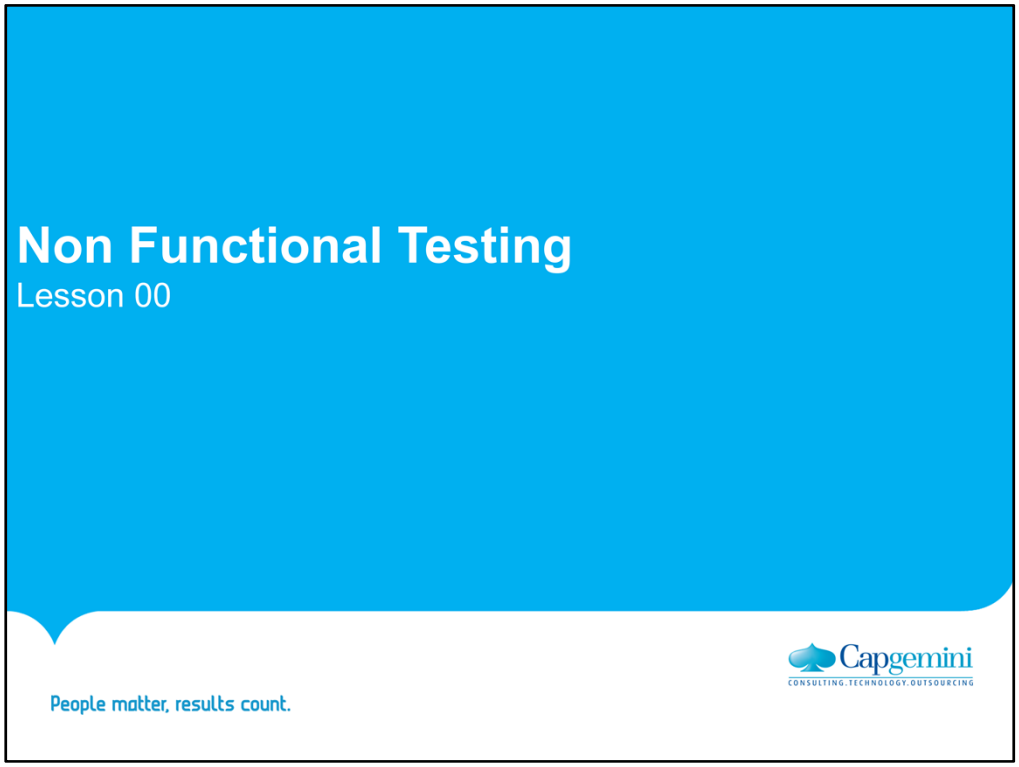


Document History

Date	Course Version No.	Software Version No.	Developer / SME	Reviewer(s)	Approver	Change Record Remarks
2013	2.0	NA	Priti Jindal	Priti Jindal		Courseware enhancements

Course Goals and Non Goals

- Course Goals
  - At the end of this program, participants will gain an understanding of what is Performance Testing
  - What are the objectives of Performance Testing?
  - What are the different types of Performance Testing?
  - Performance Testing Methodology
  - Introduction to tools used in Performance Testing
  - What is Web Security Testing?
  - OWASP Top Ten Vulnerabilities
  - ETL Testing
  - OLAP Testing
  - End to End Testing
  - DWH/BI Performance Testing
- Course Non Goals
  - This course does not cover how to perform above listed types of testing using tools

Capgemini
CONSULTING. TECHNOLOGY. OUTSOURCING

 3

Pre-requisites

- Good knowledge of Software Testing
- Good knowledge of Requirements Engineering
- Fair knowledge of Web Applications
- Familiarity with Database Concepts

Intended Audience

- Test engineers
- Test Leads

Capgemini
CONSULTING. TECHNOLOGY. OUTSOURCING

 5

Day Wise Schedule

- Day 1
  - Lesson 1: Introduction to Performance Testing
  - Lesson 2: Introduction to Web Security
- Day 2
  - Lesson 2: Introduction to Web Security (Cont.)
  - Lesson 3: Introduction to Data Warehouse, ETL & Data Warehouse Testing

Table of Contents

Table of Contents

Capgemini
CONSULTING. TECHNOLOGY. OUTSOURCING

 8

Table of Contents

Capgemini
CONSULTING. TECHNOLOGY. OUTSOURCING

 9

References

- Book Reference
- Web Reference

Capgemini
CONSULTING. TECHNOLOGY. OUTSOURCING

 10

Non Functional Testing

Lesson 1: Introduction to Performance Testing

Lesson Objectives

- To understand the following topics:
  - Performance Testing – An Overview
  - Objectives of Performance Testing
  - Types of Performance Testing
  - When To Do Performance Testing
  - Why Performance Testing
  - Performance Test Terminology
  - Performance Testing Methodology
  - Performance Testing Process/Phases
  - Introduction to Performance Testing Tools
  - Summary

Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

 2

Performance Testing

Performance Testing – An Overview

- Performance testing is a generic term that can refer to many different types of performance-related testing, each of which addresses a specific problem area and provides its own benefits, risks, and challenges
- Testing conducted to evaluate the compliance of a system or component with specified performance requirements
  - "Goal of Performance testing is not to find bugs, but to eliminate the bottlenecks"
- A bottleneck is a stage in a process that causes the entire process to slow down or stop

Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

 4

Performance Testing – An Overview (Cont.)

- Determines the speed, scalability and stability characteristics of an application, thereby providing an input to making sound business decisions
- Focuses on determining if the user of the system will be satisfied with the performance characteristics of the application
- Supports tuning, capacity planning, and optimization efforts

Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

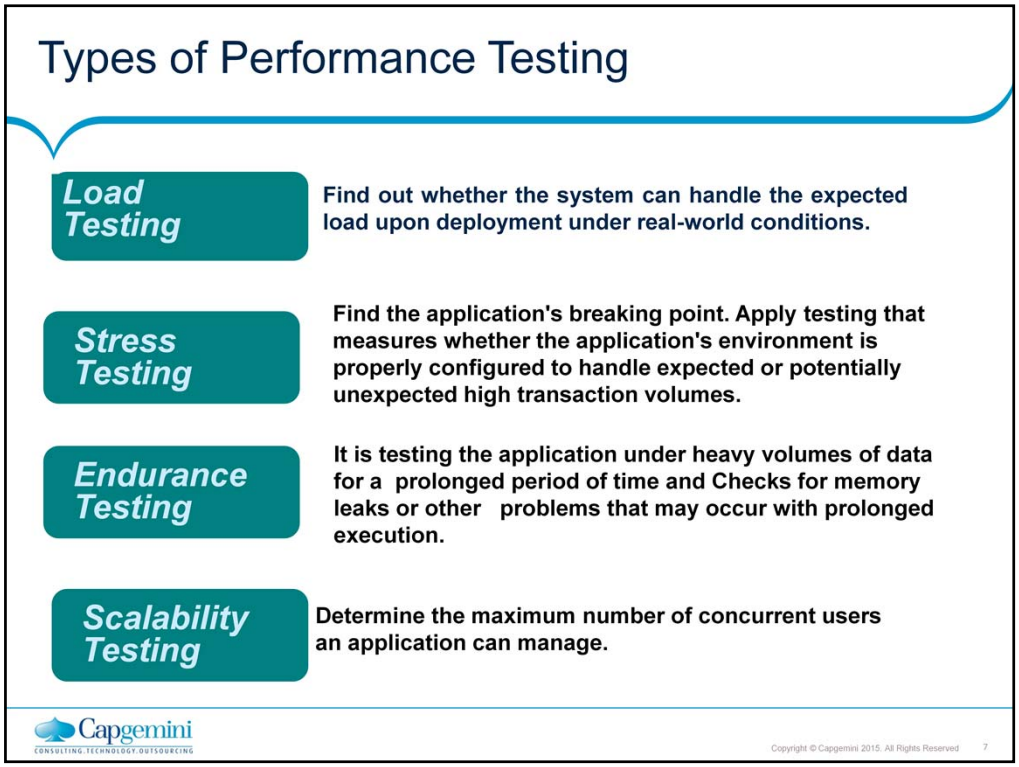
 5

Objectives of Performance Testing

- Application Response Time - How long does it take to complete a task?
- Reliability - How Stable is the system under a heavy work load?
- Configuration Sizing - Which configuration provides the best performance level?
- Capacity Planning - What H/W does the application supports?
- Acceptance - Is the system stable enough to go into Production?
- Bottleneck Identification - What is the cause of degradation in performance?
- Regression - Does the new version of Software adversely affect response time?

Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

 6

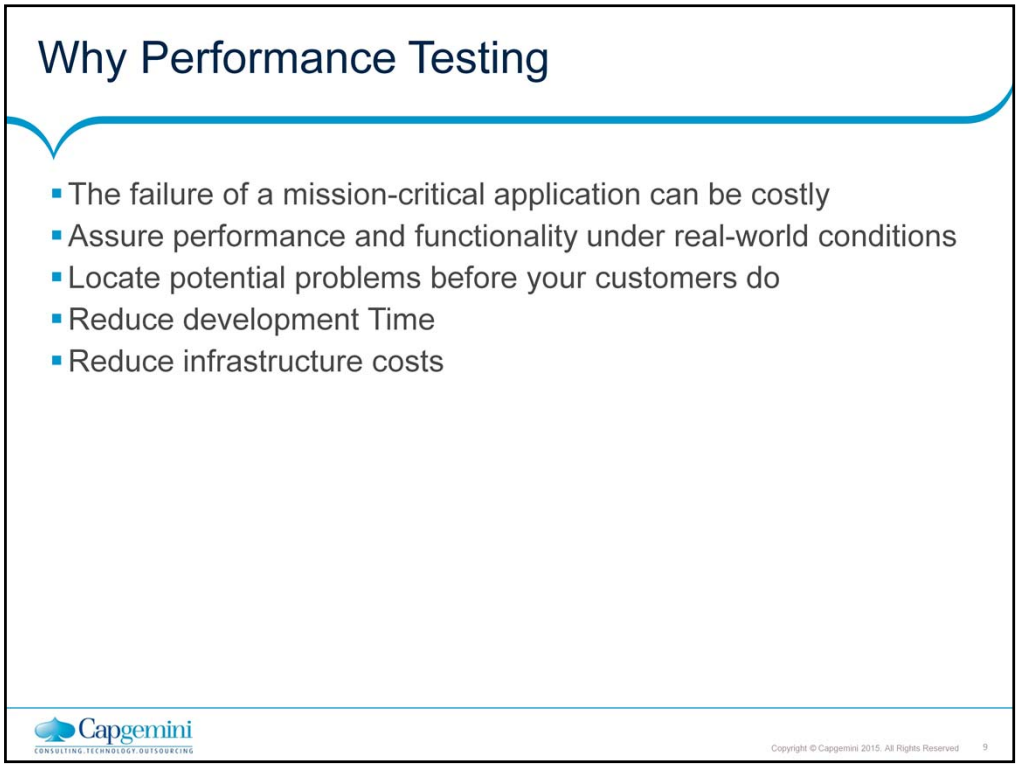

Types of Performance Testing
Load Testing
Find out whether the system can handle the expected load upon deployment under real-world conditions.
Stress Testing
Find the application's breaking point. Apply testing that measures whether the application's environment is properly configured to handle expected or potentially unexpected high transaction volumes.
Endurance Testing
It is testing the application under heavy volumes of data for a prolonged period of time and Checks for memory leaks or other problems that may occur with prolonged execution.
Scalability Testing
Determine the maximum number of concurrent users an application can manage.
Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING
Copyright © Capgemini 2015. All Rights Reserved
7

When To Do Performance Testing

- During Design and Development:
  - What is the best server to support target load
  - Define system performance requirements
- Before Release
  - Is the system reliable enough to go in to production
  - After functional testing done
- Post Deployment
  - What is the cause of performance degradation

Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

 8


Why Performance Testing
The failure of a mission-critical application can be costly
Assure performance and functionality under real-world conditions
Locate potential problems before your customers do
Reduce development Time
Reduce infrastructure costs
Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING
Copyright © Capgemini 2015. All Rights Reserved
9

Performance Test Terminology

- Scenarios
  - Using LoadRunner, you divide your application performance testing requirements into scenarios
  - A scenario defines the events that occur during each testing sessions
  - For example, a scenario defines and controls the number of users to emulate, the actions that they perform, and the machines on which they run their emulations

- Vusers
  - In a scenario, LoadRunner replaces human users with virtual users or Vusers.
  - When you run a scenario, Vusers emulate the actions of human users—submitting input to the server.
  - A scenario can contain tens, hundreds, or even thousands of Vusers.

Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

 10

Performance Test Terminology (Cont.)

- Vuser Scripts
  - The actions that a Vuser performs during the scenario are described in a Vuser script
  - When you run a scenario, each Vuser executes a Vuser script. Vuser scripts include functions that measure and record the performance of the server during the scenario.

- Transactions
  - To measure the performance of the server, you define transactions
  - Transactions measure the time that it takes for the server to respond to tasks submitted by Vusers

Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

 11

Performance Test Terminology (Cont.)

- Rendezvous Points
  - You insert rendezvous points into Vuser scripts to emulate heavy user load on the server
  - Rendezvous points instruct multiple Vusers to perform tasks at exactly the same time
  - For example, to emulate peak load on the bank server, you insert a rendezvous point to instruct 100 Vusers to simultaneously deposit cash into their accounts

- VuGen
  - The primary tool for creating Vuser Script is Virtual User Generator, (VuGen)
  - VuGen not only records Vuser scripts, but also runs them in animated display.
  - When you record a Vuser script, VuGen generates various functions that define the actions that you perform during the recording session.
  - Parameterization & Correlation are applied in script to use different data dynamically.

Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

 12

Performance Test Terminology (Cont.)

- Controller
  - You use the LoadRunner Controller to manage and maintain your scenarios
  - Using the Controller, you control all the Vusers in a scenario from a single workstation

Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

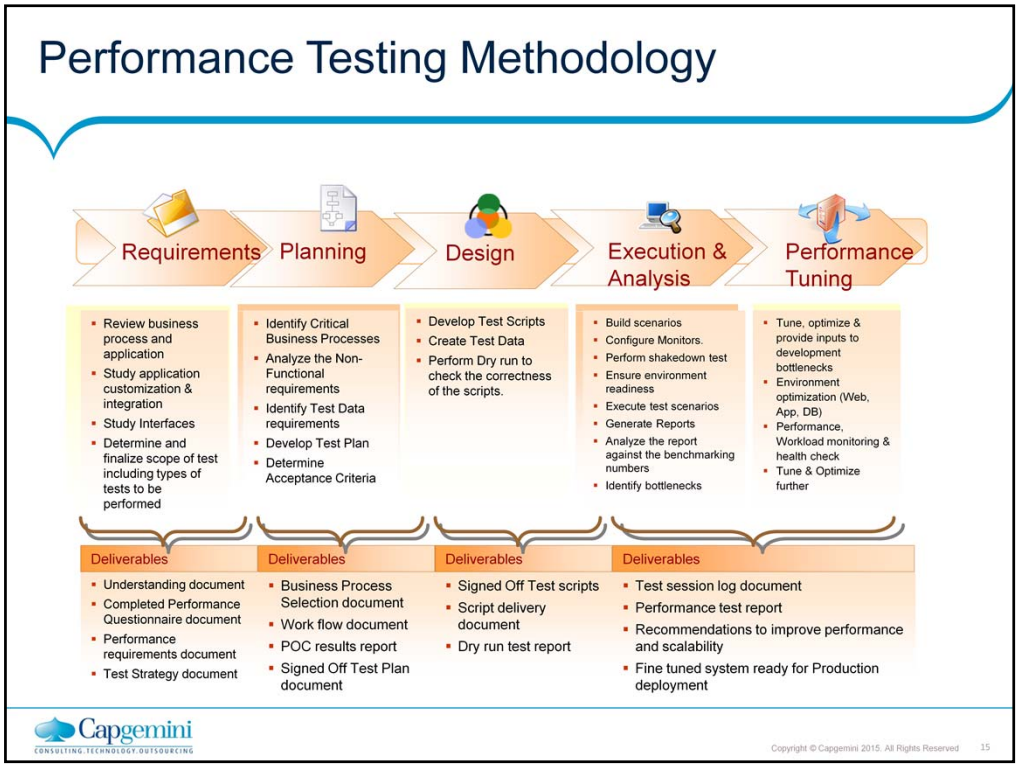
 13

Performance Test Terminology (Cont.)

- Hosts
  - When you execute a scenario, the LoadRunner Controller distributes each Vuser in the scenario to a host
  - The host is the machine that executes the Vuser script, enabling the Vuser to emulate the actions of a human user

- Performance Analysis
  - Vuser scripts include functions that measure and record system performance during load-testing sessions
  - During a scenario run, you can monitor the network and server resources
  - Following a scenario run, you can view performance analysis data in reports and graphs
  - Performance Analysis will be used to Analyse the results and create graphs and reports to present the performance test report to stake holders.

Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING


Performance Testing Methodology
Requirements
Planning
Design
Execution & Analysis
Performance Tuning
Review business process and application
Study application customization & integration
Study Interfaces
Determine and finalize scope of test including types of tests to be performed
Identify Critical Business Processes
Analyze the Non-Functional requirements
Identify Test Data requirements
Develop Test Plan
Determine Acceptance Criteria
Develop Test Scripts
Create Test Data
Perform Dry run to check the correctness of the scripts.
Build scenarios
Configure Monitors.
Perform shakedown test
Ensure environment readiness
Execute test scenarios
Generate Reports
Analyze the report against the benchmarking numbers
Identify bottlenecks
Tune, optimize & provide inputs to development bottlenecks
Environment optimization (Web, App, DB)
Performance, Workload monitoring & health check
Tune & Optimize further
Deliverables
Understanding document
Completed Performance Questionnaire document
Performance requirements document
Test Strategy document
Deliverables
Business Process Selection document
Work flow document
POC results report
Signed Off Test Plan document
Deliverables
Signed Off Test scripts
Script delivery document
Dry run test report
Deliverables
Test session log document
Performance test report
Recommendations to improve performance and scalability
Fine tuned system ready for Production deployment
Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING
Copyright © Capgemini 2015. All Rights Reserved
15

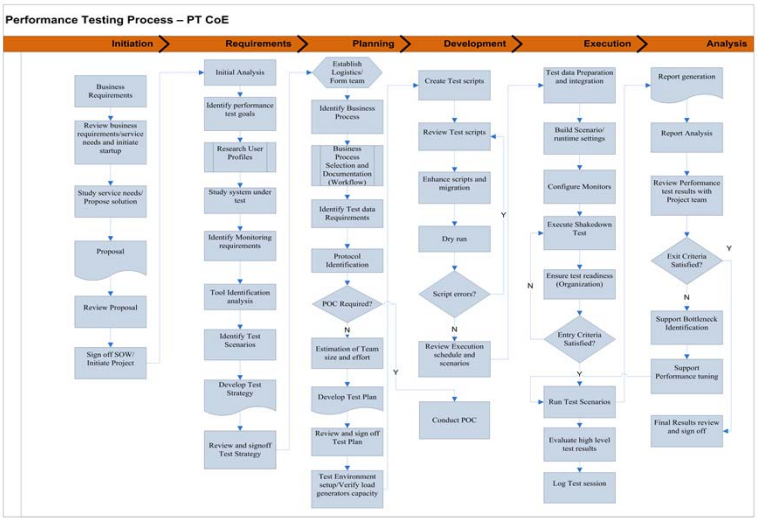
Performance Testing Methodology

- System Resource - Performance Parameters Monitored
- The basic system resource parameters monitored during performance testing include:
  - Processor Usage : Amount of processor time to process particular action
  - Memory Usage : Amount of physical memory available to process on system
  - Disk time : Amount of time, disk is busy executing a read or write request
  - Bandwidth : Shows the bits per second used by network interface

Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

 16

Performance Testing Process/Phases



Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

 17

Analyzing Performance Requirements

- The main objective of this phase is to chalk out the Performance Requirements in detail and identify the critical business scenarios which need to be monitored
- Architecture (Hardware and Software) of the application is analyzed with respect to the specific performance requirements for the project
- All the critical transactions in the application are gathered and identified for Performance Testing along with the user profile and usage pattern
- Client feedback and analysis of logs for existing application are gathered as the key inputs
- The above inputs would help in deciding the load patterns to be applied on the application and the parameters to be monitored

Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

 18

Analyzing Performance Requirements

- Activities:
  - Perform Initial analysis to identify understand project status, schedule and existing testing practices
  - Understand product engineering and support organization structure and processes
  - Complete Performance questionnaire
  - Identify goals of performance testing
  - Research User profiles
  - Study system under test and understand Application Architecture & Network topology
  - Prepare Understanding Document
  - Identify Monitoring requirements
  - Create performance test requirements document
  - Identify Type of test needed
  - Identify test scenarios
  - If required perform Tool comparison analysis, Tool recommendation & procurement
  - Prepare Test Strategy
  - Review & Signoff Test strategy

Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

 19

Performance Planning

- Test planning stage involves planning with regard to the people, software (including testing tools) and hardware resources required for the project
- Necessary Connectivity setup to test regions is established and verified during this phase
- Test data and Test plan is prepared for the requirements collected
- A decision on the test environment and the tools to be used for monitoring the parameters on each tier (Web Server, Application Layer, Database layer) is taken based on the requirements analysis
- The necessary approach for carrying out the Load, Stress and Endurance testing is detailed out during this phase along with the inputs in terms of number of virtual users, no of test runs etc

Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

 20

Performance Script Design

- The test environment is verified for test readiness initially
- After it is verified, the test scripts are recorded/ developed for the base lined test scenarios using the selected load test tool Parameterization is done for the scripts for varied user sets of data
- The results of the test scripts generated are verified with the business requirements and base lined if the same is found acceptable

Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

 21

Performance Script Design

- Activities:
  - Develop test scripts according to workflow document using identified test tool
  - Ensure scripting standards are followed
  - Conduct Script review
  - Enhance scripts and plan script migration if required
  - Ensure volume of test data
  - Conduct dry run of all test scripts
  - Publish dry run test results
  - Prepare script delivery document
  - Review execution schedule and scenarios

Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

 22

Performance Script Execution

- The test execution is carried out in the base lined test environment either over the Internet at Client location or is simulated in performance test LAB based on the chosen delivery mechanism
- Log setting to capture the test sequence of events are set and observed.
- The load is generated as per the strategy defined and the results are captured for the various load pattern and scenarios identified

Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

 23

Performance Script Execution

- Activities:
  - Generate and Integrate test data into scripts
  - Build scenario according to work load model
  - Set up Run time settings
  - Setup performance counters (Monitors)
  - Execute shakedown test
  - Ensure test readiness from all teams involved with the project
  - Run Test Scenarios
  - Monitor high level system performance counters
  - Capture metrics/ Log test session information

Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

 24

Performance Result Analysis

- The test results are reviewed and analyzed for any bottlenecks in the application by a team of experts for the various Hardware platforms, Operating systems, Databases and Software design
- Performance gaps are evaluated and solution approaches for the identified bottlenecks are defined
- Suggestion for tuning the application is also recommended

Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

 25

Performance Result Analysis

- Activities:
  - Create performance test results report
  - Publish report and Maintain error log
  - Review Performance test results with Project team
  - Verify results with requirements
  - Analyze reports for bottlenecks and recommend performance improvement solutions
  - Support performance tuning activity
  - Re run Test scenarios
  - Re run test scenarios until requirements are satisfied
  - Project Closure

Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

 26

Introduction to Performance Testing Tools

- Protocol Support:
  - Load testing tools either emulate load or simulate users
  - Simulation involves duplication of actual user activity on the GUI/front-end with the intention of replaying it again
  - Emulation involved protocol replay - for this a rich API of protocol-related functions are required
  - A good tool will not be restricted to a single protocol and should support multiple protocols including HTTP/S, FTP, SMTP, Oracle NCA, DB2 CLI, Citrix ICA, SAP, WAP, Voice XML, Peoplesoft, SIEBEL

Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

 27

Introduction to Performance Testing Tools

- Record & Playback support :
  - This category details how easy it is to record & playback a test
  - Is there object recognition when recording and playing back or does it appear to record ok but then on playback (without environment change or unique id's, etc changes) fail?
  - How easy is it to read the recorded script
- Strong scripting language :
  - The scripting language supported by the automated tool should be understandable and precise
  - It should not generate lengthy codes which are difficult to maintain
  - It should resemble to common languages like C, C++, Java etc. It should be easy to debug

Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

 28

LoadRunner

- LoadRunner is HP\Mercury Interactive tool for testing the performance of applications
- LoadRunner stresses your entire application to isolate and identify potential client, network, and server bottlenecks
- LoadRunner enables you to test your system under controlled and peak load conditions. LoadRunner can runs thousands of Virtual Users that are distributed over a network
- Reduces the personal requirements by replacing the human users with virtual users (Vuser)
- As Vusers can run on a single machine, Load runner reduces the hardware requirements

Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

 29

LoadRunner

- LoadRunner controller allows you to easily and effectively control all the Vusers from a single point of control
- LoadRunner monitors the application performance online, enabling you to fine tune your system during test execution
- LoadRunner automatically records the performance of the application during a test. You can choose from a wide variety of graphs and reports to view the performance data
- Because LoadRunner tests are fully automated you can easily repeat them as often as you need
- LoadRunner check performance delays occurring in network, CPU performance, I/O delays, database locking

Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

 30

QALoad

- QALoad is Compuware tool for testing the performance of applications
- What QALoad Does
  - Records users interactions with the application using the Script Development Workbench
  - Records application business process at the protocol level
  - QALoad executes multiple Virtual Users against an application to test the software and hardware servers and business logic (Web Servers, Database Servers, networks, Windows and Unix Servers, etc.)
- What QALoad Does Not Do
  - QALoad does not test the graphical user interface (GUI)
  - QALoad does not execute fine-grained tests to verify business process functionality

Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

 31

eLoad

- E-Load provides the easiest and most accurate way to test the scalability of your e-commerce and e business applications
- E-Load is the load and scalability testing component of the e-TEST suite. Like its companion products, e-Tester and e-Manager, e-Load requires no programming and is operated using an intuitive graphical user interface and powerful Visual Scripts
- Allows you to access e-Load from any networked machine using a web browser
- Allows multiple users to collaborate during testing by connecting to the same in progress test session to view and analyze results

Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

 32

eLoad

- e-Load Features:
- E-Load offers the following advantages for load testing Web-based applications:
  - Accurately emulates real user interactions and tests for correct responses
  - Requires no programming and re-uses your functional and regression tests scripts with no modifications
  - Enables you to vary load conditions on-the-fly to try "what-if" scenarios, and create comprehensive reports and graphs with the touch of a button

Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

 33

JMeter

- Apache JMeter is a 100% pure Java desktop application designed to load test functional behavior and measure performance. It was originally designed for testing Web Applications but has since expanded to other test functions
- Apache JMeter may be used to test performance both on static and dynamic resources (files, Servlets, Perl scripts, Java Objects, Data Bases and Queries, FTP Servers and more)
- It can be used to simulate a heavy load on a server, network or object to test its strength or to analyze overall performance under different load types
- You can use it to make a graphical analysis of performance or to test your server/script/object behavior under heavy concurrent load

Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

 34

JMeter

- Apache JMeter features include:
  - Can load and performance test many different server types:
    - Web - HTTP, HTTPS
    - SOAP
    - Database via JDBC
    - LDAP
    - JMS
    - Mail - POP3
  - Complete portability and 100% Java purity
  - Full Swing and lightweight component support (precompiled JAR uses packages javax.swing.*)
  - Full multithreading framework allows concurrent sampling by many threads and simultaneous sampling of different functions by separate thread groups

Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

 35

JMeter

- Caching and offline analysis/replaying of test results
- Highly Extensible:
  - Pluggable Samplers allow unlimited testing capabilities
  - Several load statistics may be chosen with pluggable timers
  - Data analysis and visualization plug-ins allow great extendibility as well as personalization
  - Functions can be used to provide dynamic input to a test or provide data manipulation
  - Scriptable Samplers (BeanShell is fully supported; and there is a sampler which supports BSF-compatible languages)

Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

 36

Summary

- In this lesson, you have learnt:
  - What is Performance Testing?
  - Objectives of Performance Testing
  - IGATE Performance Testing Methodology
  - Different tools used in Performance Testing

Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

 37

Non Functional Testing

Lesson 2: Introduction to Web Security

Lesson Objectives

- To understand the following topics:
  - Security Testing
  - Why Security Defects Occur?
  - OWASP Top Ten Vulnerabilities
  - Cross Site Scripting (XSS)
  - Injection Flaws
  - Broken Authentication and Session Management
  - Failure To Restrict URL Access
  - Cross Site Request Forgery(CSRF)
  - Unvalidated Redirects and Forwards
  - Insecure Direct Object References
  - Security Misconfiguration
  - Insecure Cryptographic Storage
  - Insecure Communications
  - Summary

Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

 2

Security Testing

Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

 3

Security Testing

Why Security Testing?

With more than one million new web applications being launched each month and successful hacker attacks in the news each week.... application security is no longer an afterthought...

Hackers are concentrating their efforts on web-based applications – online banking, shopping carts, forms, login pages, dynamic content, etc.. Accessible 24/7 from anywhere in the world, insecure web applications provide easy access to backend corporate databases and also allow hackers to perform illegal activities using the attacked sites.

If these web applications are not secure, then organizations entire database of sensitive information is at serious risk. A Gartner Group study reveals that 75% of cyber attacks are done at the web application level.

A Security test is a method of evaluating the security of a application or network by simulating an attack by a malicious user knows as a Black Hat Hacker, or Cracker

In General

- Tool Based Application security scanning for detecting the vulnerabilities at
  - Web Applications, Infrastructure
  - Web Services, database, Network
- Regulatory Compliance test for HIPPA, PCI, SOX etc...
- Inline with industry security standards includes SANS Top 20, OWASP Top 10, and WASC Threat Classification

Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

 4

Are you Aware?

- Web applications are the #1 focus of hackers:
  - 75% of attacks at Application layer (Gartner)
  - XSS and SQL Injection are #1 and #2 reported vulnerabilities (MITRE)
- Most sites are vulnerable:
  - 90% of sites are vulnerable to application attacks (Watchfire)
  - 78% of easily exploitable vulnerabilities affects Web applications (Symantec)
  - 80% of organizations will experience an application security incident by 2010 (Gartner)
  - 2/3 Web applications are vulnerable (Gartner)

Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

 5

Are you Aware?

- Web applications are high value targets for hackers:
  - Financial & Banking Data like Customer data, credit cards data, ID theft, fraud, site defacement, etc.. are few high value targets
- Compliance requirements:
  - Payment Card Industry (PCI) Standards, GLBA, HIPPA, FISMA are the recommended web security compliances

Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

 6

Why Security Defects Occur?

- Root Cause:
  - Developers are not trained to write or test for secure code
  - Network security (firewall, IDS, etc.) does not protect the Web Application Layer
- Current State:
  - Organizations do security test tactically at a late & costly stage in the SDLC
  - Gap exists between security standards and development standards resulting in vulnerabilities not getting fixed
  - Testing coverage is incomplete without security testing

Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

 7

Why Security Defects Occur?

- Application Security Testing should be an integral part of the release and life cycle of every web application
- As the number of web applications are growing every day and the frequent discovery of new vulnerabilities, the best way of ensuring security in web applications is to include security testing as part of the SDLC
- Unfortunately, the reality is that security testing is not given enough importance

Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

 8

OWASP Top Ten Vulnerabilities

Application Threat	Negative Impact	Example Impact
Cross Site scripting	Identity Theft, Sensitive Information Leakage, …	Hackers can impersonate legitimate users, and control their accounts.
Injection Flaws	Attacker can manipulate queries to the DB / LDAP / Other system	Hackers can access backend database information, alter it or steal it.
Broken Authentication and Session Management	Session Tokens not guarded or invalidated properly	Hackers can steal session tokens of the application users after signoff.
Failure to Restrict URL Access	Hacker can access unauthorized resources	Hacker can forcefully browse and access any static page past the login page
Cross-Site Request Forgery	Attacker can invoke "blind" actions on web applications, impersonating as a trusted user	Hackers can get customer details thru trial &error method to perform illegal financial transactions such as funds transfers.
Unvalidated Redirects and Forwards	Phishing attack	An attacker can redirect the user to fake HDFC bank and steal his netbanking credentials
Insecure Direct Object Reference	Attacker can access sensitive files and resources	Hackers can manipulate Web Application URL to get contents of the sensitive file(instead of the harmless one)
Security Misconfiguration	Attackers can gain unauthorized access to some or complete system data	Malicious application messages may assist hackers in developing further attacks
Insecure Cryptographic Storage	Weak encryption techniques may lead to broken encryption	Confidential information (SSN, Bank A/c details, Credit Cards) can be decrypted by malicious users
Insecure Communications	Sensitive info sent unencrypted over insecure channel	Unencrypted data like bank statements can be used by hacker to impersonate user

Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

 9

Cross Site Scripting(XSS) Overview

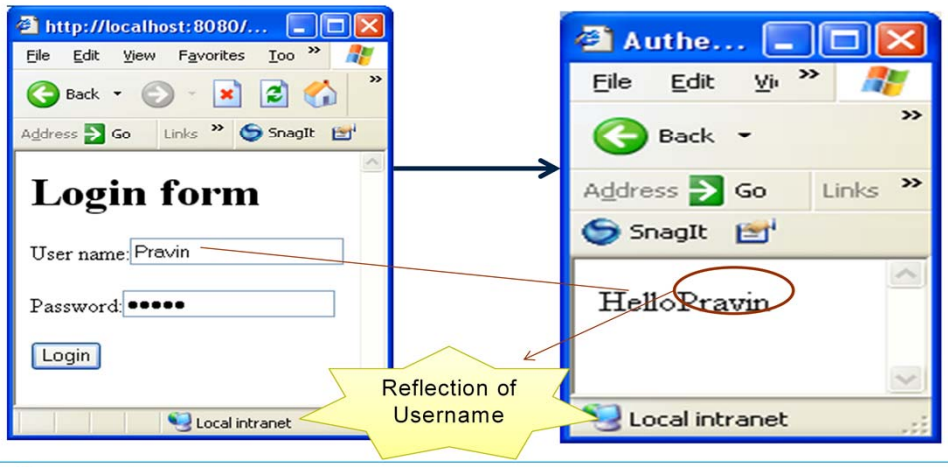
- Cross-Site Scripting attacks are injection problem, in which some harmful javascript are entered in the web pages
- The injected script execute when the victims accesses the page
- Due to the execution of the script, the attacker can hijack user sessions, deface web sites, redirect users to attackers web sites

Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

 10

Cross Site Scripting Scenario

- Valid Credentials are required for login in the application

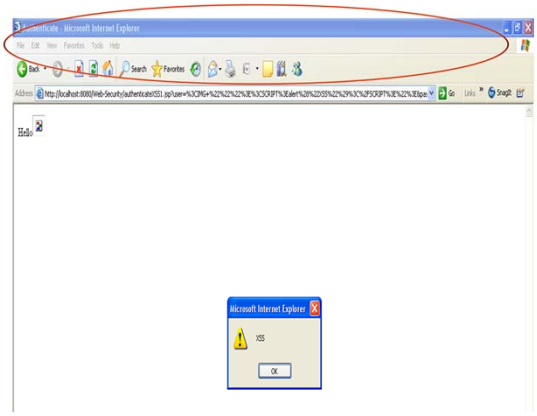


Cross Site Scripting Scenario(contd.)

- Script can be entered in the textbox instead of the normal text and script can be executed

Or .. Even this works
<IMG SRC=javascript:
alert('XSS')>

Cross Site Scripting Scenario(contd.)



Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

XSS Causes and Prevention

- Causes:
  - Poor validations
  - Allowing any script program to run, without prompting end user with a warning
- Prevention:
  - Carefully validate all data before processing it
  - Validate the length, characters, format before accepting the input.

Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

Injection Flaws Overview

- Injection flaws occur when an application uses unvalidated data to form any of the following queries:
  - SQL
  - LDAP
  - XPATH
- An attacker can inject queries instead of the valid inputs and perform malicious activities

Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

 15

SQL Injection Overview

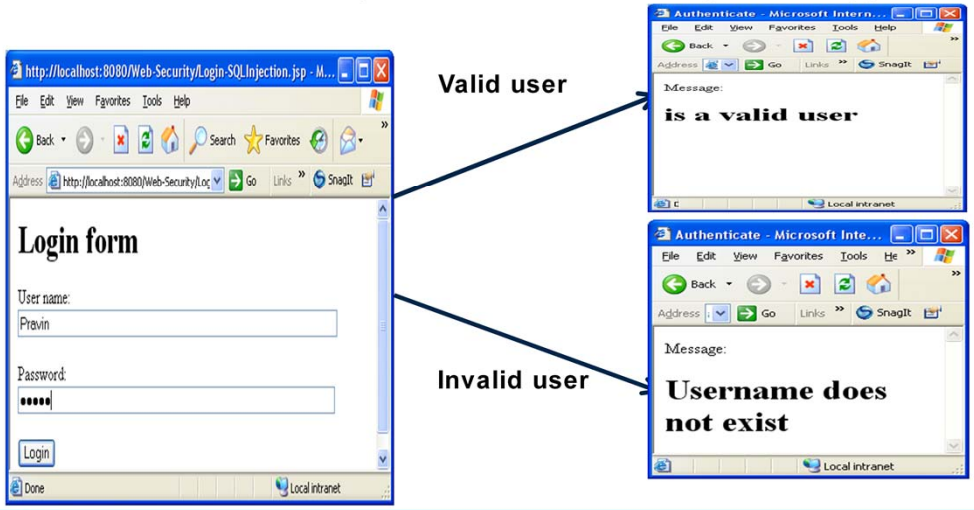
- SQL Injection attack is one of the most prominent type of injection flaw
- By entering malicious SQL commands as inputs, the attacker can manipulate the backend SQL query
- Injection can result in data loss or corruption. Injection can sometimes lead to complete host takeover

Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

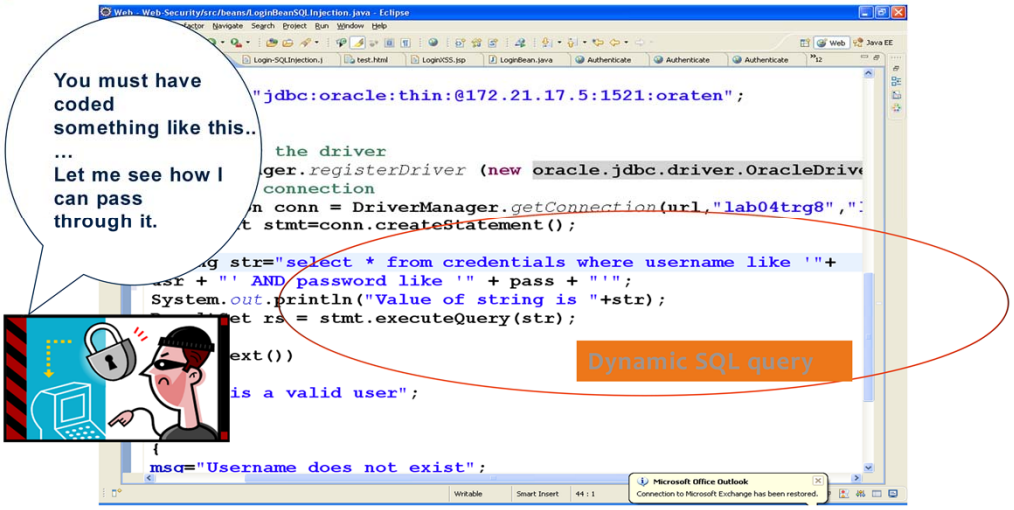
 16

Injection Flaws Scenario

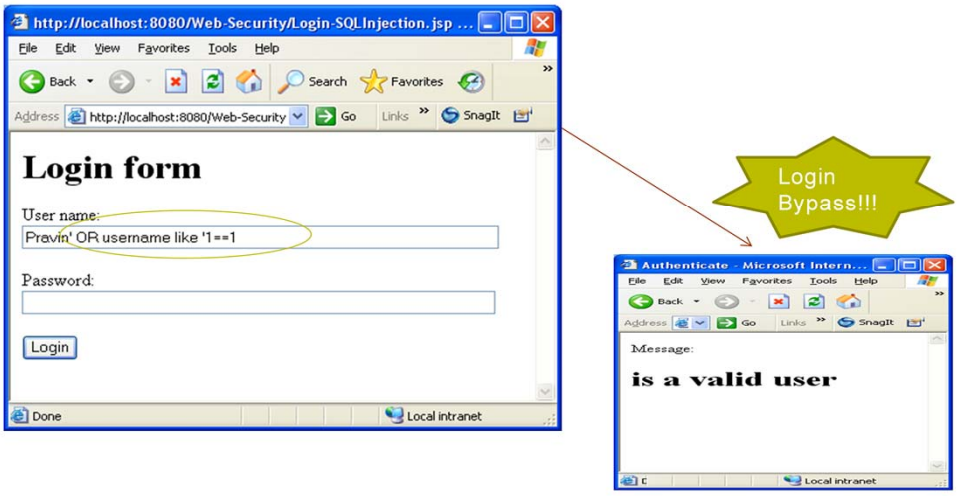
- Valid Credentials are required for authenticated login in the application



Injection Flaws Scenario(contd.)



Injection Flaws Scenario(contd.)



Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

Injection Flaws Causes and Prevention

- Causes:
  - User input is not filtered for escape characters
  - Use of dynamic or concatenated queries
- Prevention:
  - Use parameterized queries
  - Perform Input Validation

Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

 20

Broken Authentication and Session Management Overview

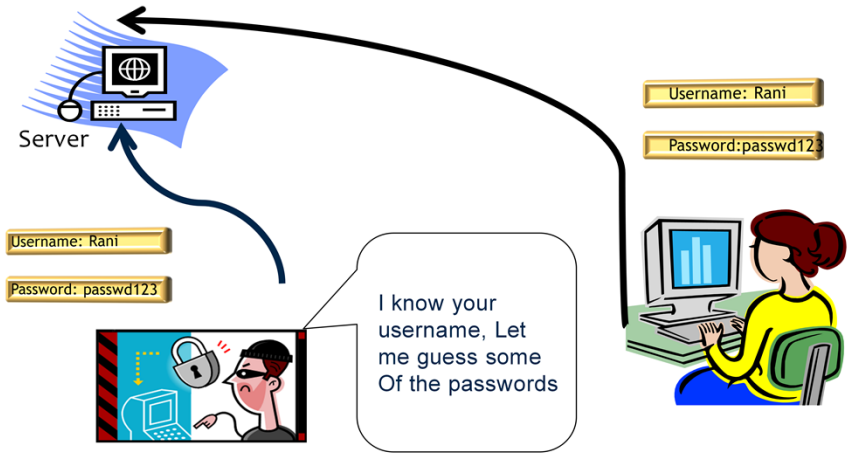
- This is related to the flaws in Authentication and session management schemes which have flaws in areas such as:
  - Logout
  - Password management
  - Timeouts
  - Remember me
  - Secret question
  - Account update, etc.
- Such flaws may allow some or even all accounts to be attacked
- Once successful, the attacker can do anything the victim could do

Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

 21

Broken Authentication and Session Management Scenario 1

- Password as a dictionary word

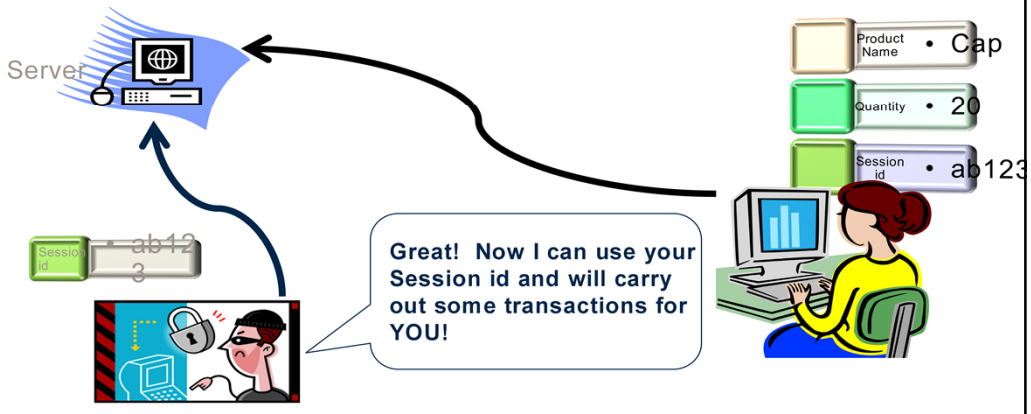


Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

 22

Broken Authentication and Session Management Scenario 2

- Poor Session Management. The Session Id of the victim can be gained by the attacker which then can be used to hijack the user session



Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

 23

Broken Authentication and Session Management Causes

- Credentials are transferred to the server in insecure manner
- Session invalidation is not managed properly
- Custom session management mechanism could be complex but, not very reliable
- Using URL Rewriting for session management
- Not implementing a strong authentication mechanism
- Not Implementing a strong password policy
- Application does not use a different Session ID each time a user logs in

Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

 24

Broken Authentication and Session Management Prevention

- Use SSL/TLS at least for authentication related processes
- Use of inbuilt session management mechanism
- Do not accept any session identifier from the URL or in the request
- Limit code of custom cookies for authentication or session management
- Implement a strong authentication mechanism, use Captcha while resetting the password
- Implement a strong password policy when allowing passwords
- Ensure that every page has a logout link, also keep timeout period for session

Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

 25

Failure To Restrict URL Access Overview

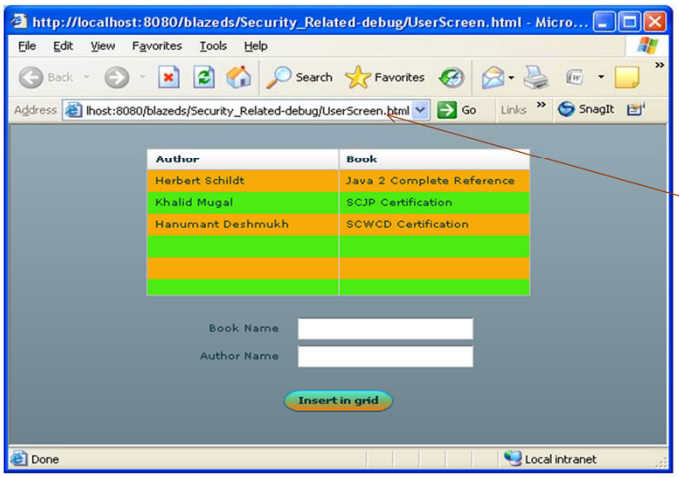
- Forced browsing: It is the primary attack method for failure to URL access
- It requires guessing the links and brute force techniques to find unprotected pages
- Attacker can change the URL of a restricted page and try to access it

Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

 26

Failure To Restrict URL Access Scenario 1

- Hidden or Special URLs:



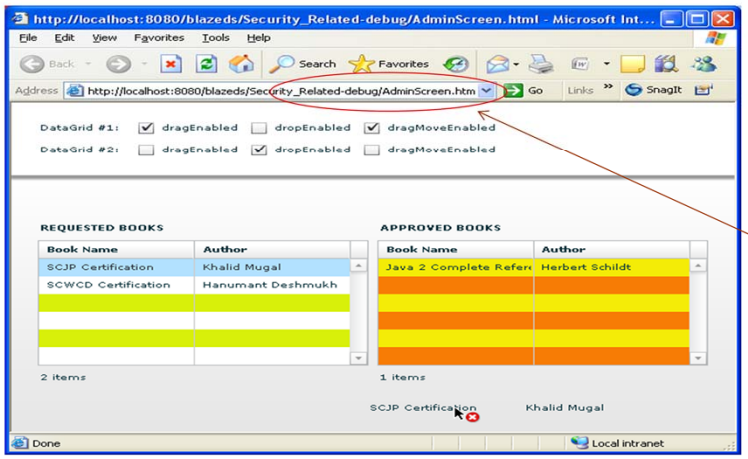
There might be XXXRoleScreen.html as well when the application has UserScreen.html

Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

 27

Failure To Restrict URL Access Scenario 2

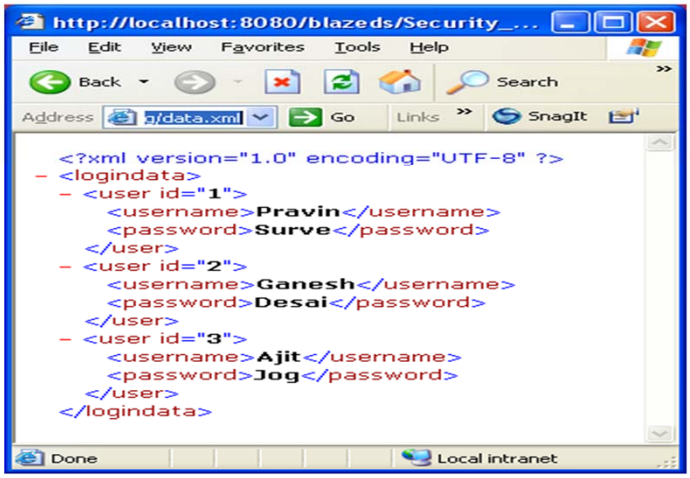
- Attacker can access to Admin Page



Access To Admin Page is obtained by using AdminScreen.htm

Failure To Restrict URL Access Scenario 3

- Attacker can gain access of some hidden files



Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

 29

Failure To Restrict URL Access Causes And Prevention

- Causes:
  - Applications does not apply authorization check in the pages
- Prevention:
  - The role based authorization checks must be applied on all pages
  - The enforcement mechanism(s) should deny all access by default, requiring explicit grants to specific users and roles for access to every page

Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

 30

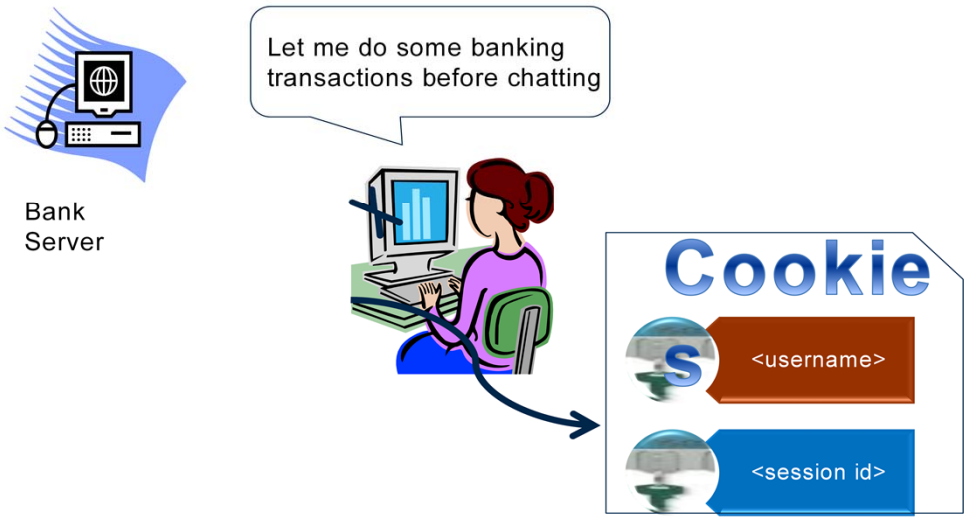
Cross Site Request Forgery(CSRF) Overview

- Browsers send credentials like session cookies automatically
- Attacker creates forged HTTP requests and tricks a victim into submitting them via image tags, malicious links, or numerous other techniques
- If the user is authenticated, the attack succeeds
- Attackers can update account details, make purchases, logout and even login

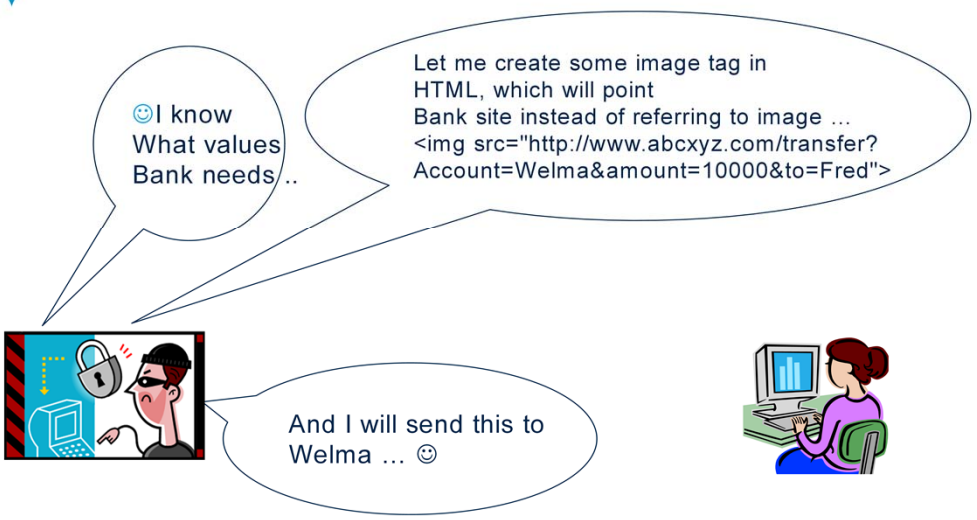
Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

 31

Cross Site Request Forgery Scenario(contd.)



Cross site Request Forgery Scenario(contd.)

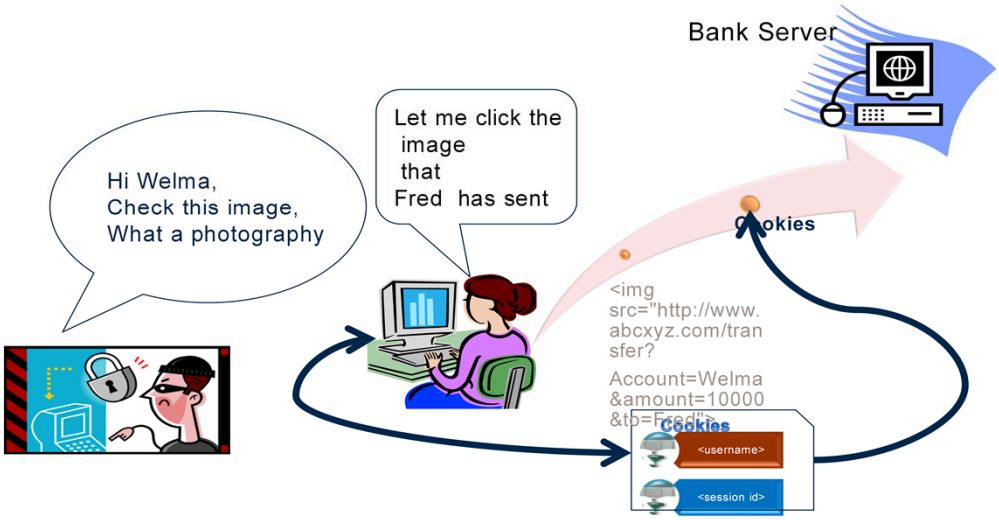


Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

Capgemini Internal

 33

Cross site Request Forgery Scenario (contd.)

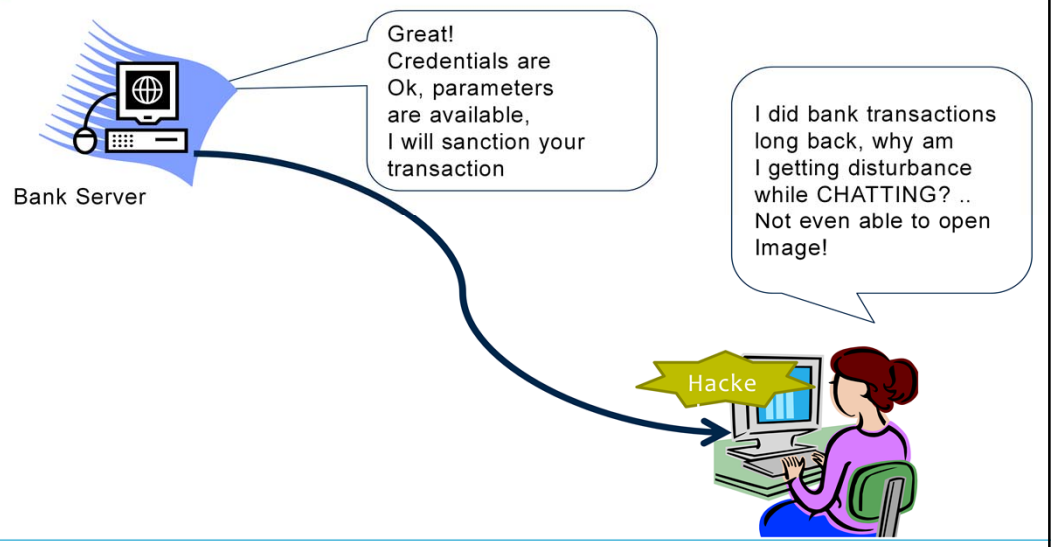


Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

Capgemini Internal

 34

Cross Site Request Forgery Scenario(contd.)



Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

Capgemini Internal

 35

Cross Site Request Forgery Causes and Prevention

- Causes:
  - Users identity from cookies
  - Clients not logging out
- Prevention:
  - Inclusion of unpredictable token in each HTTP Request
  - Inclusion of token in hidden field
  - Limit session lifetime and invalidate session as user logs off.

Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

Unvalidated Redirects and Forwards Overview

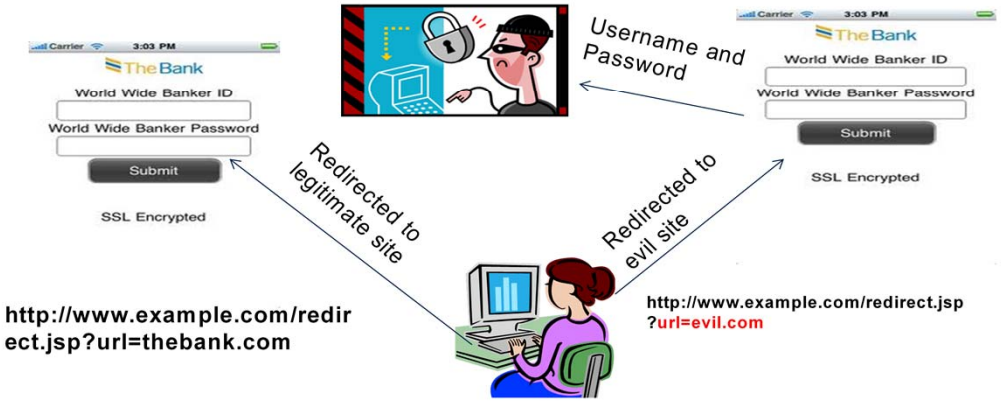
- Applications frequently redirect users to other pages, or use internal forwards in a similar manner
- Unvalidated redirects and forwards happen when, attacker redirects user to unintended pages or websites like phishing, malware sites

Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

 37

Unvalidated Redirects Scenario

- The application has a page called “redirect.jsp” which takes a single parameter named “url”. The attacker crafts a malicious URL that redirects users to a malicious site that performs phishing



Unvalidated Redirects and Forwards Causes and Prevention

- Causes:
  - Source of request not checked before forwarding or redirecting
  - User accesses link in email or forum, or from social networking site
- Prevention:
  - Simply avoid using redirects and forwards.
  - If used, don't involve user parameters in calculating the destination. If used apply necessary validation
  - Permit redirection only to valid or limited number of sites

Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

 39

Insecure Direct Object References Overview

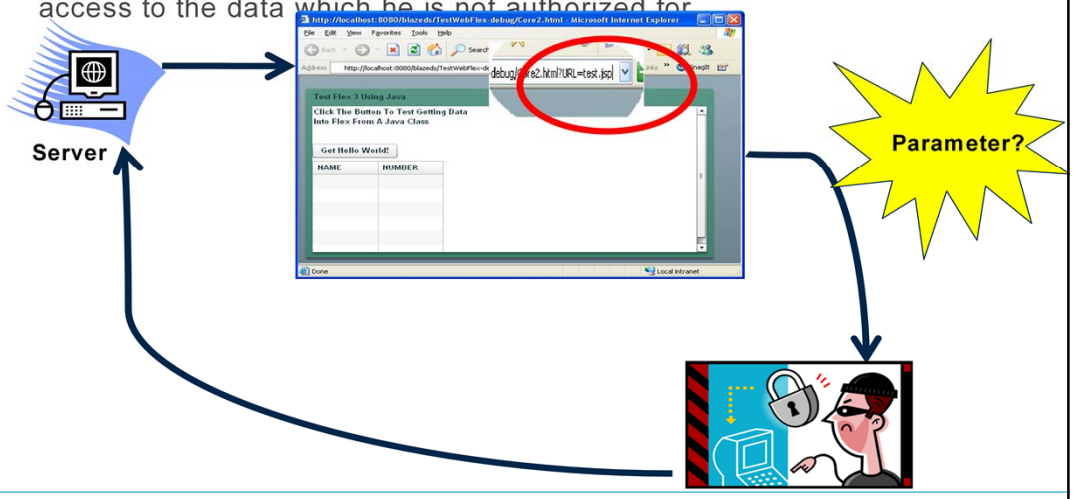
- Applications frequently display records or objects based on unique reference IDs in web pages
- Attacker changes that value of the parameter that directly refers to a system object to another object that he is not authorized for
- Applications don't always verify the user is authorized for the target object. This results in an insecure direct object reference flaw
- Such flaws can compromise all the data that can be referenced by the parameter

Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

 40

Insecure Direct Object Reference Scenario

- Attacker may guess a parameter value and if the guess is right he can gain access to the data which he is not authorized for



Insecure Direct Object Reference Causes and Prevention

- Causes:
  - Private object references like filenames, parameters are exposed to end users
  - Exposing direct references to database objects
- Prevention:
  - Include an access control check to ensure the user is authorized for the requested object.

Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

Security Misconfiguration Overview

- Good security requires having a secure configuration defined and deployed for the:
  - Application
  - frameworks
  - application server
  - web server,
  - database server
  - platform.
- Application Misconfiguration attack exploits configurationweaknesses in the web application

Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

 43

Security Misconfiguration Overview

- Attacker accesses
  - default accounts
  - unused pages
  - unpatched flaws
  - unprotected files and directories, etc.. to gain unauthorized access to or knowledge of the system
- Such flaws frequently give attackers unauthorized access to some system data or functionality
- Occasionally, such flaws result in a complete system compromise

Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

 44

Security Configuration Causes and Prevention

- Causes:
  - Exceptions not handled properly
  - Insecure server level configurations
- Prevention:
  - Handling all exceptions/errors using proper using custom error pages.
  - Turn on all security configurations on the server and the frameworks
  - Update the server with latest version and its patches

Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

 45

Insecure Cryptographic Storage

- The most common flaw in this area is simply not encrypting data that deserves encryption
- When encryption is employed, unsafe key generation and storage, not rotating keys, and weak algorithm usage are other related issues

Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

 46

Insecure Cryptographic Storage Causes and Prevention

- Causes:
  - Use of user defined/custom cryptographic algorithms
  - Use of weak algorithms
  - Storage of private keys on machines
  - Use of weak encoding, which can be easily decoded
- Prevention:
  - Do not use user defined cryptographic algorithms or weak algorithms
  - Do not generate keys online
  - Store keys secretly

Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

Insecure Communications Overview

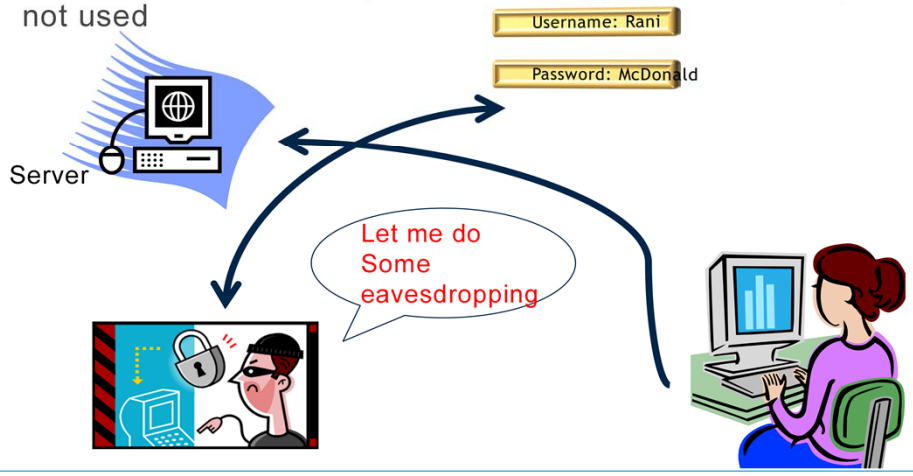
- Using SSL for communications with end users is critical, as they are very likely to be using insecure networks to access applications
- Because HTTP includes authentication credentials or a session token with every single request, all authenticated traffic needs to go over SSL, not just the actual login request

Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

 48

Insecure Communication Scenario

- Communication without HTTPS Protocol. The attacker can sniff the sensitive data which is passed unencrypted as HTTPS protocol is not used



Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

 49

Insecure Communication Prevention

- Use SSL for all connections that are authenticated or transmitting sensitive or value data, such as credentials, credit card details, health and other private information

Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

OWASP Top Ten Vulnerabilities - Recap

Application Threat
Cross Site scripting
Injection Flaws
Broken Authentication and Session Management
Failure to Restrict URL Access
Cross-Site Request Forgery
Unvalidated Redirects and Forwards
Insecure Direct Object Reference
Security Misconfiguration
Insecure Cryptographic Storage
Insecure Communications

Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

 51

Summary

- In this lesson, you have learnt:
  - What is Web Security?
  - Why today's web applications are not safe?
  - OWASP Top Ten Vulnerabilities
  - Causes & Preventions of OWASP Top Ten Vulnerabilities

Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

 52

Non Functional Testing

Lesson 3: Introduction to Data Warehouse, ETL & Data Warehouse Testing

Lesson Objectives

- To understand the following topics:
  - What is a Data Warehouse?
  - Need for Data Warehouse
  - Data Warehouse Architecture
  - Type of DWH Testing
  - ETL Process
  - ETL Testing
  - OLAP
  - OLAP Testing
  - End to End Testing
  - DWH/BI Performance Testing
  - SOA & Web Services
  - Summary

Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

 2

Introduction To Data Warehouse

Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

 3

What is Data Warehouse

- The concept of data warehousing is deceptively simple. Data is extracted periodically from the applications that support business processes and copied onto special dedicated computers
- There it can be validated, reformatted, reorganized, summarized, restructured, and supplemented with data from other sources
- The resulting data warehouse becomes the main source of information for report generation, analysis, and presentation through ad hoc reports, portals, and dashboards
- Data Warehouse is a single, complete and consistent store of enterprise data
  - It is obtained from a variety of sources
  - It is Central repository of information
  - It is a collection of master as well as transactional information
  - It contains read-only data
  - It contains historical data (spanning across years) for analysis purpose
  - It enables managers to make business decisions

Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

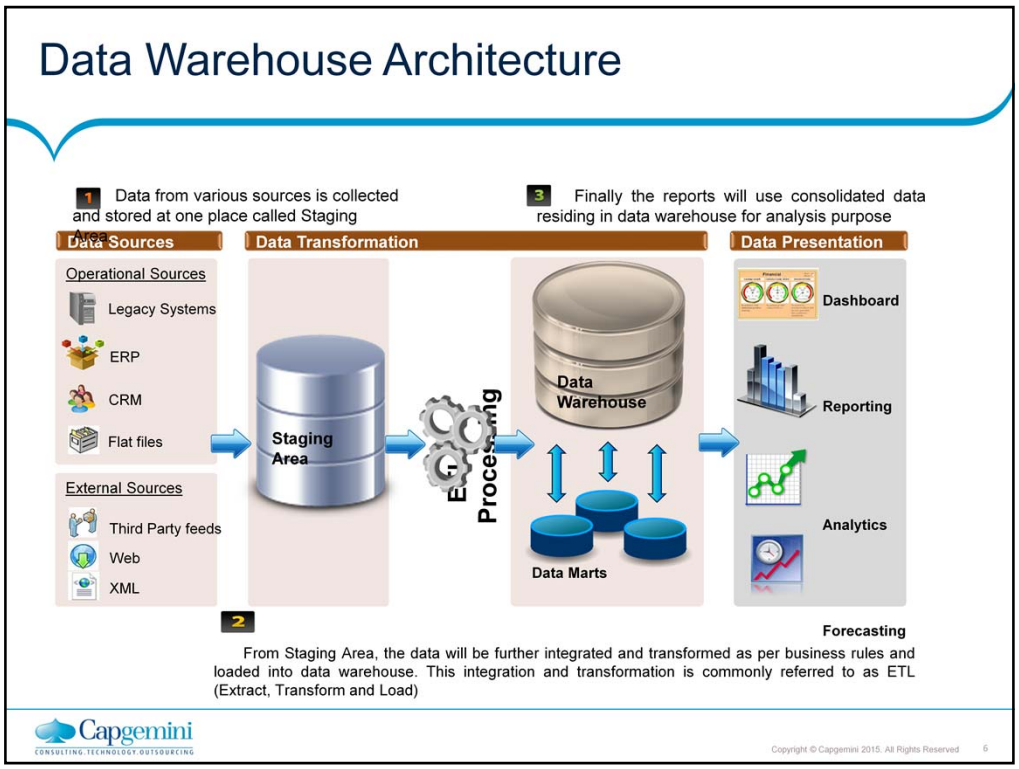
 4

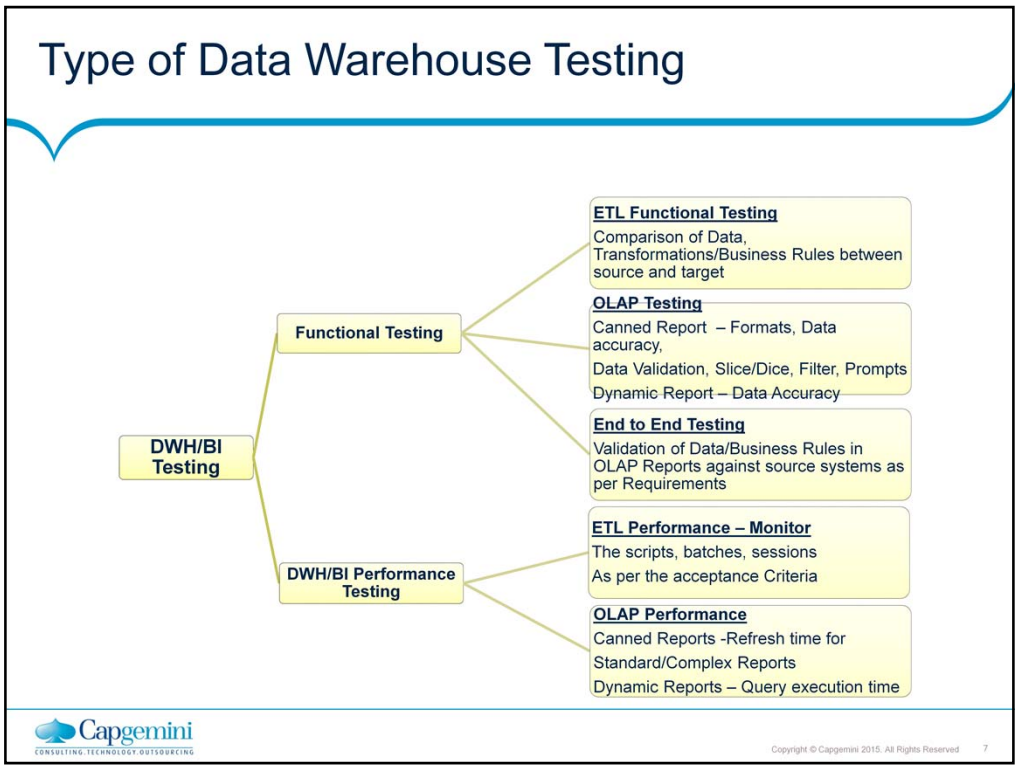
Need of Data Warehouse

- An On-line transaction processing system (OLTP) or operational system is used to typically deal with the everyday running of one aspect of an enterprise
- Organizations might have various OLTP systems covering individual aspects of business such as HR, Sales, CRM, Accounting etc. These systems are usually designed independently of each other and it is difficult for them to share information in a holistic way
- Hence there is a need to have a separate informational system all together which will provide a consolidated view of organizational data
- Data Warehouse is required to meet the following needs:
  - Provide integrated, company-wide view of information by consolidating data from disparate source systems
  - Separate research and decision support functions from the operational systems
  - Improve performance of business reports
  - Foundation for data mining, data visualization, advanced reporting and OLAP tools

Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

 5


Data Warehouse Architecture
1 Data from various sources is collected and stored at one place called Staging Area
3 Finally the reports will use consolidated data residing in data warehouse for analysis purpose
Data Sources
Data Transformation
Data Presentation
Operational Sources
Legacy Systems
ERP
CRM
Flat files
External Sources
Third Party feeds
Web
XML
Staging Area
ETL Processing
Data Warehouse
Data Marts
Dashboard
Reporting
Analytics
Forecasting
2
From Staging Area, the data will be further integrated and transformed as per business rules and loaded into data warehouse. This integration and transformation is commonly referred to as ETL (Extract, Transform and Load)
Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING
Copyright © Capgemini 2015. All Rights Reserved
6


Type of Data Warehouse Testing
DWH/BI Testing
Functional Testing
DWH/BI Performance Testing
ETL Functional Testing
Comparison of Data, Transformations/Business Rules between source and target
OLAP Testing
Canned Report – Formats, Data accuracy,
Data Validation, Slice/Dice, Filter, Prompts
Dynamic Report – Data Accuracy
End to End Testing
Validation of Data/Business Rules in OLAP Reports against source systems as per Requirements
ETL Performance – Monitor
The scripts, batches, sessions
As per the acceptance Criteria
OLAP Performance
Canned Reports -Refresh time for Standard/Complex Reports
Dynamic Reports – Query execution time
Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING
Copyright © Capgemini 2015. All Rights Reserved
7

ETL Process

- ETL stands for Extract, Transform and Load
- It is the process of extracting, refining and reorganizing the data from the source system and storing it in Enterprise Data Warehouse (EDW)
- The first part of an ETL process involves extracting the data from various source systems
- The transform stage applies a series of rules or functions to the extracted data from the source to derive the data for loading into the end target
- Below are some transformations involved in DWH

Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

 8

ETL Process

- Selecting only certain columns/records to load
- E.g. if the source data has three columns roll_no, age, and salary, then the extraction may take only roll_no and salary. Similarly, the extraction mechanism may ignore all those records where salary is not present (salary = null)
- Translating coded values (e.g. if the source database stores 1 for male and 2 for female, but the warehouse stores M for male and F for female)
- Deriving a new calculated value (e.g. sale_amount = qty * unit_price)
- Joining data from multiple sources (e.g. lookup, merge)
- Aggregation (e.g. Rollup — Total sales for each store, for each region, etc.)
- Splitting a column into multiple columns (e.g. converting a comma-separated list, specified as a string in one column, into individual values in different columns)
- The load phase loads the data into the end target, usually the data warehouse

Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

 9

ETL Testing

- ETL Testing primarily involves Comparison of Data between Source and target as per Transformations/ Business Rules and checking that the process is getting completed within specified time period
- Below is the list for various validations applicable in ETL testing:
  - Verify that data transformation from source to destination works as expected
  - Verify that expected data is added in target system
  - Verify that all database fields are loaded without any data truncation
  - Verify record count between source and destination match
  - Verify that for rejected data proper error logs are generated with all details
  - Verify NULL value fields for default values
  - Verify that duplicate data is not loaded

Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

 10

OLAP

- OLAP stands for Online Analytical Processing
- OLAP can be defined as the process of converting raw data into business information through multidimensional analysis
- Typical applications of OLAP include business reporting for sales, marketing, management reporting, business process management, budgeting and forecasting, financial reporting etc.
- OLAP consists of three basic analytical operations: consolidation (roll-up), drill-down, and slicing and dicing
  - Consolidation involves the aggregation of data that can be accumulated and computed in one or more dimensions. For example, all sales offices are rolled up to the sales department or sales division to anticipate sales trends.
  - Drill-down is a technique that allows users to navigate through the details. For instance, users can view the sales by individual products that make up a region's sales.
  - Slicing and dicing is a feature whereby users can take out (slicing) a specific set of data of the OLAP cube and view (dicing) the slices from different viewpoints.

Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

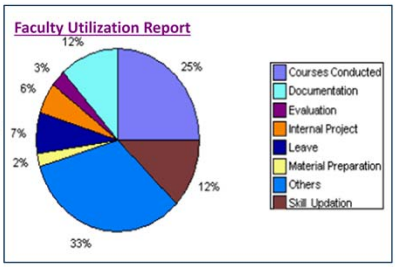
 11

OLAP Testing

- The primary focus of OLAP testing is on displaying the correct information of data warehouse in correct manner to the end user

Raw Data

Emp Cat	Emp Id	Actv	Main Actvt	Sub Actvt	Category
T	3866	269	Email	Email	Others
T	3937	354	Training	Others.	Internal Projec
T	4961	354	Training	Others.	Internal Projec
T	4961	301	Training	lab	Courses Cond
T	4961	344	Miscellaneous	Others	Others
T	5085	331	Evaluation	Others	Evaluation
T	5085	354	Training	Others.	Internal Projec
T	5602	344	Miscellaneous	Others	Others
T	5602	277	Leave	Leave	Leave
T	4022	269	Email	Email	Others
T	4743	332	Evaluation	Test Evaluation	Evaluation

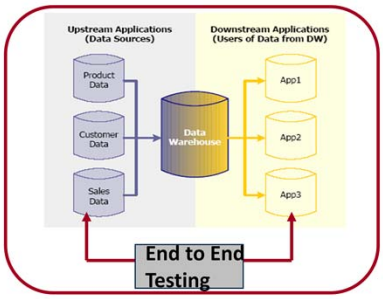


- Below is the list for various validations applicable in OLAP testing:
  - Verify data from data warehouse is mapped correctly to the reports
  - Verify report layout as per design
  - Verify Drill down/up functions
  - Validate computations and aggregations

Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

 12

End to End Testing



- All the stages (i.e., the source, staging, data warehouse and reports) are to be tested for end to end reconciliation of data. E2E testing ensures that data moves through all stages in the expected way, generating the desired output
- This end-to-end validation is essential for detecting inherent defects due to the interdependency of code/data between all the stages

Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

 13

DWH/BI Performance Testing

- Performance testing ensures that loading of the data and subsequent queries on the databases does not kill the system and results are within acceptable performance limits
- As the volume of data in a data warehouse grows, ETL load times can be expected to increase and performance of queries and report generation can become a concern
- Below is the list for various Performance test validations :
  - Verify that ETL processes are completed within the agreed upon window using peak load data
  - Compare ETL process timings; component by component to point out any bottlenecks
  - Verify the response time for data retrieval at different level of aggregations
  - Verify the report generation time is within specified SLAs
  - Verify Refresh time of reports

Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

 14

Quiz

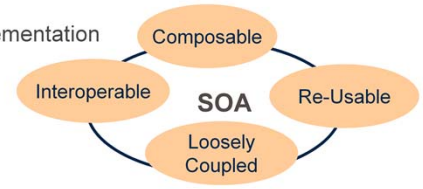
- What is full form of ETL?
- What is full form of OLTP?
- What is full form of OLAP?
- What is use of Staging area?
- Give an example of transformation
- What is involved in ETL testing?
- What are basic OLAP operations?
- Display of the correct information is covered under what type of testing?
- Why is End to end testing required?
- What testing is required when the volume of data in a data warehouse grows?

Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

 15

About SOA

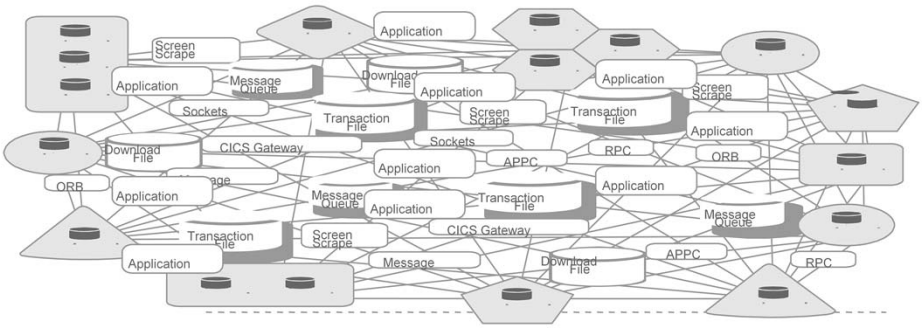
- Service-Oriented Architecture (SOA) is an architectural style
- Applications built using an SOA style deliver functionality as services that can be used or reused when building applications or integrating within the enterprise or trading partners
- SOA in other terms
  - A service-oriented architecture is essentially a collection of services
  - Services are based on heterogeneous technologies
  - Application functions are modularized and presented as services
  - A service is an implementation of a well-defined business functionality
  - Services are loosely coupled
  - Service interface is independent of the implementation



Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

 16

Non SOA based framework



- Tightly integrated interfaces are difficult to change
- The more interfaces the more complex the application: interface logic may exceed business logic
- In such circumstances, re-use becomes difficult and impractical

Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

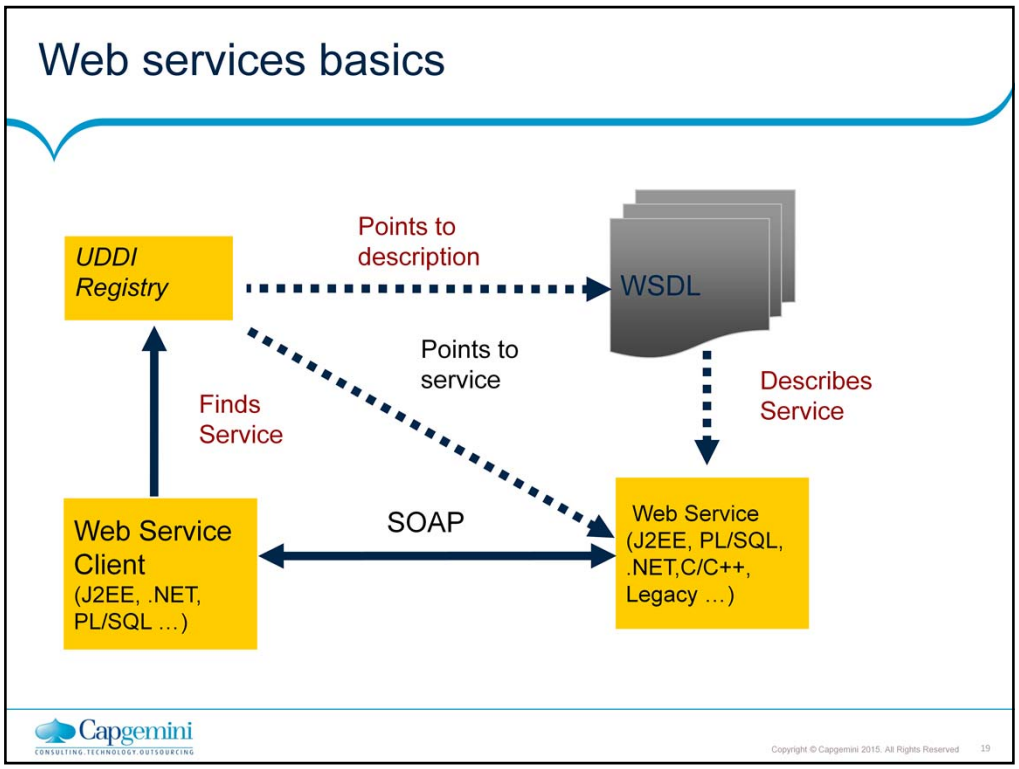
 17

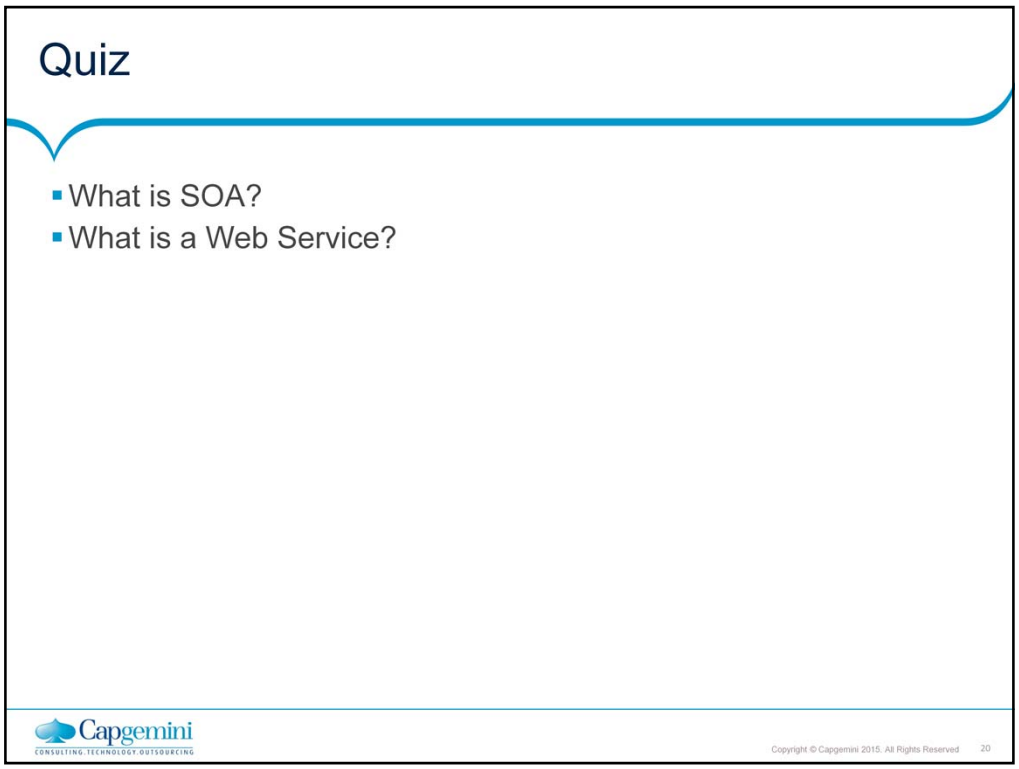
Web services & SOA

- SOA is not Webservices, but web services are the preferred standards-based way to realize SOA
- Web services are software systems designed to support interoperable machine-to-machine interaction over a network
- This interoperability is gained through a set of XML-based open standards, such as WSDL, SOAP, and UDDI
- These standards provide a common approach for defining, publishing, and using web services
- Interoperability is the most important principle of SOA
- This can be realized through the use of web services, as one of the key benefits of web services is interoperability, which allows different distributed web services to run on a variety of software platforms and hardware architectures

Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

 18


Web services basics
UDDI Registry
Points to description
WSDL
Points to service
Finds Service
Describes Service
Web Service Client (J2EE, .NET, PL/SQL …)
SOAP
Web Service (J2EE, PL/SQL, .NET,C/C++, Legacy …)
Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING
Copyright © Capgemini 2015. All Rights Reserved
19


Quiz
What is SOA?
What is a Web Service?
Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING
Copyright © Capgemini 2015. All Rights Reserved
20

Summary

- In this lesson, you have learnt:
  - Why do we need Data Warehouse?
  - Introduction to Data Warehouse Architecture
  - Types of Data Warehouse Testing
  - What is ETL & ETL Testing?
  - OLAP Testing
  - End to End Testing
  - DWH/BI Performance Testing
  - SOA & Web Services
  - Summary

Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

 21