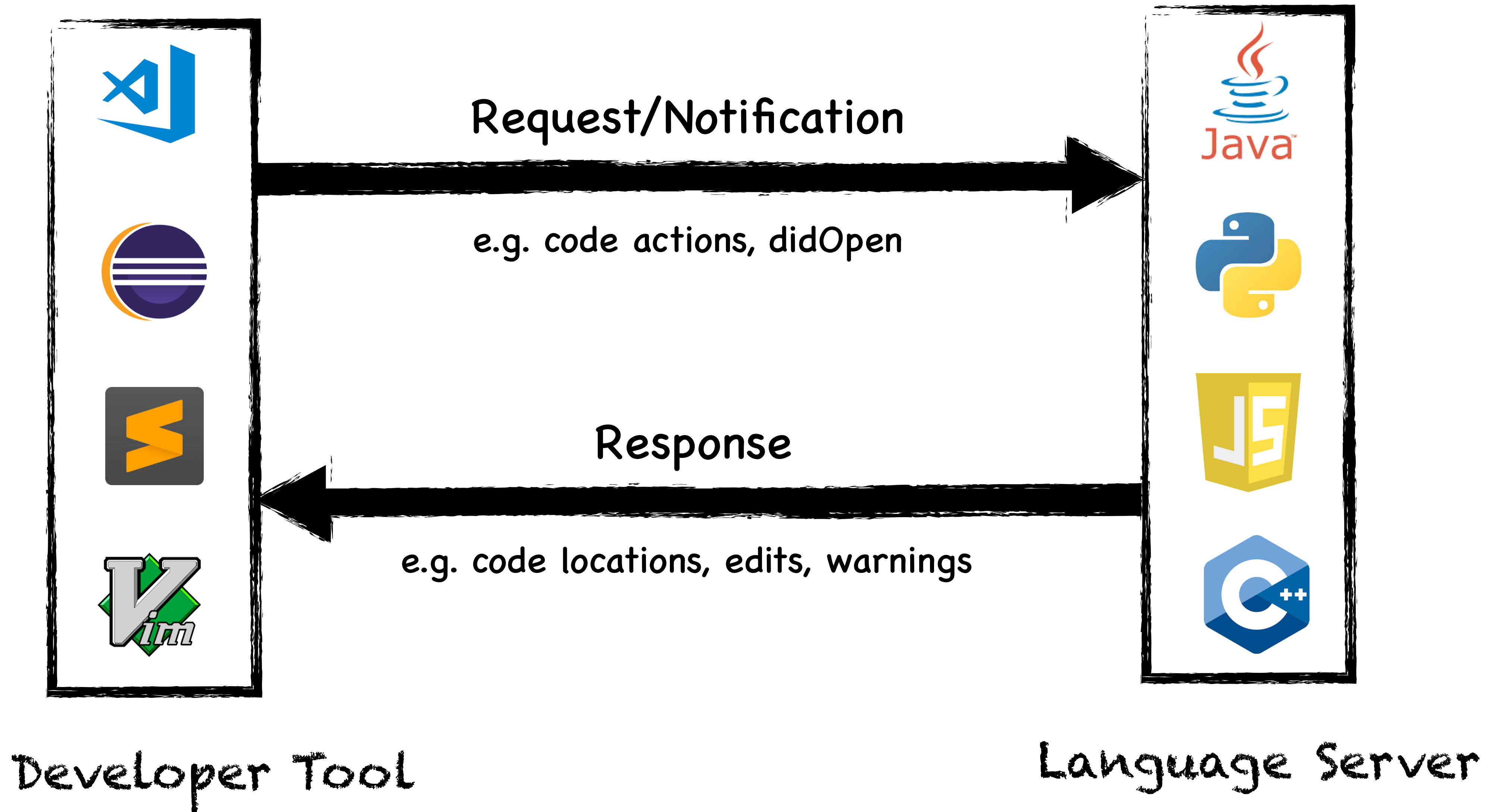


DRY and Use
For IDE Integration



Linghui Luo, Paderborn University

Language Server Protocol (LSP)

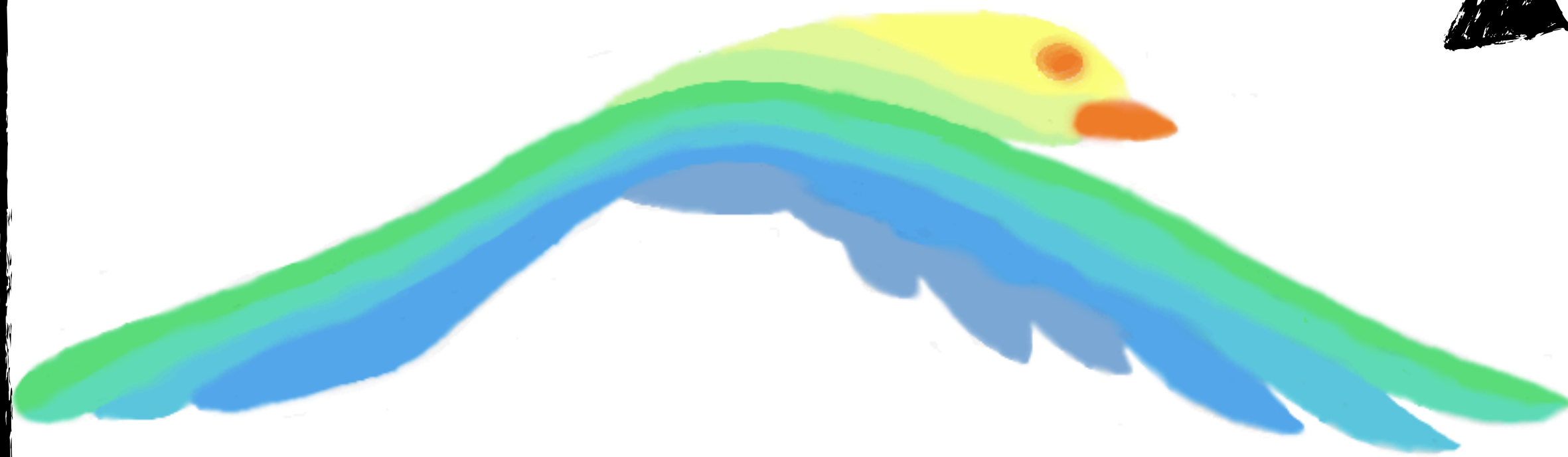
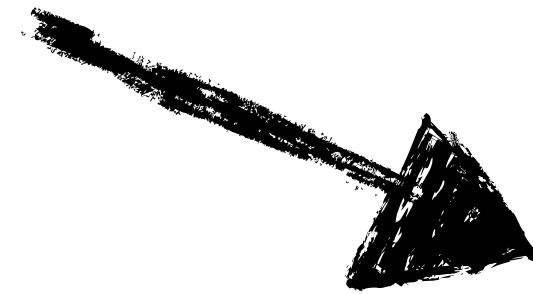


A Reusable IDE Integration Framework

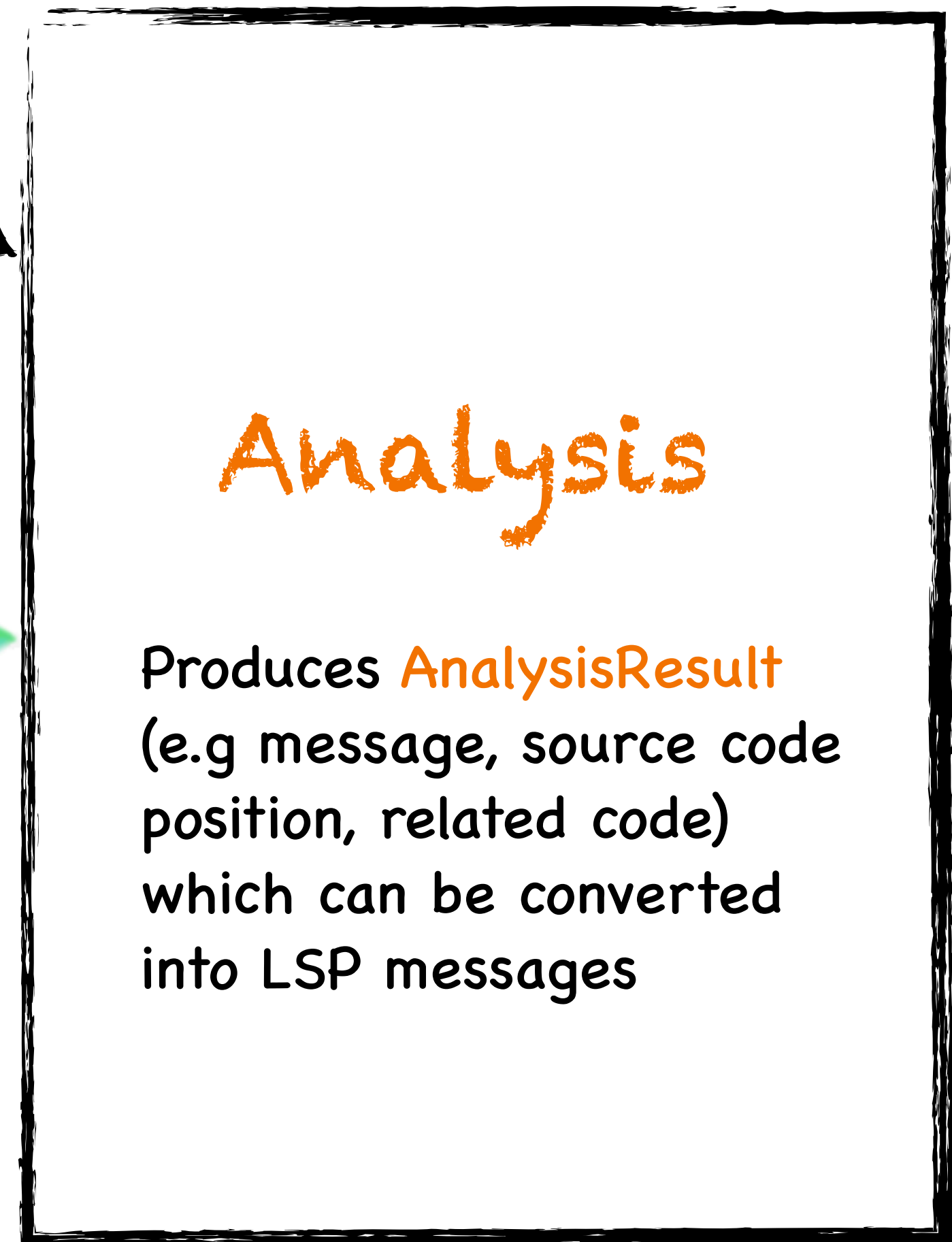


Developer Tool

addAnalysis(**Analysis**, language)



MagpieBridge



Analysis

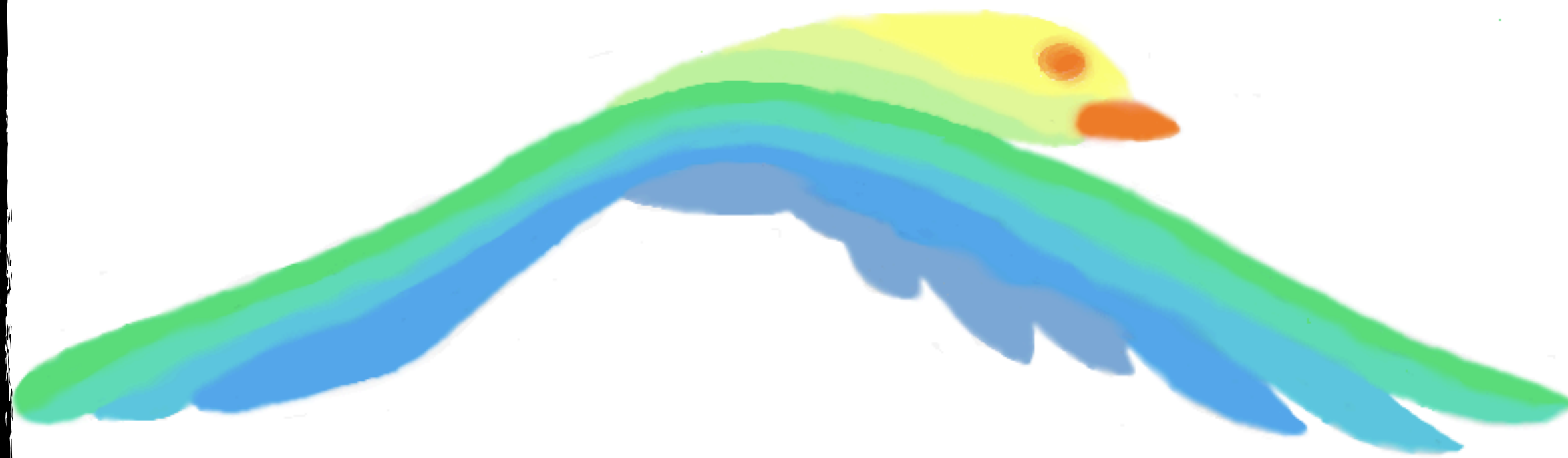
Produces **AnalysisResult**
(e.g message, source code
position, related code)
which can be converted
into LSP messages

MagpieServer

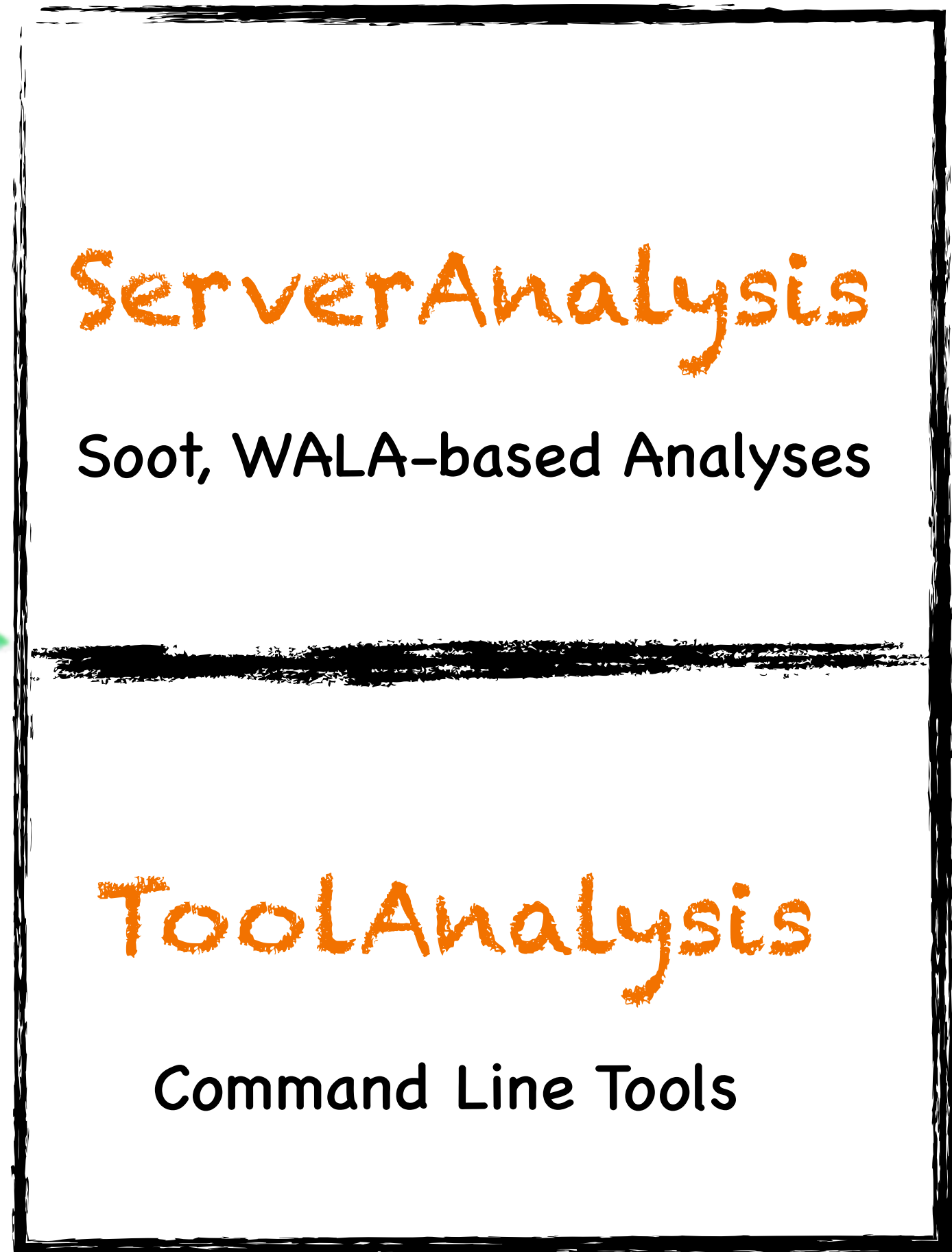
A Reusable IDE Integration Framework



Developer Tool



MagpieBridge



MagpieServer

ServerAnalysis - CogniCrypt

E:\COOP\DemoProjectMagpieBridge\src\RSA2.java (DemoProjectMagpieBridge) - Sublime Text (UNREGISTERED)

File Edit Selection Find View Goto Tools Project Preferences Help

```
8  import java.security.SignatureException;
9
10 public class RSA2 {
11     private PublicKey publicKey;
12     private PrivateKey privateKey;
13
14     public RSA2() throws NoSuchAlgorithmException {
15         KeyPairGenerator kpgen = KeyPairGenerator.getInstance("RSA");
16         kpgen.initialize(512);
17         KeyPair keyPair = kpgen.generate
18             this.privateKey = keyPair.getPrivate();
19             this.publicKey = keyPair.getPublic();
20     }
21
22     public byte[] sign(String message) throws InvalidKeyException, NoSuchAlgorithmException, SignatureException {
23         Signature instance = Signature.getInstance("SHA256withRSA");
24         byte[] bytes = message.getBytes();
25         instance.update(bytes);
26         instance.sign();
27         return bytes;
28     }
29
30     public boolean verify(String message, byte[] signature)
31         throws NoSuchAlgorithmException, InvalidKeyException, SignatureException {
32         Signature instance = Signature.getInstance("SHA256withRSA");
33         instance.initVerify(publicKey);
34         instance.update(message.getBytes());
35         boolean isVerfied = instance.verify(signature);
36         return isVerfied;
37     }
38 }
39 }
40
```

Bildschri... 100% Ansichten

src\RSA2.java:

25:5	CogniCrypt	error	Unexpected call to method update on object of type java.security.Signature. Expect a call to one of the following methods initSign,initVerify
16:5	CogniCrypt	error	First parameter (with value 512) should be any of {2048, 4096}
33:5	CogniCrypt	error	First parameter was not properly generated as generated Pubkey

cognicrypt, Line 16, Column 22 Spaces: 2 Java

Zur Suche Text hier eingeben

DEU 09:31 18.07.2019

ServerAnalysis - FlowDroid

The screenshot displays the Visual Studio Code interface with the following components:

- Explorer:** Shows the project structure for 'DEMOPROJECTFD', including folders like '.idea', '.settings', 'src', 'main', 'java', 'demo', 'webapp', and 'target'. The file 'Database.java' is selected.
- Editor:** Displays the code for 'Database.java' with the following content:

```
43 public static void deleteUser(String username) {  
44     try {  
45         Statement stmt = getInstance().conn.createStatement();  
46         StringBuilder str = new StringBuilder();  
47         str.append("DELETE FROM USER WHERE USER.NAME = '");  
48         str.append(username);  
49         str.append("'");  
50         String query = str.toString();  
51         stmt.execute(query);  
52     } catch (SQLException e) {  
53         e.printStackTrace();  
54     }  
55 }  
56  
57 }  
58
```
- Problems Panel:** Shows two FlowDroid analysis results:
 - Found a sensitive flow to sink [stmt.execute(query);] from the source [req.getParameter("userName");] at line 109 in DemoServlet.java FlowDroid(req.getParameter("userN
 - Found a sensitive flow to sink [stmt.executeUpdate(query);] from the source [req.getParameter("userName");] at line 68 in DemoServlet.java FlowDroid(req.getParameter(
- Terminal/Output:** The bottom panel is currently empty.
- Status Bar:** Shows 'Ln 52, Col 31 Spaces: 2 UTF-8 CRLF Java'.

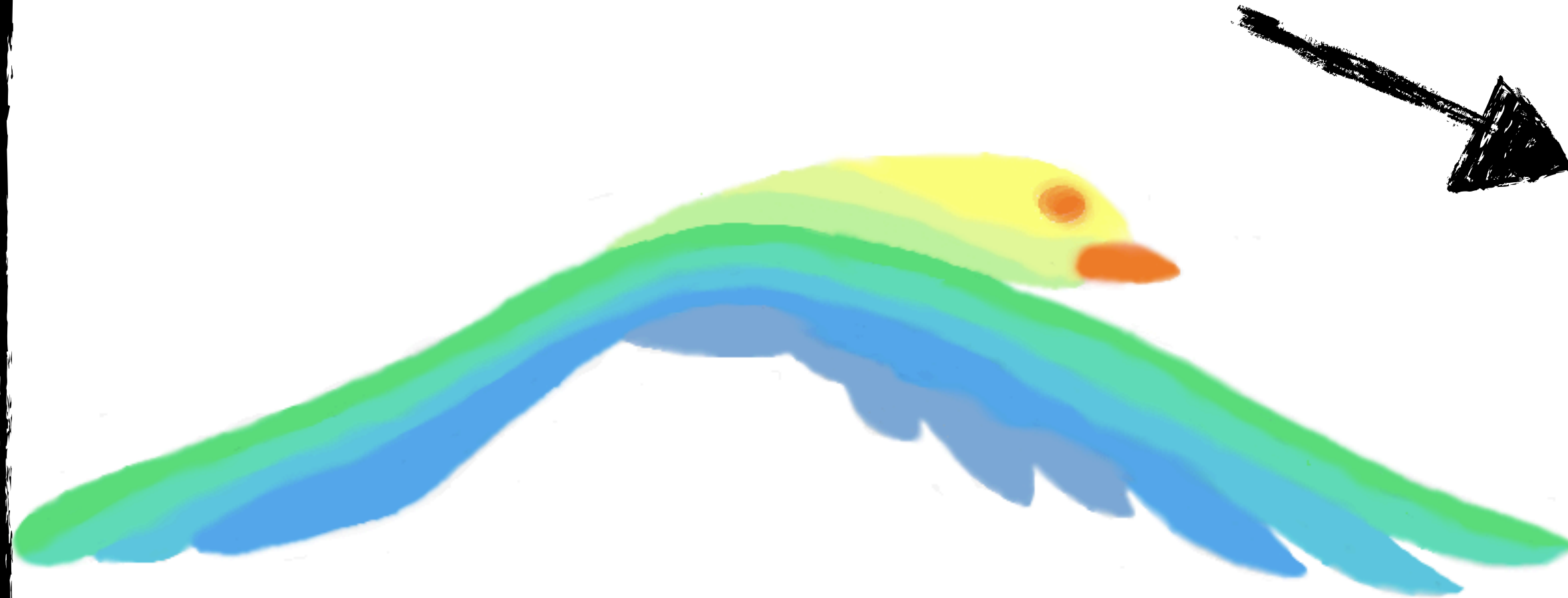
ToolAnalysis - Facebook Infer

The image shows a screenshot of a web-based IDE (Gitpod) running on Chrome. The IDE interface includes a menu bar (File, Edit, Selection, View, Go, Debug, Terminal, Help), an Explorer sidebar on the left showing a project structure for 'MAGPIEBRIDGE' with folders like 'core' and 'analysis', and a main editor window displaying Java code in 'MagpieHttpHandler.java'. The code is partially visible, showing a method that processes request parameters and generates an HTML response. A yellow lightbulb icon indicates an Infer warning at line 59. Below the code, a 'Problems' panel lists several warnings:

- JavaProjectService.java: src/main/java/magpiebridge/projectservice/java 1
- NULL_DEREFERENCE: object `JavaProjectService.projectType` last assigned on line 174 could be null and is dereferenced at line 176. infer [176, 5]
- SourceCodePositionFinder.java: src/main/java/magpiebridge/util 1
- RESOURCE_LEAK: resource of type `java.io.FileReader` acquired by call to `new()` at line 34 is not released after line 59. **Note**: potential exception at line 37 infer [59, ...]
- MagpieHttpHandler.java: src/main/java/magpiebridge/core/analysis/configuration 2
- RESOURCE_LEAK: resource of type `java.io.InputStreamReader` acquired by call to `new()` at line 57 is not released after line 58. infer [58, 71]

Reusable Project Services

addProjectService(language, **IService**)



MagpieBridge

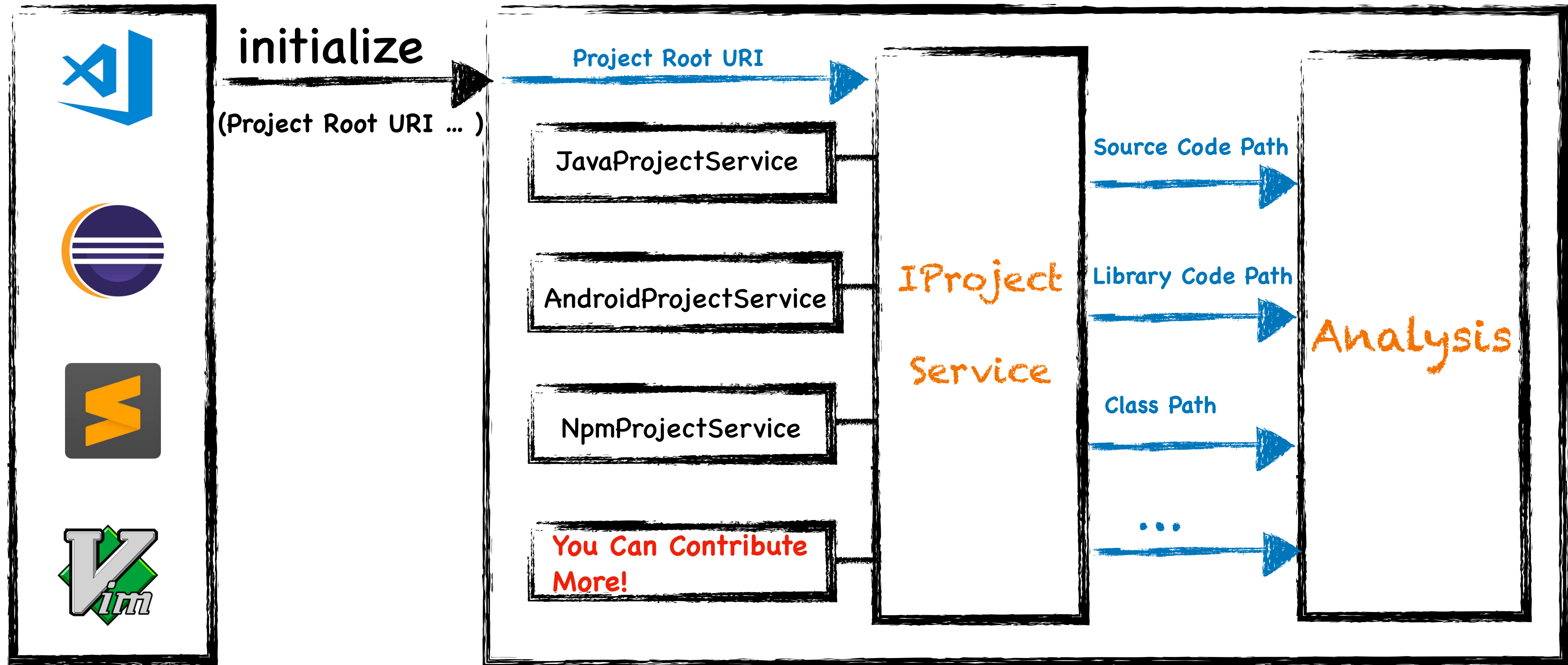
IService
Service

Resolves project scope by leveraging popular build tools (e.g. Maven, Gradle, NPM)

Developer Tool

MagpieServer

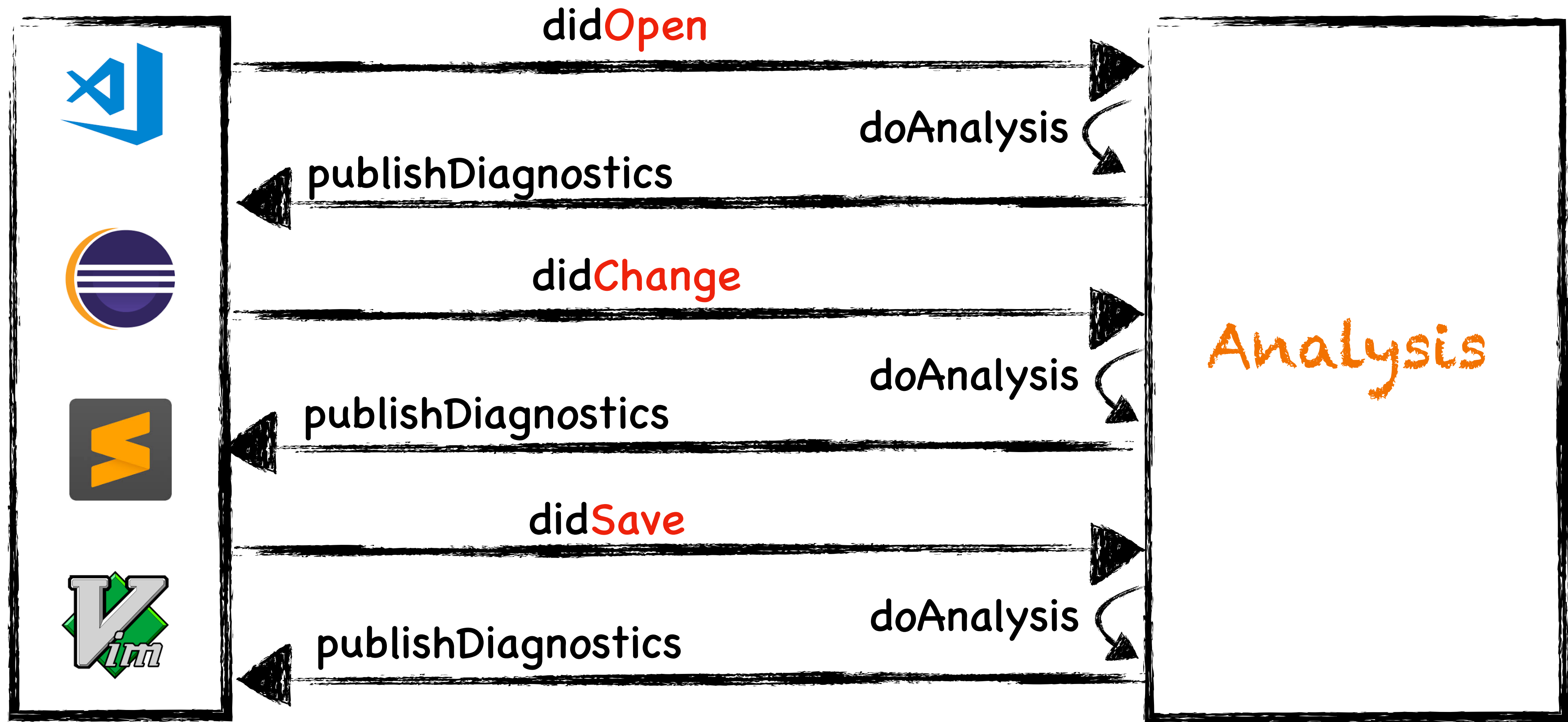
Reusable Project Services



Developer Tool

MagpieServer

Instant Detection



Developer Tool

MagpieServer

IDE Features for Diagnostics

Markers with different severities

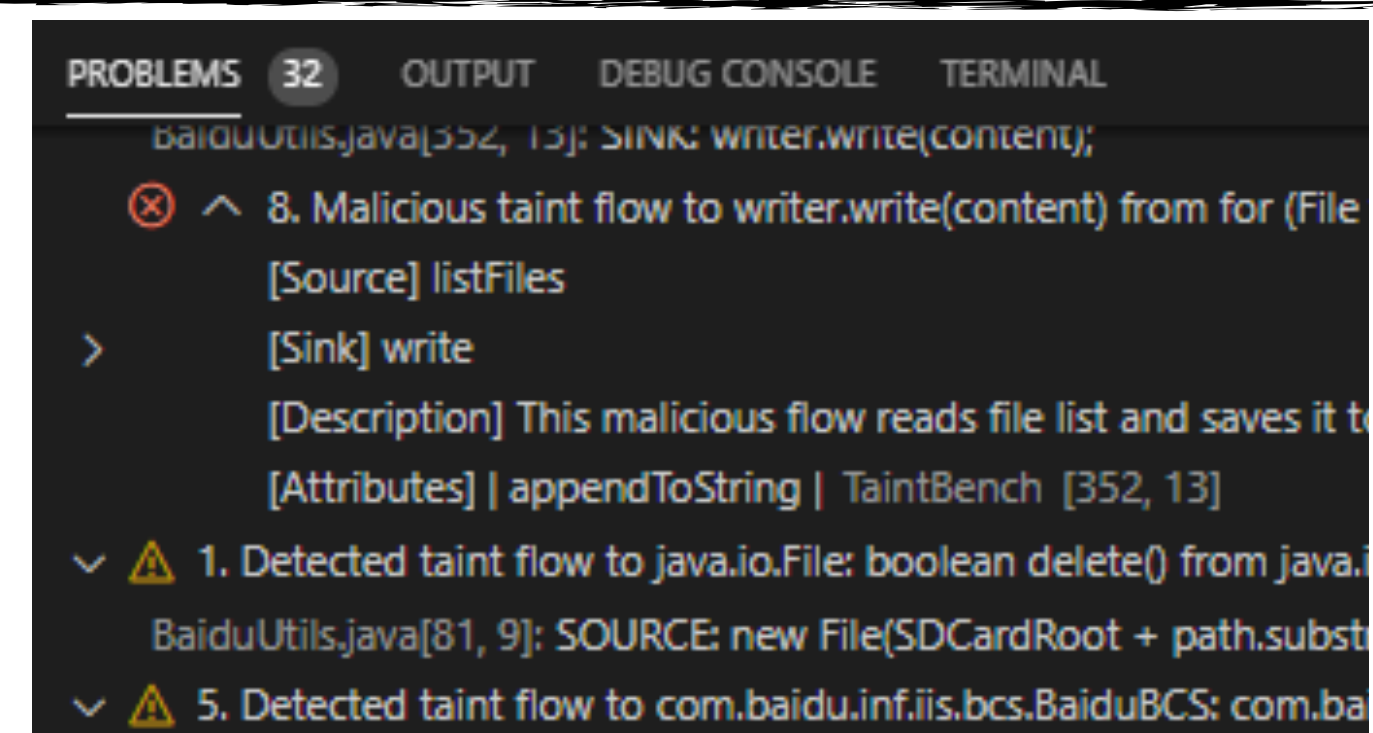
(**ERROR**, **WARNING**, **INFO**)

Related code in hover message

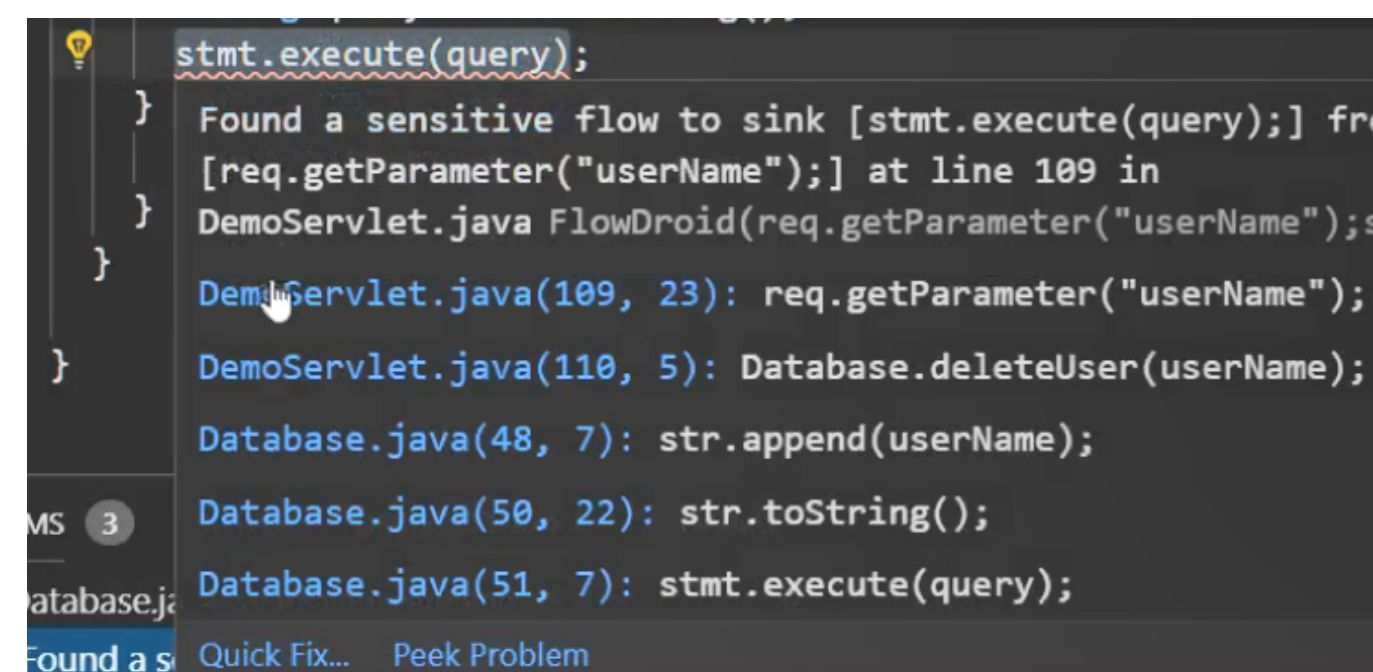
(Witness path)

Advanced features

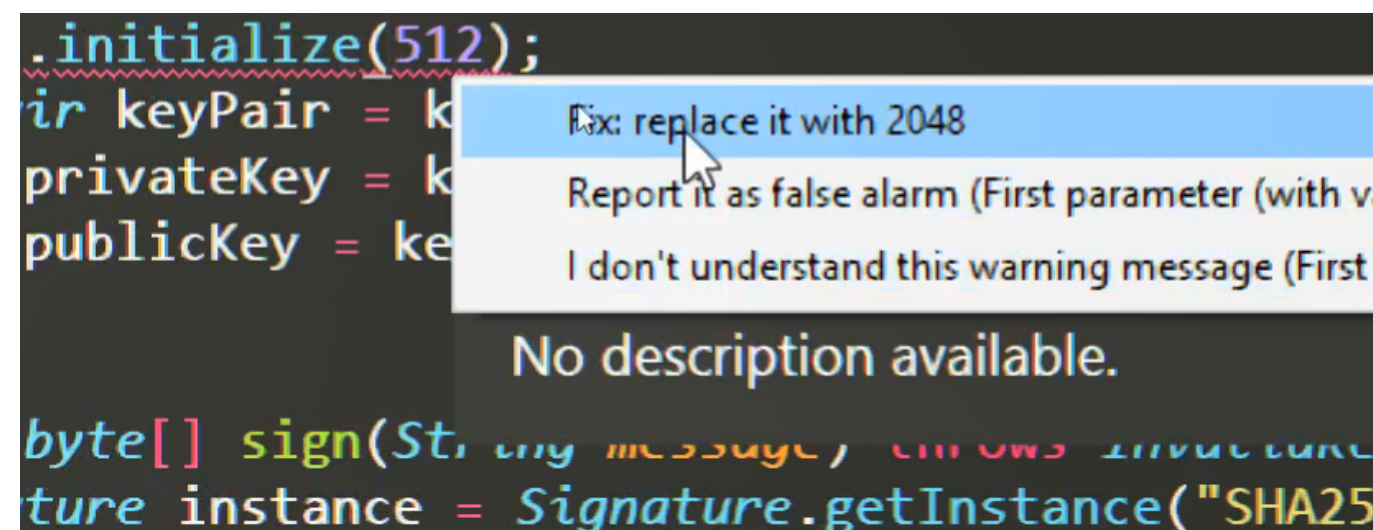
(Quick fixes, Open URI, False alarm reporting ...)



```
PROBLEMS 32 OUTPUT DEBUG CONSOLE TERMINAL
BaiduUtils.java[352, 13]: SINK: writer.write(content);
8. Malicious taint flow to writer.write(content) from for (File
[Source] listFiles
[Sink] write
[Description] This malicious flow reads file list and saves it to
[Attributes] | appendString | TaintBench [352, 13]
1. Detected taint flow to java.io.File: boolean delete() from java.io
BaiduUtils.java[81, 9]: SOURCE: new File(SDCardRoot + path.subst
5. Detected taint flow to com.baidu.inf.iis.bcs.BaiduBCS: com.ba
```

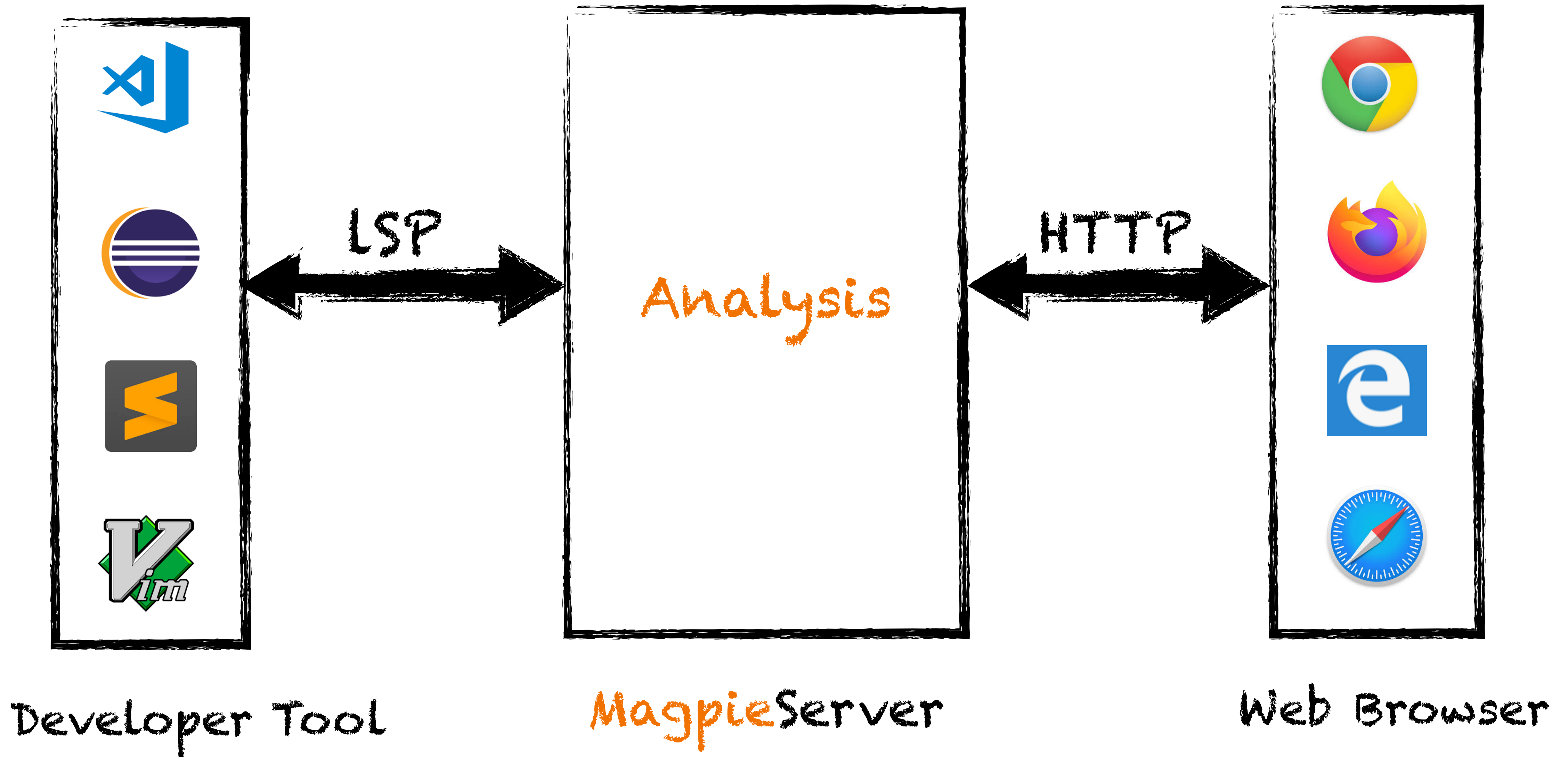


```
stmt.execute(query);
} Found a sensitive flow to sink [stmt.execute(query);] from
[req.getParameter("userName");] at line 109 in
} DemoServlet.java FlowDroid(req.getParameter("userName");)
} DemoServlet.java(109, 23): req.getParameter("userName");
} DemoServlet.java(110, 5): Database.deleteUser(userName);
Database.java(48, 7): str.append(userName);
Database.java(50, 22): str.toString();
Database.java(51, 7): stmt.execute(query);
Found a s Quick Fix... Peek Problem
```

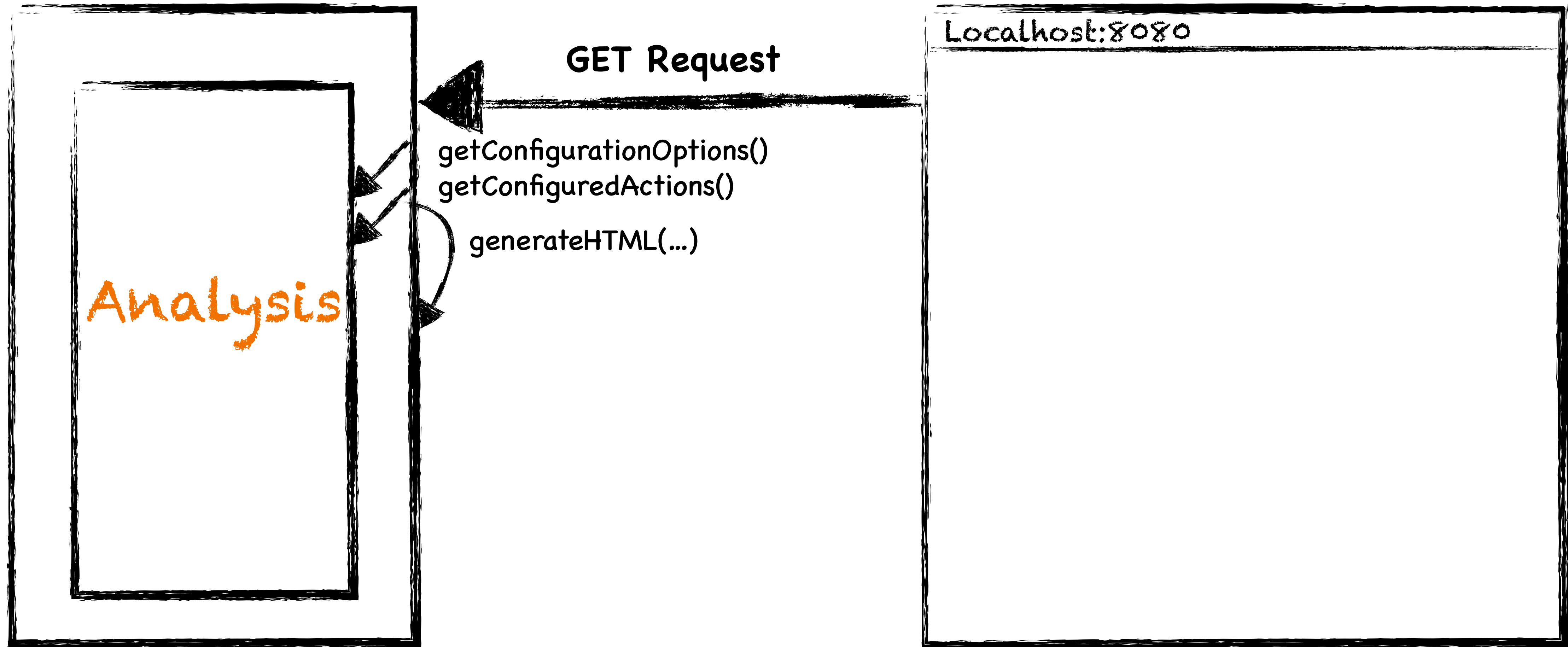


```
.initialize(512);
private keyPair = k
privateKey = k
publicKey = ke
Fix: replace it with 2048
Report it as false alarm (First parameter (with va
I don't understand this warning message (First
No description available.
byte[] sign(String message, throws Structure
ture instance = Signature.getInstance("SHA25
```

MagpieBridge Provides More User Control



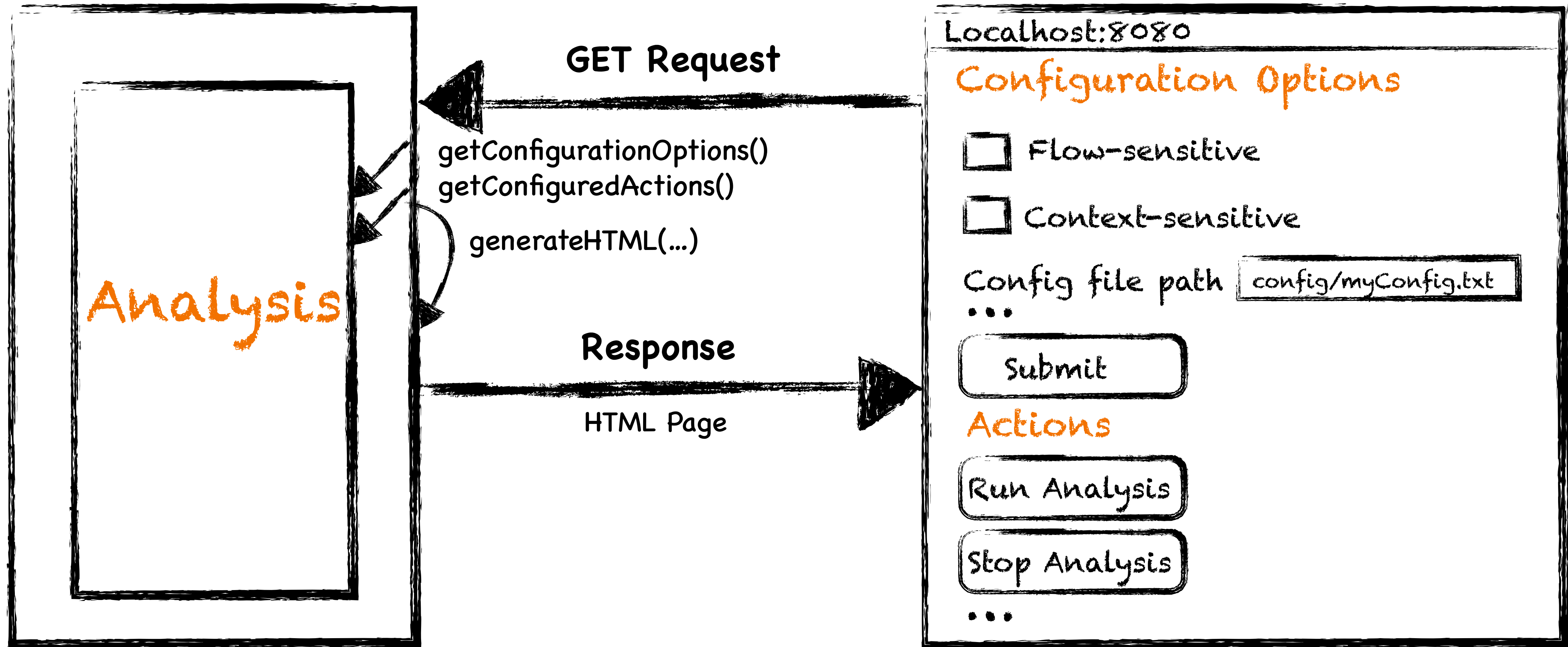
MagpieBridge Provides More User Control



MagpieServer

Web Browser

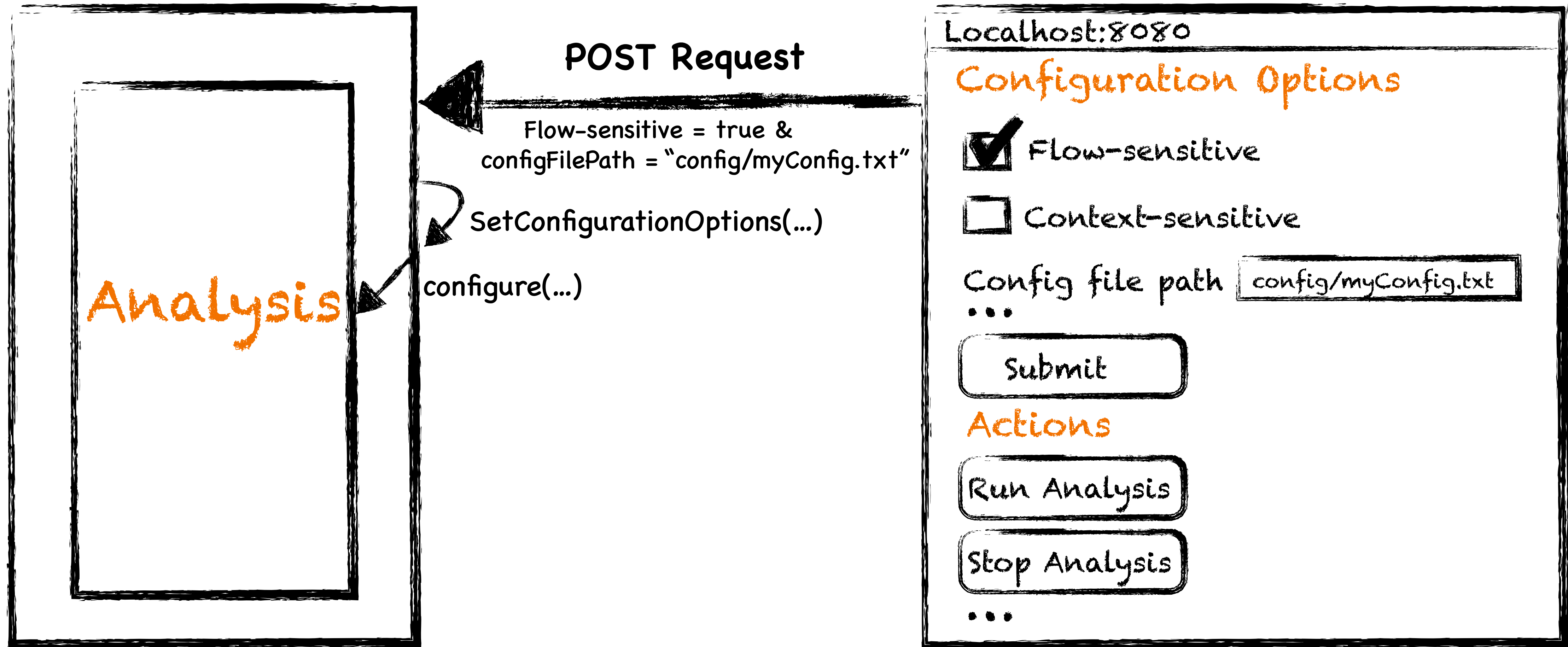
MagpieBridge Provides More User Control



MagpieServer

Web Browser

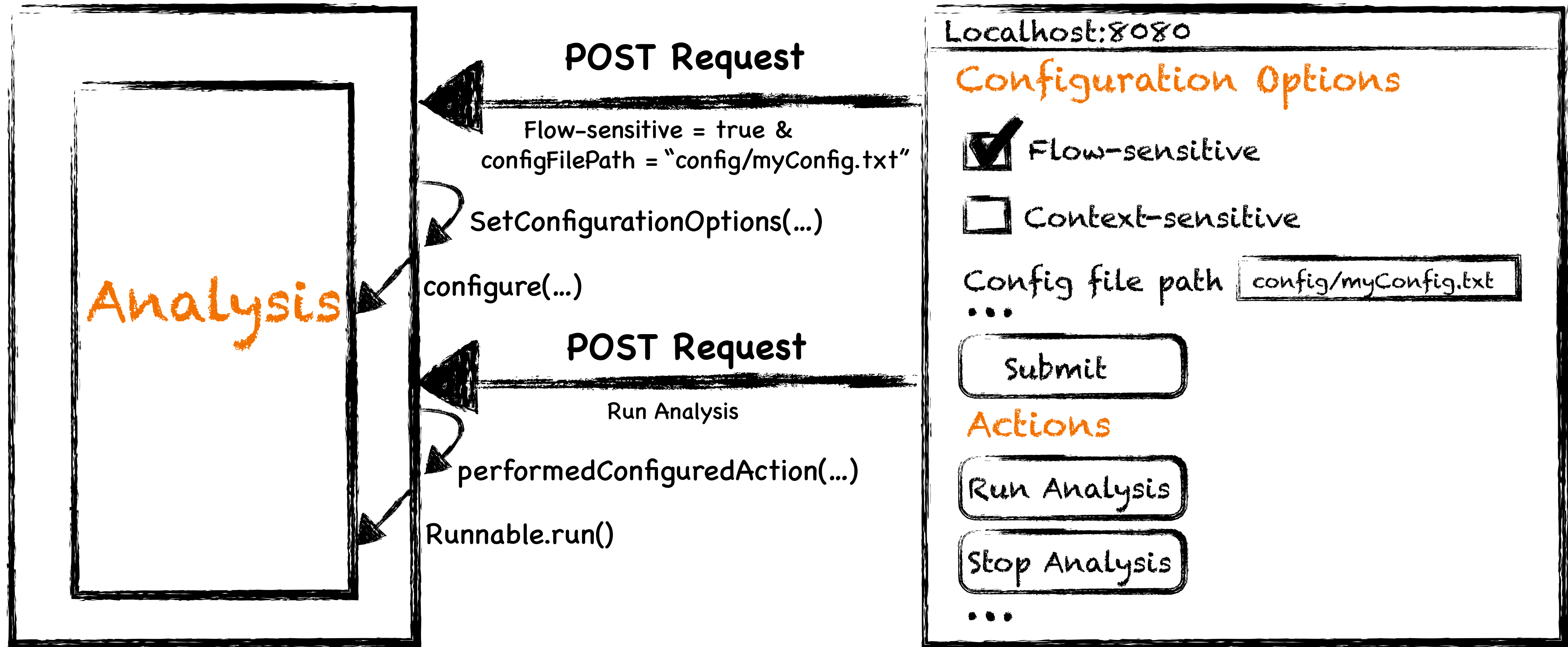
MagpieBridge Provides More User Control



MagpieServer

Web Browser

MagpieBridge Provides More User Control



MagpieServer

Web Browser

Interested? Visit

<https://github.com/MagpieBridge>

to find Tutorials and Examples