \frac{\text{executed\_statements}}{\text{total\_number\_statements}} \\
\text{branch\_coverage} &= \frac{\text{executed\_branches}}{\text{total\_number\_branches}}
\end{align*}
\]

Usage
- To control the comprehensiveness of a test suite
- Often used as test stopping criterion
Defect Density

- Defect Density is the number of confirmed defects detected in software/component during a defined period of development/operation divided by the size of the software/component.

\[
\text{defect\_density} = \frac{\text{number\_confirmed\_defects}}{\text{size}}
\]

Usage:
- For comparing the relative number of defects in various software components (or software products) so that high-risk components can be identified and resources focused towards them.
Defect Coverage

- Defect Coverage is the number of confirmed defects detected in software/component during a defined period of development/operation divided by the total number of defects.

\[
defect\_coverage = \frac{number\_confirmed\_defects}{total\_number\_defects}
\]

Usage:
- To assess the effectiveness of a test suite.
- Might be applied for certain types of defects (e.g., severity=major; priority=high)
Next Lecture

• Date/Time:
  • Friday, 15-Nov, 10:15-12:00
• Topic:
  • Refactoring (and TDD)
• Labs:
  • Continue working on Homework 5
  • Go to Assessment Labs next week!