**Project Name:** Navisys-FrontOffice (Policy Administration System)

**Technical Stack & Implementation Details :**

**Technologies Used in Project:**

1. **OWASP ESAPI Framework:**

**Obective:** Used to Prevent our application from Security Vulnerabilities.

**Implementation:** OWASP ESAPI SecurityFilter Servlet which prevents application from the vulnerabilities such as SQL Injection, OS Command Injection, CLRF, XSS Cross Site Scripting etc.,

1. **SSL (https) –** Precautions taken at application level & at other downstream applications when implementing Secure Socket Layer at Load Balancer Proxy settings.
2. **ASynchronous Logging :** Implemented this strategy to reduce the performance hit during the application runtime using Logback & sl4j logging framework.
3. **Veracode & green Light Plugin:** Used for application scanning for Security Vulnerabilities. We have handled both Sandbox Scanning & also Policy Scanning to get green signal for application to deployment stage. Veracode Green Light is an IDE (eclipse) plugin to identify Security Vulnerabilities at development level itself.
4. **Splunk :** Used for **Log Analytics** over our application log archives to identify ORA errors, Java Exceptions, Memory Overflow etc, during runtime. This has been implemented at all of our environments such as DEV, QA, STAGE & PROD. Splunk DashBoard Configuration is done to monitor the logs in graphical representations such as bar chart, pie chart etc. We have used it for database query using |dbxquery search.
5. **AppDynamics & XRebel :** This is an Application Performance Monitoring Tool used to identify our application performance & memory leak during runtime. AppDynamics APM agent is configured at Server & Integration environments such as DEV, QA, STG, Performance & PROD environments. XRebel is another APM tool we have used to identify application call trace & performance at developer level itself before rolling out to integration environments.
6. **Selenium Framework:** We have used Selenium WebDriver automation to reduce QA time & COST.
7. **Katalon Studio :** This is another Testing Automation Tool we have used at developer level to identify the Test Case Failures during development time itself before delivering it to integration.
8. **Java VisualVM :** It is a built-in tool of Oracle jdk, we have used to find Java Memory Leaks during runtime and to take heap dump.
9. **AngularJS, Bootstrap4 CSS3 –** Are used in our automation application called BCMS (Batch Cycle Made Simple) for UI design and architecture.
10. **SpringBoot –** Is used for background web service development of above said BCMS application.
11. **GitHub –** Source Code Versioning & Management. We have migrated from PVCS to GitHub.
12. **Jenkins –** Worked on implementing CI/CD pipe-line set up as well. Integrating **SonarQube/Scanner, Veracode Scanner** into Jenkin pipe-line.
13. **Dactical :** Tool used for DBCR (Database Change Request ) automation in GitHub-Jenkin CI/CD pipe-line