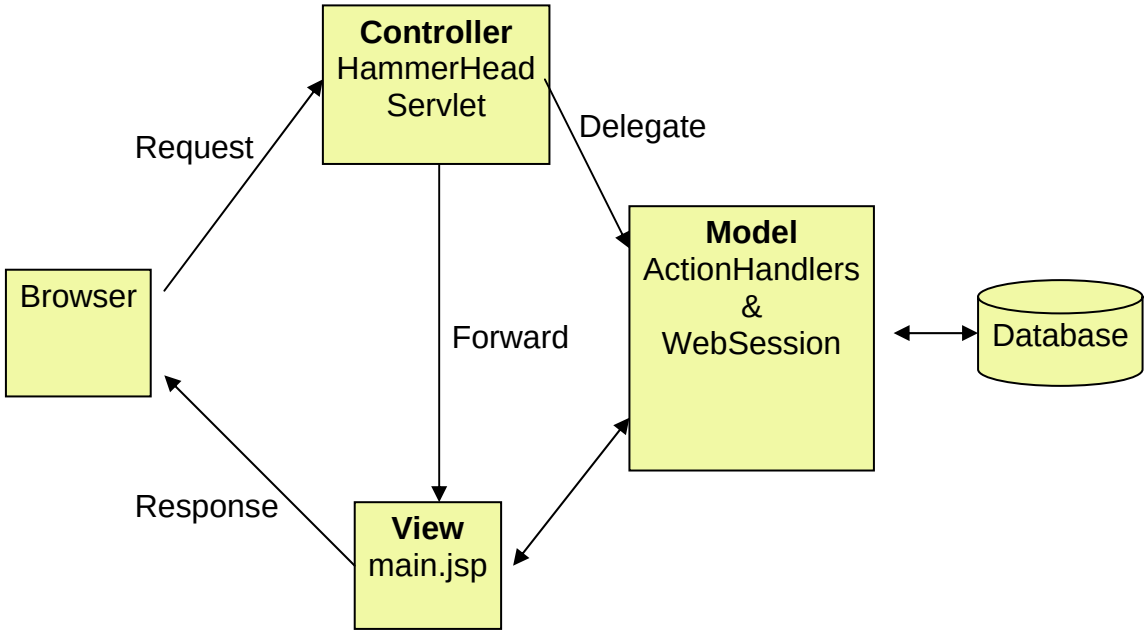
Solving the WebGoat Labs (DRAFT)

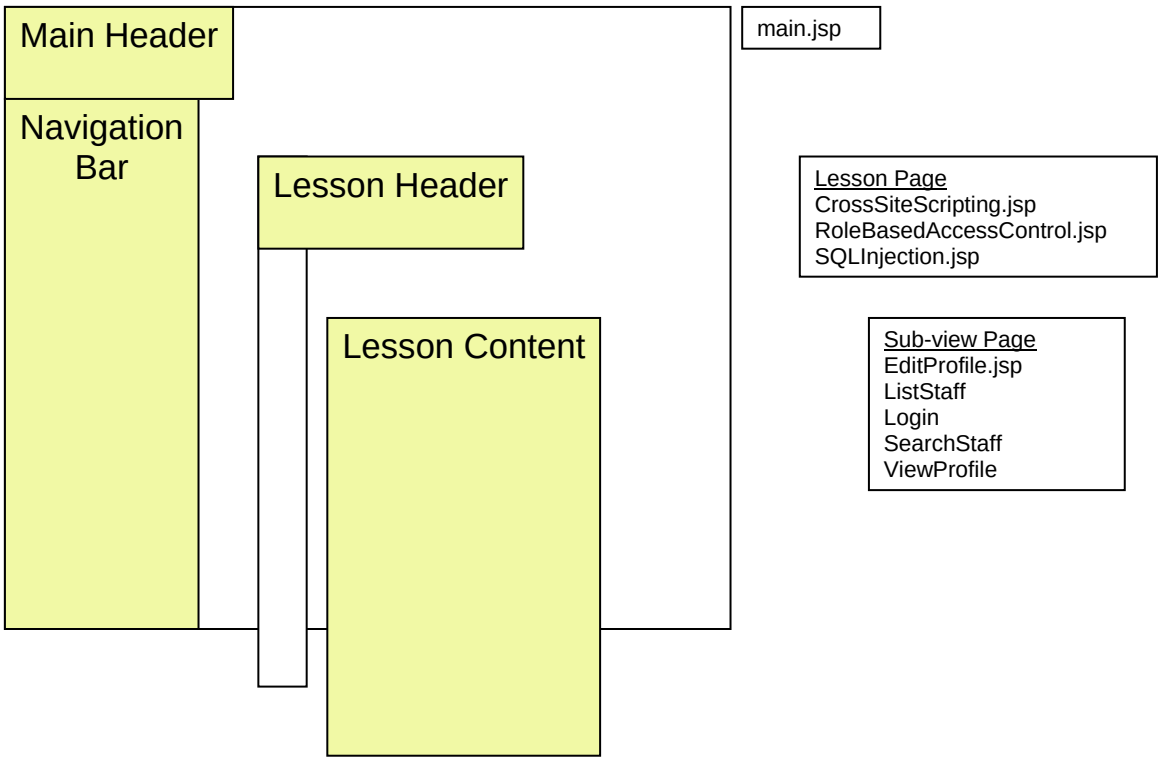
1) Labs are programming exercises
2) All user login passwords are the same as the first name.

Architecture Overview

1) All labs use a custom Action Handler that is invoked from the main WebGoat servlet HammerHead.java

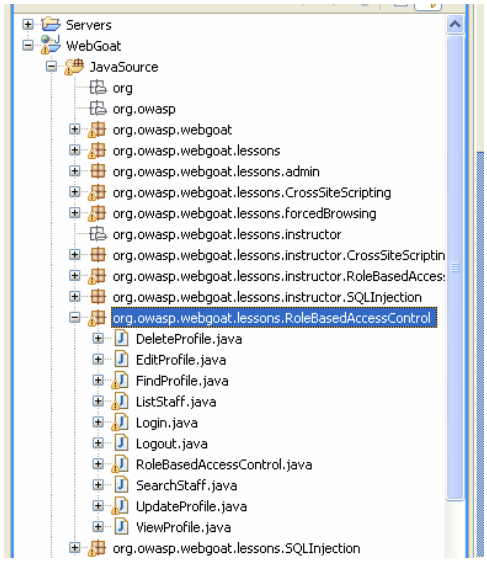


2) The Action Handler (lesson objects) will execute their business logic, load the data into the WebGoat WebSession object, and then turn control over to the view component (JSP)
3) The WebGoat presentation only allows for a lesson to write into the Lesson Content portion of the webpage.



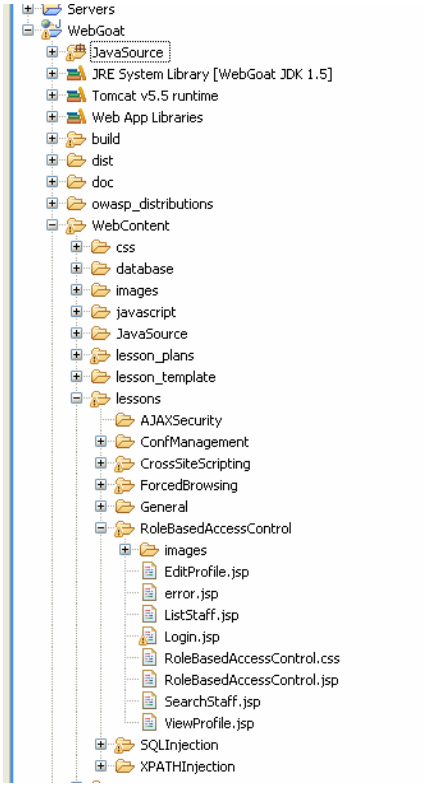
Where to put your code

1) After identifying the ActionHandler for your lesson all the classes involved for that lesson will be in that folder.
    a. For Example: RoleBasedAccessControl java files would be in the org.owasp.webgoat.lessons.instructor.RoleBasedAccessControl folder inside the Eclipse Package Explorer view.



The action handler for RoleBasedAccessControl would be RoleBasedAccessControl.java. This is entry point into WebGoat for this Lab

b. For Example: RoleBasedAccesControl JSPs would be in the WebContent/Lessons/RoleBasedAccessControl folder inside the Eclipse Package Explorer



Except for the CrossSiteScripting lab the JSPs do not require modification

2) All the labs are designed so the Method to be fixed has a _BACKUP method which contains the original source code.
   a. For Example: RoleBasedAccessControl/ListStaff.java has one method where the developer is supposed to make their changes. ListStaff.getAllEmployees(WebSession s, int userID) it also has a corresponding ListStaff.getAllEmployees_BACKUP(…) method
   b. The getAllEmployees method is the method you are supposed to fix in order to solve the lesson.
3) RoleBasedAccessControl

WebGoat Access Control Policy

- Overall Policy

Roles \ Assets	Search	List Staff	View Profile	Edit Profile	Create / Delete Profile
Employee	X	X (Self Only)	X	X (Portions)	
Manager	X	X	X		
HR	X	X	X	X (Others Only)	X
Admin	X	X	X	X	X

- Data Access Policy
  - Employees can see their data
  - Employees can edit portions of their data
  - Managers can see their data and their employees' data
  - HR can see and edit all employees. HR cannot edit their data

WebGoat Lab Database Schema

- Employee
  - userid INT NOT NULL PRIMARY KEY
  - first_name VARCHAR(20)
  - last_name VARCHAR(20)
  - ssn VARCHAR(12)
  - password VARCHAR(10)
  - title VARCHAR(20)
  - phone VARCHAR(13)
  - address1 VARCHAR(80)
  - address2 VARCHAR(80)
  - manager INT
  - start_date CHAR(8)
  - salary INT
  - ccn VARCHAR(30)
  - ccn_limit INT
  - disciplined_date CHAR(8)
  - disciplined_notes VARCHAR(60
  - personal_description VARCHAR(60)
- Roles
  - userid INT NOT NULL
  - role VARCHAR(10) NOT NULL
  - PRIMARY KEY (userid, role)
- Ownership
  - employer_id INT NOT NULL
  - employee_id INT NOT NULL
  - PRIMARY KEY (employee_id, employer_id)

WebGoat Lab Organization Chart