Server Side Web Scripting

* Java
* PHP
* Node.js
* ASP.NET

Sandbox – serve to protect the user from malicious script.

Java SE – client server application

Java ME

Java EE – to develop a server centric which can be accessed through the web

Java Web Application

Netbeans environment

Java Web

Application Server – a web server with a Java Virtual Machine

Apache Tomcat

Glassfish Server

Java EE Version – Java EE 7 web – latest

Frameworks – for web application (netbeans)

* SpringWeb MVC
* Java Server Faces
* Struts 1.3.10
* Hibernate

META-INF

WEB-INF

Source Packages

Libraries

* JDK
* Tomcat
* MySQL JDBC Driver

Logical Structure

War file – web archive, zip with a wire extension

SERVLETS

HTTP Servlets

HTTP Servlet Request

HTTP Servlet Response

Serving Binary Content – ex. images, connect to the database

Servlet – query the image from the database

Servlet – java class

Servlet method – doGet, doPost, doHead, doTrace, doOption etc.

Methods - .getMethod, .getRequestURL(), .getRequestURI()

Java – object oriented

Header - .getHeader(String name), .getHeaderName(), .getDateHeader(String name)

Payload/Body - .getReader(), .getInputStream()

Get Request - .getQueryString(), .getParameter(String name), .getParameterName()

Response - .setStatus(), .setHeader(name, value), .getWriter() , . getOutputStream()

* Handling Request Parameter (GET)
* Handling Request Parameter (POST)
* Request Dispatching – processing a request between you and other components

Code Smells – God class, Long Method

2 Things To do: (good practice)

1. Divide and Concure – “include”
2. Separation of concerns – division of labor –“forward”

* Request Dispatch Inclusion

MVC – model view controller

Model – represent data

View – presentation of data

Controller – trigger

JSP

Jasper – component of Tomcat

* 3 Different Directives – JSP Directives
  + Include directives
  + Tag library directive
* JSP Standard Actions
  + jsp:attribute
  + jsp:include
  + jsp:element
  + jsp:body
  + jsp:useBean
  + jsp:plugin
  + jsp:fallback
  + jsp:forward
  + jsp:param
  + jsp:params
* EL Expressions
  + .paramValues
  + .header
  + .param
  + .headerValues
  + .cookie
  + .applicationscope
  + .requestscope
* JSP Scriplets
  + 3 Type Scriptlets
    - Scriplet Scriplet
    - Scriptlet Expression
    - Scriptlet Declaration
      * Instance method
      * Method
      * You can create helper methods
* JSTL – jsp standard tagline library
  + Namespaces
  + Package

<sql:setDataSource/>

sql:update

sql:param

sql:transaction

sql:dateParam

sql:query

fmt:formatDate

fmt:setBundle

fn:trim

fn:split

fn:substring

fn:length

* Session Handling – stateless communication
* Cookie – extension that is used to identify a particular client
  + Set-cookie
  + Cookie jar
  + Non-persistent cookies – when browser is closed there will be no cookie
  + Persistent cookie – it is still there for a period of time even if the browser is closed
  + Timeout

HTTPS – secure cookie

HTTP – plain text communication

http only cookie – cannot retrieve using scripts such as javascripts (script cannot extract them)

Java – cookie are internally

Request.getSession – return a session

Cookie expired – request.getSession(true) will not return a cookie

Scope object – different scope

Session.setAttribute

Request.getSession(false) – retrieve previous session

Session.getAttribute

Session.invalidate()

JSESSIONID – default cookie

URL rewriting

* Sessions
  + .getAttribute
  + .setAttribute
  + .getLastAccessedTime
  + .setMaxInactiveInterval
* Context Scope
  + .contextInitialized
  + .contextDestroyed
* PHP

Php – similar with JSP

* Very much like C structure
* Similar with javascript functions
* A procedural language

PHP Interpreter

PHP API’s – ex. text processing, credit card processing etc.

Superglobals – available in the global scope (everywhere)

$GLOBALS

$\_SERVER

$\_GET

$\_POST

$\_FILES

$\_COOKIE

$\_SESSION

$\_REQUEST

$\_ENV

* String Function

String processing capabilities

Regular expression

PHPSESSIONID – cookie in PHP

Session\_start(); - find out if there is an incoming cookie value

Heredoc –

PHP – concatenate using dot “.”

* Session Function

session\_abort

session\_commit

session\_destroy

MySQLi – improved extension, procedural syntax, object oriented sysntax

* Javascript - nodeJS platform

MEAN Stack Application

M – mongodb

E – expressJS

A – AngularJS

N – nodeJS

BSON

JSON

* NodeJS – search for the website

Npm- node package manager

File System

OS

Stream

Query String

* There are 3rd party modules in nodeJS

Nodemon – node monitor, detect edits and do live editing

File System – library in nodeJS

NodeJS – is asynchronous, callback action do things in parallel

WriteHead – you can set status code

Query String – module for extracting and return an associate array

* ExpressJS

Express

Express\_session – you can track session and define session variables

Pug – template engine

Pug file – is like a view

nodeJS – is the controller

* Web Application Security

Packet sniffer

Identity theft

Category: OWASP Top Ten Project – Open Web Application Security

Let’s Encrypt – certificate free for one month , to serve HTTPS traffic

CPU Processing power

* Hashed Algorithm
* SHA Algorithm
* Salted Hash
* Password hash()
* Injection
* Sql Injection
* Cross Site Request Forgery (CSRF)
* Cross Site Scripting (XSS)