Usability Test of MagpieBridge Web Extension with FlowDroidLSP Integration.

Introduction:

In this user study, I want to compare two tools integrated in Eclipse IDE. Both of this tool performs taint analysis on a Java program and in presence of an error provides error information. One of the tools provides error information as an error message with source and sink information. The other tool with the similar error message also provides the option to view data-flow path visualization of the flow from source to sink. I want to compare the usability of both this tool with a usability test.

Taint Analysis:

Taint analysis is a technique that is mostly used to detect security vulnerabilities. It tracks untrusted input and sensitive data collected from a user or some untrusted source. If it finds out this data is used in any operation without any kind of security checks then it reports that the data is tainted. For ensuring the security of a system we must ensure that the data is secure to perform any kind of operations like saving into the database, sending data to another source etc. So, we check the data with different validation methods to make sure the data is secure. Taint analysis can detect various kinds of security vulnerabilities like SQL injection where data may be tainted with some vulnerable query string and if executed by database program the security of the system may be compromised, Cross-site-scripting where the data is tainted with some scripts so if the data is used in an environment where a script can be run then it creates security vulnerability, etc.

When performing the taint analysis, because of the limitation of static analysis many times the analysis gives errors that are not actually error which is called false-positive error. To identify this false positive error the programmer generally checks the code from source to sink for taint analysis error.

Task Overview:

Here, each participant will get two tasks, each task has two taint analysis error the participant must find whether any of this taint analysis error is false positive or not. The participant must solve this task using the two tools mentioned above. The participants will use two tools for two

tasks, one tool for each of the task. The tasks will be performed in eclipse IDE and the tools are plugins of Eclipse.

The user will be given a demo task before the user study to get familiarize with the tools and data-flow visualization.