OWASP – Worked on vulnerabilities

1.Cross-Site Scripting (XSS)

1.Created the Framework which blacklist xss character from input based on configuration(Application level -àSite level àParameter level)

2.Broken Authentication and Session Management

1.Authorization happened after the request was processed, fix the design

2.Fix the server configuration to ensure session are not accessible through java script

3.Un-validated Redirects and Forwards

1.Used was able to perform the operation after the logout, fix the vulnerability

4.Web Parameter Tampering

1.Fixing the issue case by case bases

OWASP -Attack

1.Denial of Service

2.CSRF

1.Enhance the framework to prevent CSRF attack

3.Account lockout attack

1.In an account lockout attack, an attacker attempts to lock out user accounts by purposely failing the authentication process as many times as needed to trigger the account lockout functionality

2.Exploit Broken “Authentication vulnerabilities “

3.Solution: Do not show the login id to user instead show the generic error message(not the use case specific message)

http://www.excelsior-usa.com/blog/java/cert-secure-coding-standard-for-java-theory-and-practice/

http://www.architectingsecurity.com/2011/03/14/secure-coding-guidelines-for-java/

https://www.securecoding.cert.org/confluence/display/java/The+CERT+Oracle+Secure+Coding+Standard+for+Java

http://www.atsec.com/downloads/pdf/secure-coding-guidelines.pdf