HEINZ NIXDORF INSTITUT
UNIVERSITÄT PADERBORN

Integration of Multiple Static Analysis Tools in a Single Interface

- G. S. Varma

- Supervisors:
- Prof. Dr. Eric Bodden
- Dr.-Ing. Ben Hermann

Problem Statement

- How to integrate the results of multiple static analysis tools

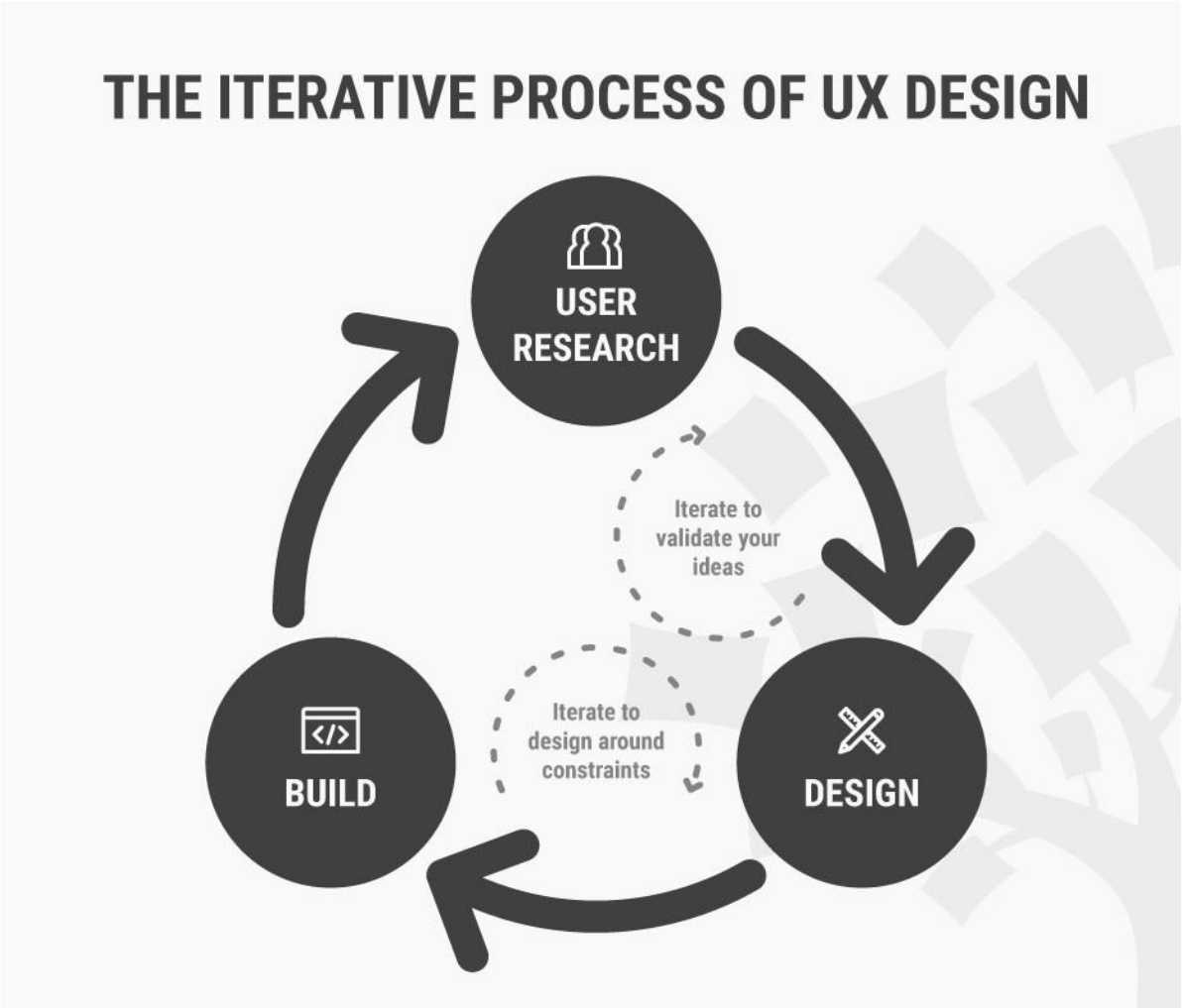
  in a unified user interface?

  - 3 Research Questions

Research Questions

- RQ 1: How to display results of the same codebase from different analysis tools?
- RQ 2: What feedback works to know that bug fixing is on-going?
- RQ 3: How to carry traceability of bug fixing?

Research Methodology



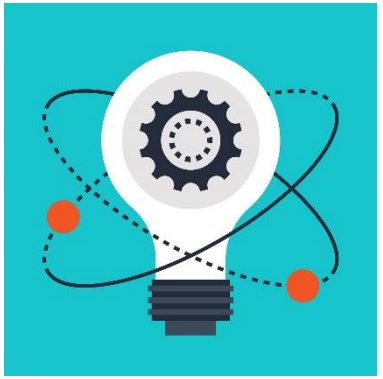
- How to Change Your Career from Graphic Design to UX Design. url: https://www.interaction-design.org/literature/article/how-to-change-your-career-fromgraphic-design-to-ux-design.

Our Approaches

- Software Engineering disciplines:
  - Complex datasets
  - Compiler reporting
  - Continuous integration
  - Refactoring tools
  - Issue tracker
  - Stack Overflow
  - Gamification
  - Usability Engineering

Evaluation

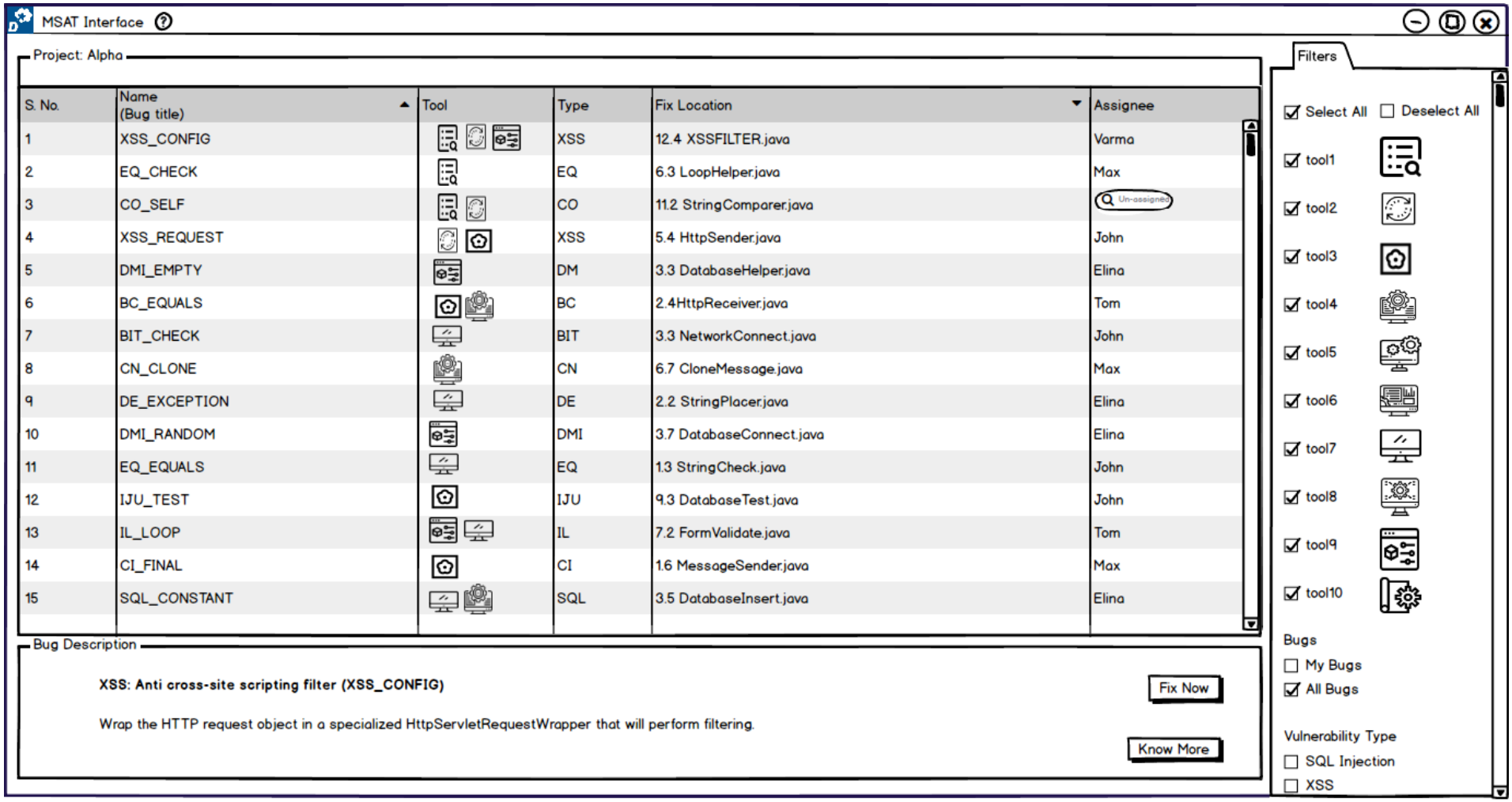
- Experimental Design



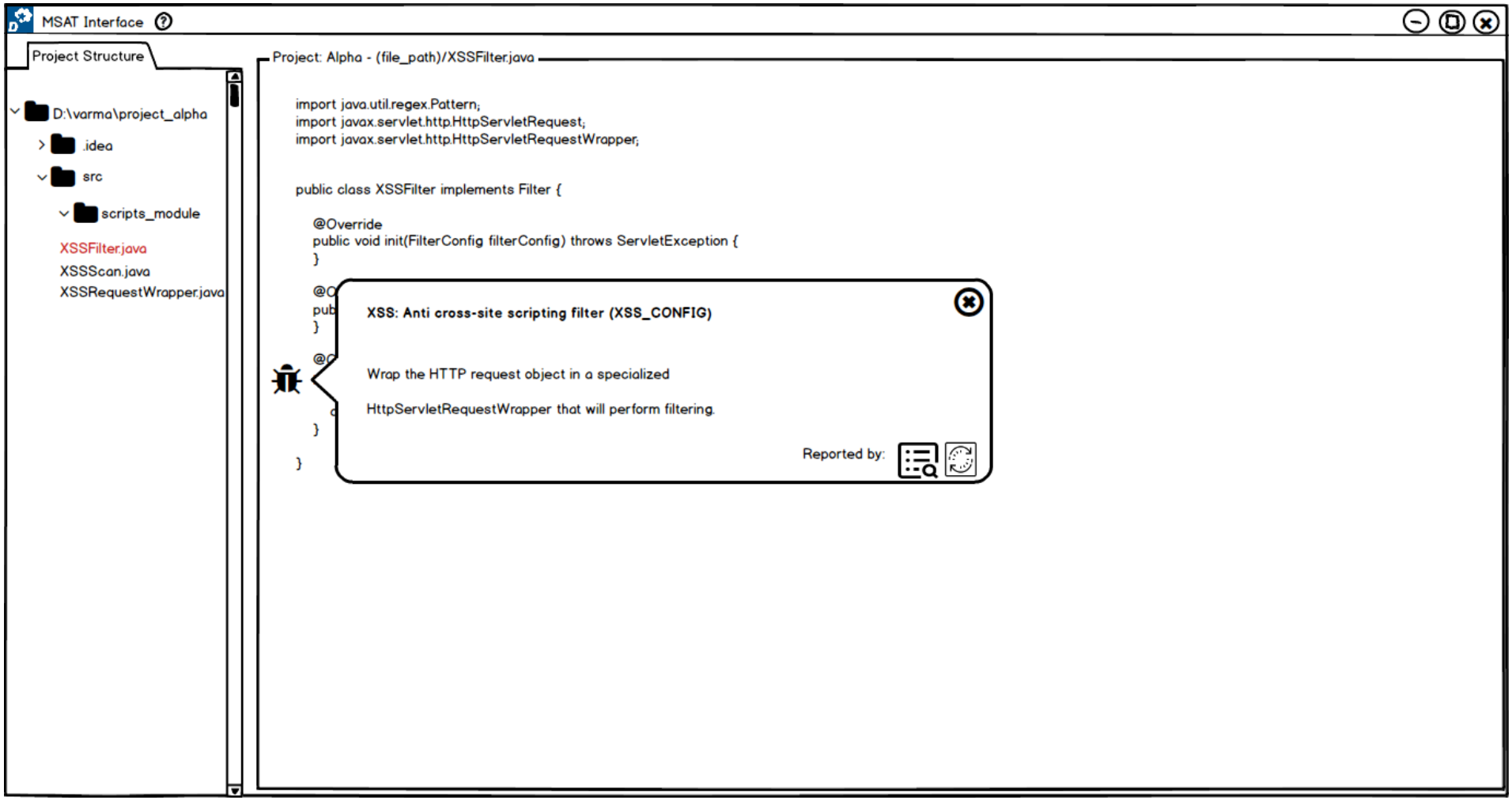
  - Recruit Test Users
  - Order of evaluation altered
  - Perform Tasks (Metric 1 – Task Success)
  - Likert Scale (Metric 2 – Perceived Usability)
  - Voting (Metric 3 – Preferred Design)
  - Usability inspection methods: Cognitive Walkthrough

❖ Rensis Likert. “A technique for the measurement of attitudes.” In: Archives of psychology (1932).

Analysis View



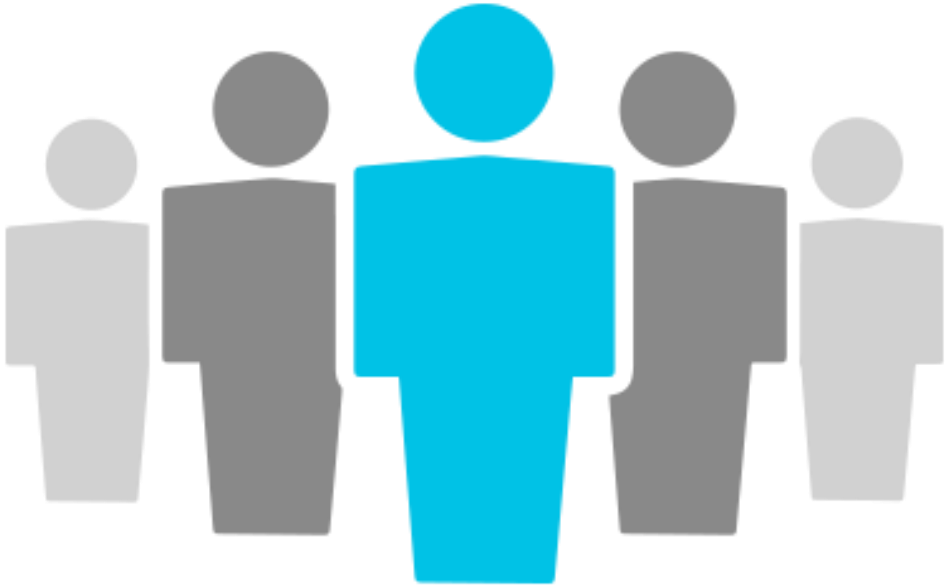
Code View


MSAT Interface
Project Structure
Project: Alpha - (file_path)/XSSFilter.java
D:\varma\project_alpha
.idea
src
scripts_module
XSSFilter.java
XSSScan.java
XSSRequestWrapper.java
import java.util.regex.Pattern;
import javax.servlet.http.HttpServletRequest;
import javax.servlet.http.HttpServletRequestWrapper;
public class XSSFilter implements Filter {
@Override
public void init(FilterConfig filterConfig) throws ServletException {
}
}
XSS: Anti cross-site scripting filter (XSS_CONFIG)
Wrap the HTTP request object in a specialized
HttpServletRequestWrapper that will perform filtering.
Reported by:

UX Design Cycle 1

UX 1

- Users: 5
- Sub research questions: 9
- Each session: ~ 90 minutes



Added db2 database mapping after reading forum post

Jul 17 2014 10:53

by Daniel Lewis in revision 91687a1146419dd23ceaed299185512696643dc1 (git)

Files: 11 changed

Findings: 4 12 1

Add getDelegationState() in DelegateTask.

Jul 17 2014 10:30

by Anya Hill in revision 812b1e277d844fa48307bcd7c692a6f395c85fbb (git)

Files: 14 changed

Findings: 3 12 5

TASK_TIMEOUT

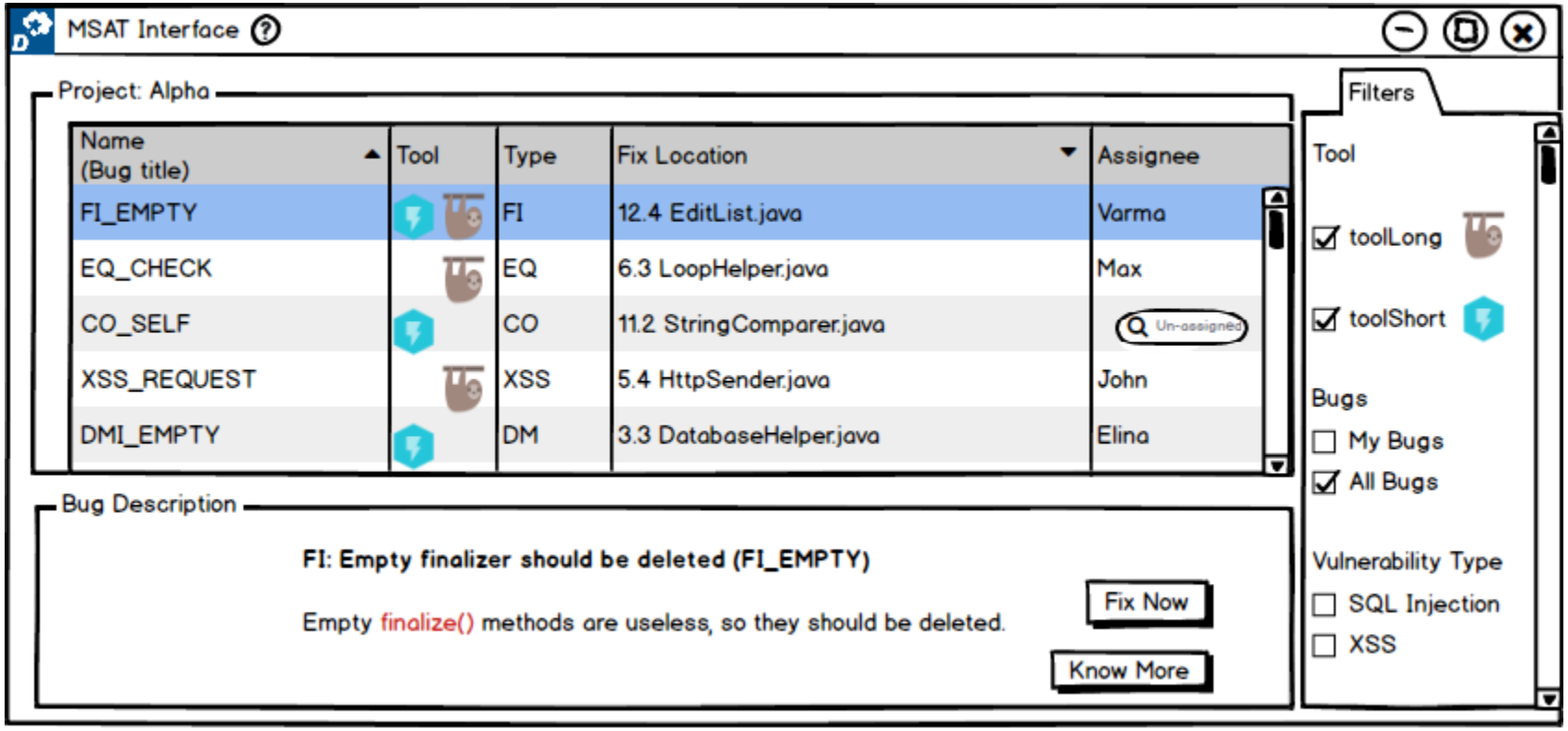
Jul 17 2014 08:46

by Jacob Nelson in revision 997da57af6f2c08d504473d3e9837788b7592dcb (git)

Files: 14 changed

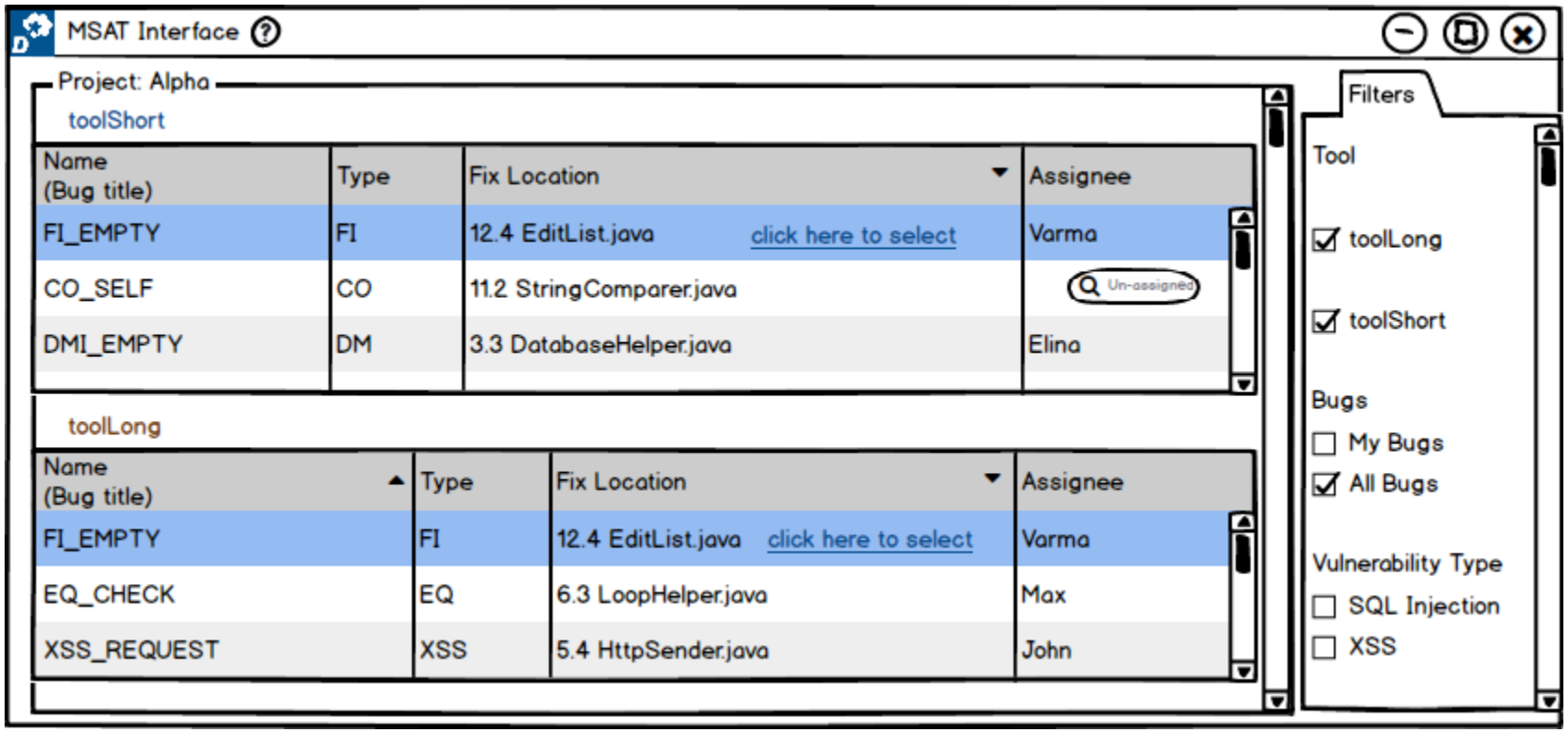
Findings: 5 12 3

[RQ 1.1] Does a separate list or single list help the user to identify the common bug?



- Single List

[RQ 1.1] Does a separate list or single list help the user to identify the common bug?



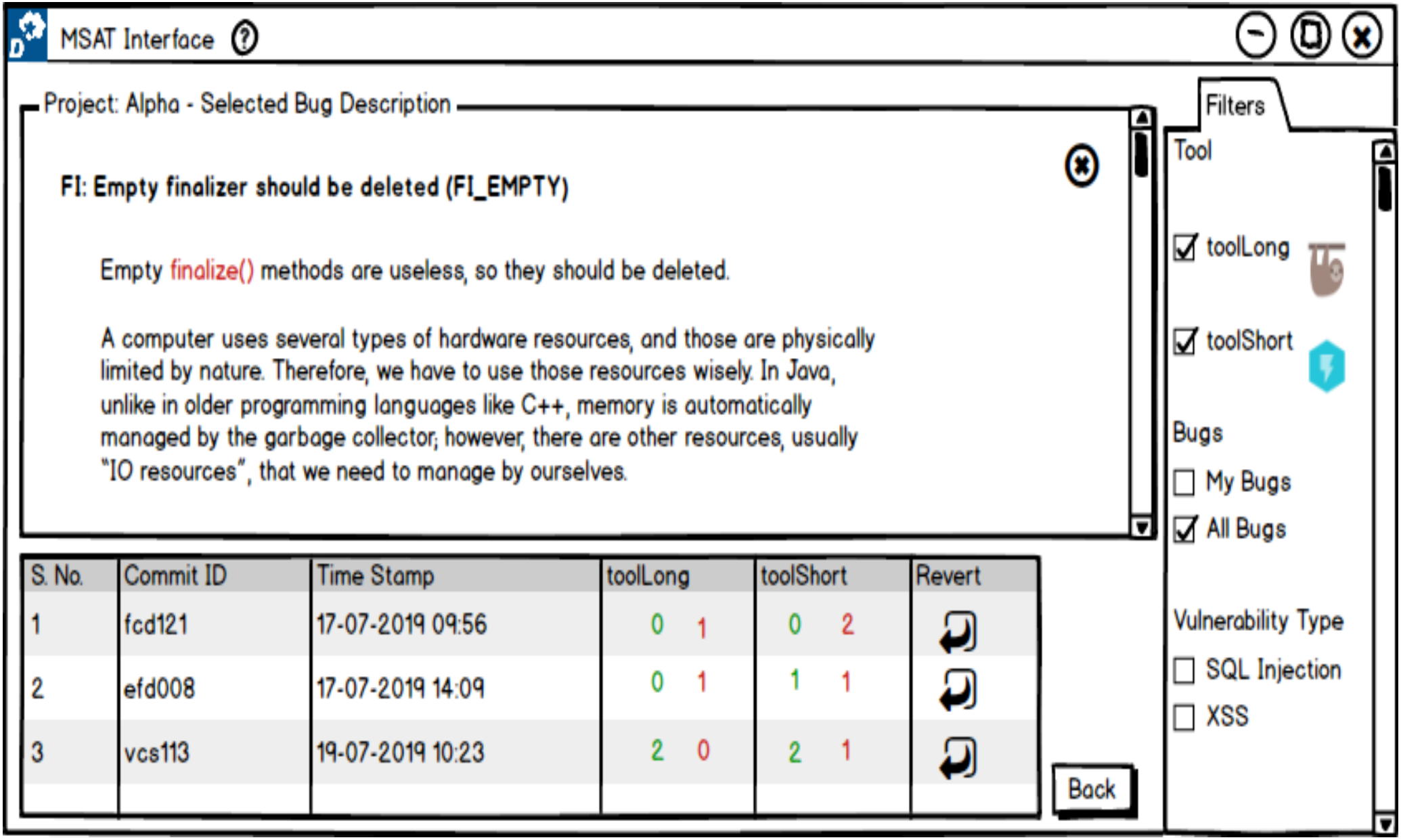
- Seperate List

[RQ 1.1] Does a separate list or single list help the user to identify the common bug?

- Results:

	Single List	Separate List
Task Success	100 %	100 %
Usability	8	7.6
Votes	2	3

  - Separate List – “more effective when using more tools”


MSAT Interface
Project: Alpha - Selected Bug Description
FI: Empty finalizer should be deleted (FI_EMPTY)
Empty finalize() methods are useless, so they should be deleted.
A computer uses several types of hardware resources, and those are physically limited by nature. Therefore, we have to use those resources wisely. In Java, unlike in older programming languages like C++, memory is automatically managed by the garbage collector; however, there are other resources, usually "IO resources", that we need to manage by ourselves.
S. No.
Commit ID
Time Stamp
toolLong
toolShort
Revert
1
fcd121
17-07-2019 09:56
0 1
0 2
2
efd008
17-07-2019 14:09
0 1
1 1
3
vcs113
19-07-2019 10:23
2 0
2 1
Back
Filters
Tool
toolLong
toolShort
Bugs
My Bugs
All Bugs
Vulnerability Type
SQL Injection
XSS

UX 1 – Lessons

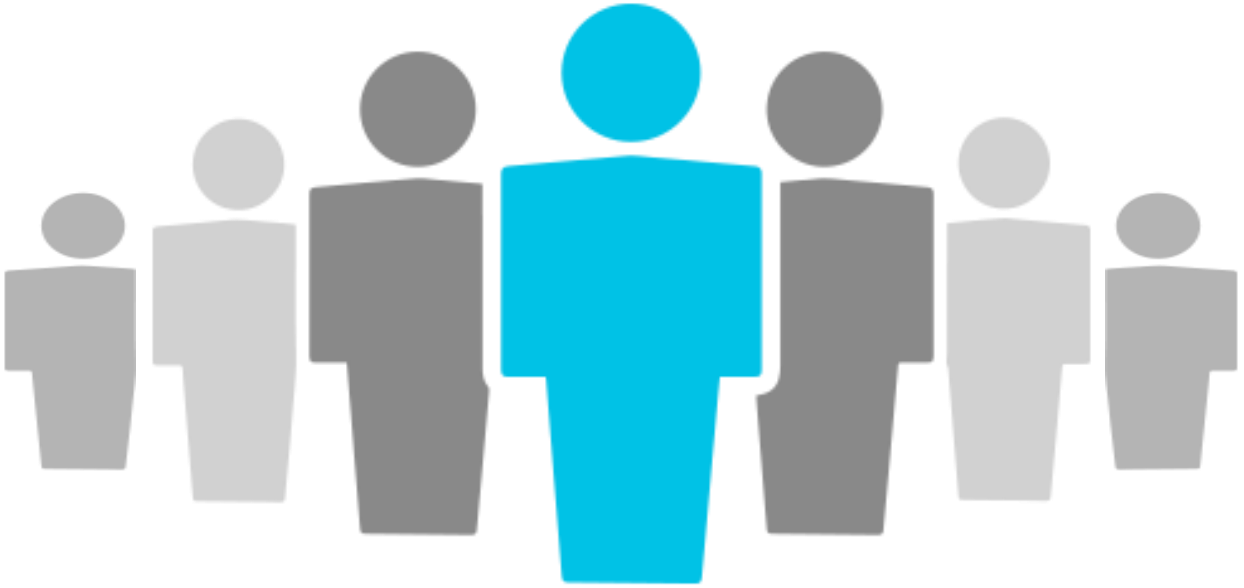
- Analysis View

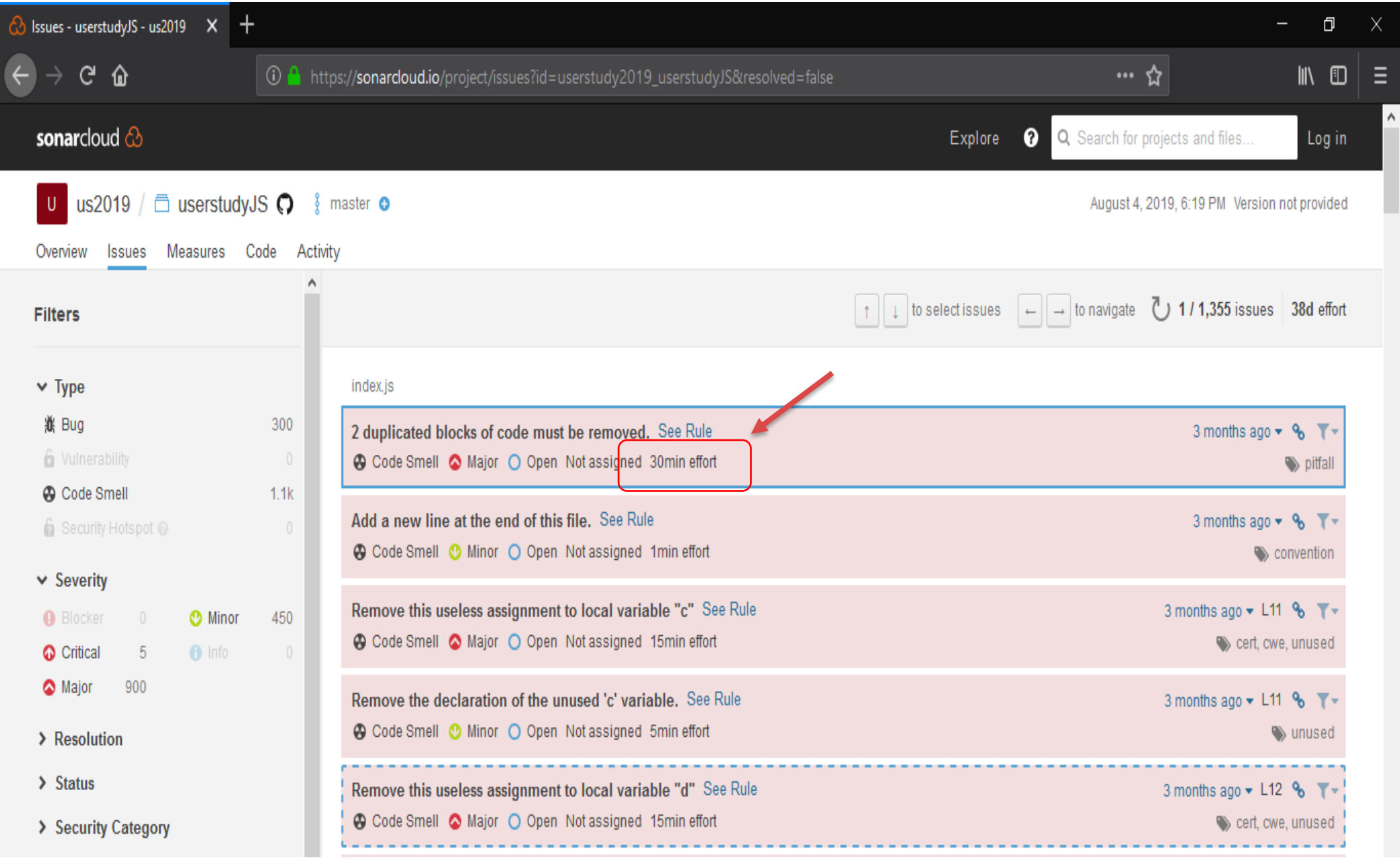
- Improvisations for next UX cycle:
  - Increase code base
  - Volume of bugs (+ scroll)
  - Integrate more tools
  - Code view perspective
  - + new sub RQ’s

UX Design Cycle 2

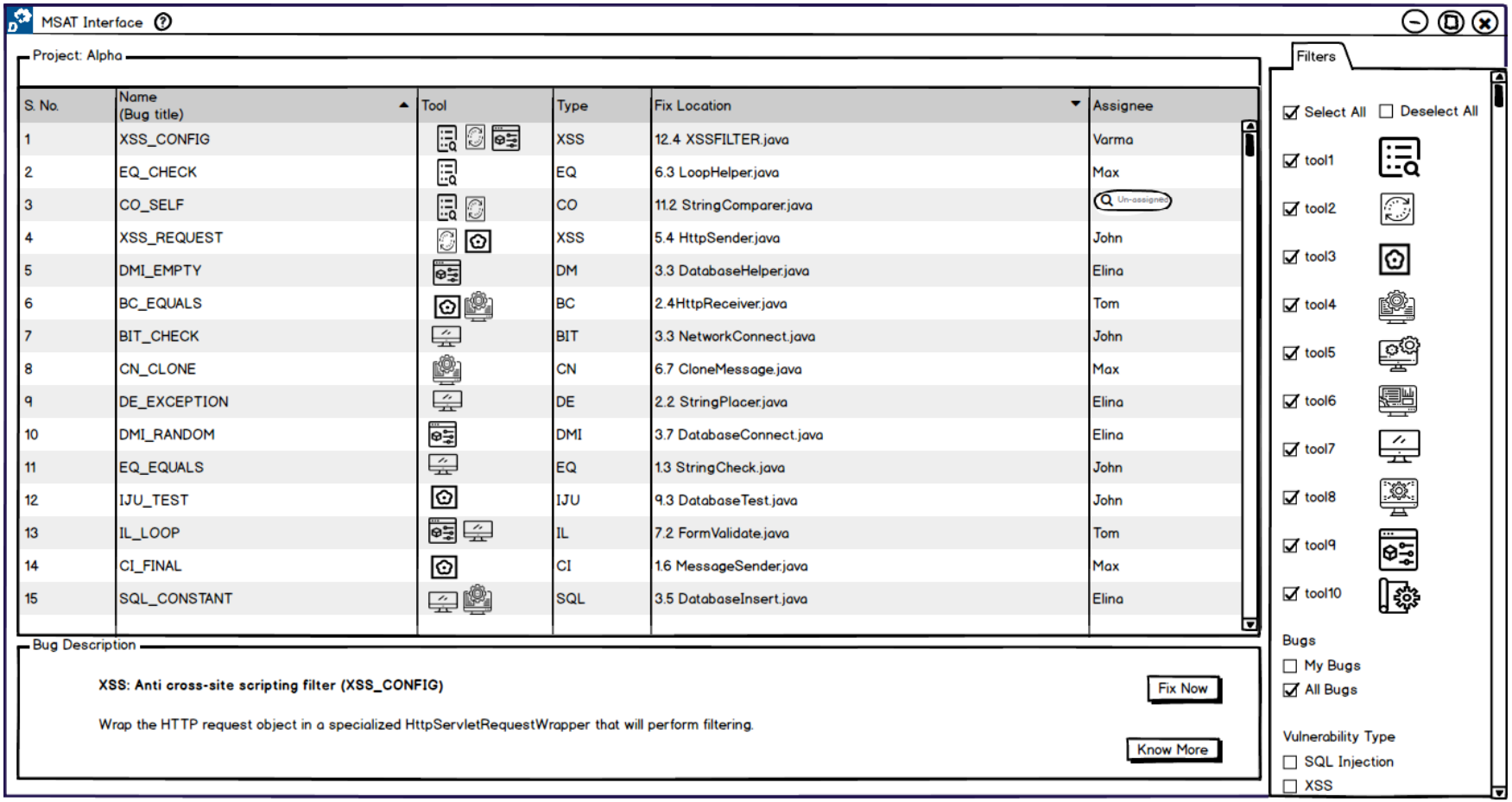
UX 2

- Users: 7
- Sub research questions: 9
- Each session: ~ 105 minutes



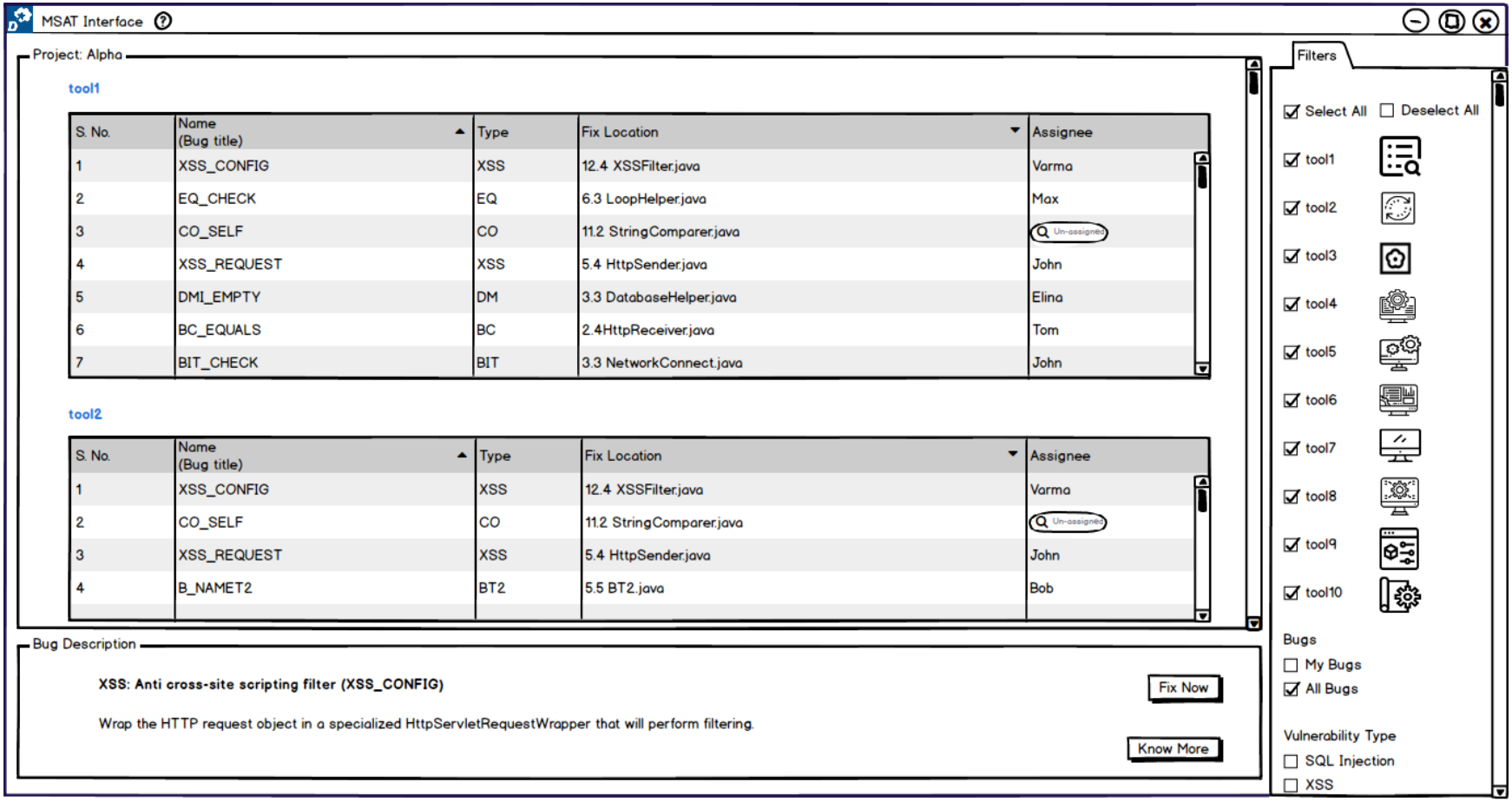

Issues - userstudyJS - us2019
https://sonarcloud.io/project/issues?id=userstudy2019_userstudyJS&resolved=false
sonarcloud
Explore
Search for projects and files...
Log in
us2019 / userstudyJS master
August 4, 2019, 6:19 PM Version not provided
Overview Issues Measures Code Activity
Filters
to select issues
to navigate
1 / 1,355 issues
38d effort
Type
Bug 300
Vulnerability 0
Code Smell 1.1k
Security Hotspot 0
Severity
Blocker 0
Minor 450
Critical 5
Info 0
Major 900
Resolution
Status
Security Category
index.js
2 duplicated blocks of code must be removed. See Rule
Code Smell Major Open Not assigned 30min effort
3 months ago
pitfall
Add a new line at the end of this file. See Rule
Code Smell Minor Open Not assigned 1min effort
3 months ago
convention
Remove this useless assignment to local variable "c" See Rule
Code Smell Major Open Not assigned 15min effort
3 months ago L11
cert, cwe, unused
Remove the declaration of the unused 'c' variable. See Rule
Code Smell Minor Open Not assigned 5min effort
3 months ago L11
unused
Remove this useless assignment to local variable "d" See Rule
Code Smell Major Open Not assigned 15min effort
3 months ago L12
cert, cwe, unused

[RQ 1.1] Does a separate list or single list help the user to identify the common bug?



- Single List

[RQ 1.1] Does a separate list or single list help the user to identify the common bug?



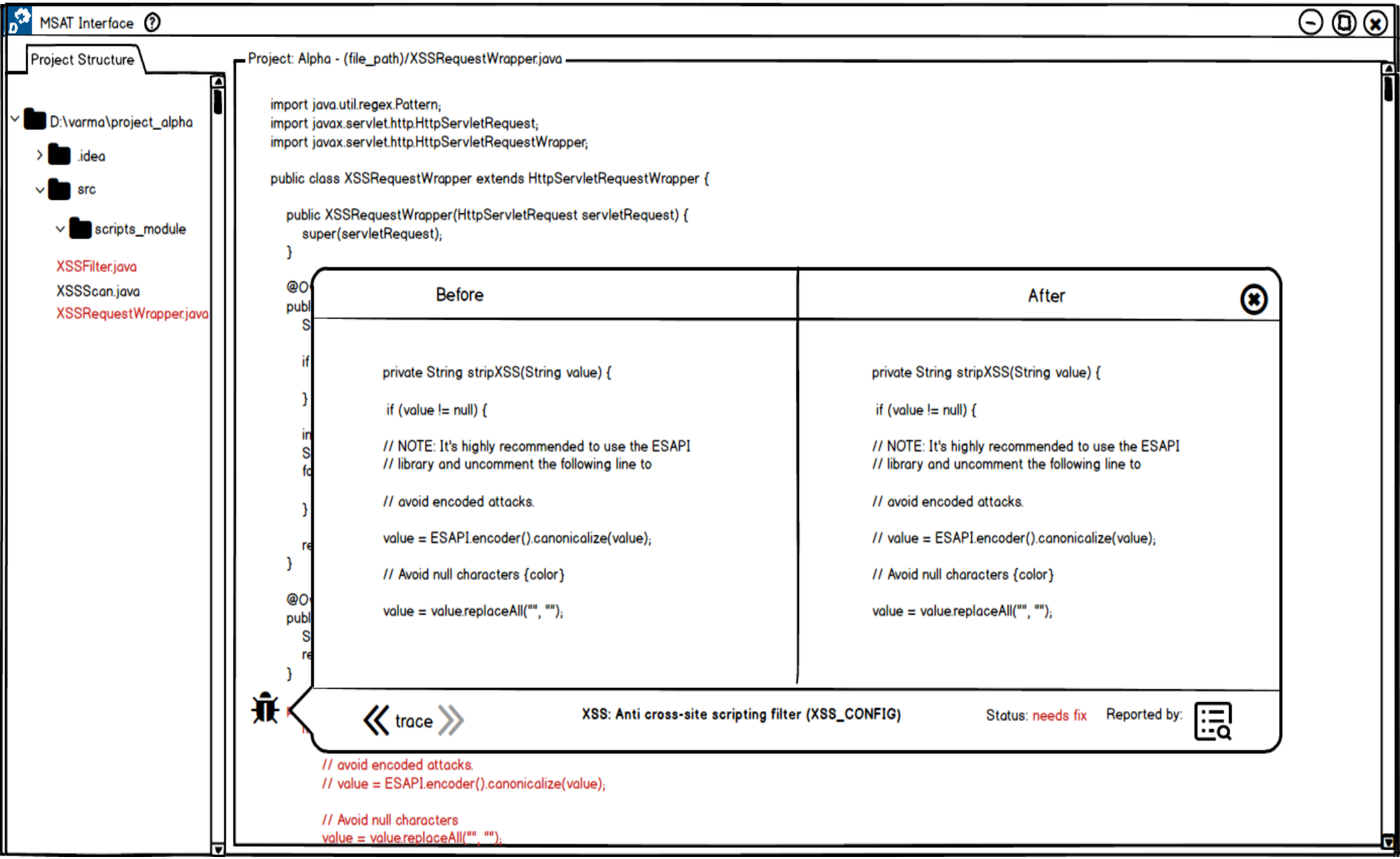
- Separate List

[RQ 1.1] Does a separate list or single list help the user to identify the common bug?

- Results:

	Single List	Separate List
Task Success	71.43 %	42.85 %
Usability	8.14	5.43
Votes	5	0

  - Single List – “effortless to perceive, more user friendly”


MSAT Interface
Project Structure
Project: Alpha - (file_path)/XSSRequestWrapper.java
D:\varma\project_alpha
.idea
src
scripts_module
XSSFilter.java
XSSScan.java
XSSRequestWrapper.java
import java.util.regex.Pattern;
import javax.servlet.http.HttpServletRequest;
import javax.servlet.http.HttpServletRequestWrapper;
public class XSSRequestWrapper extends HttpServletRequestWrapper {
public XSSRequestWrapper(HttpServletRequest servletRequest) {
super(servletRequest);
}
Before
private String stripXSS(String value) {
if (value != null) {
// NOTE: It's highly recommended to use the ESAPI
// library and uncomment the following line to
// avoid encoded attacks.
value = ESAPI.encoder().canonicalize(value);
// Avoid null characters {color}
value = value.replaceAll("", "");
After
private String stripXSS(String value) {
if (value != null) {
// NOTE: It's highly recommended to use the ESAPI
// library and uncomment the following line to
// avoid encoded attacks.
// value = ESAPI.encoder().canonicalize(value);
// Avoid null characters {color}
value = value.replaceAll("", "");
trace
XSS: Anti cross-site scripting filter (XSS_CONFIG)
Status: needs fix
Reported by:
// avoid encoded attacks.
// value = ESAPI.encoder().canonicalize(value);
// Avoid null characters
value = value.replaceAll("", "");

UX 2 – Lessons

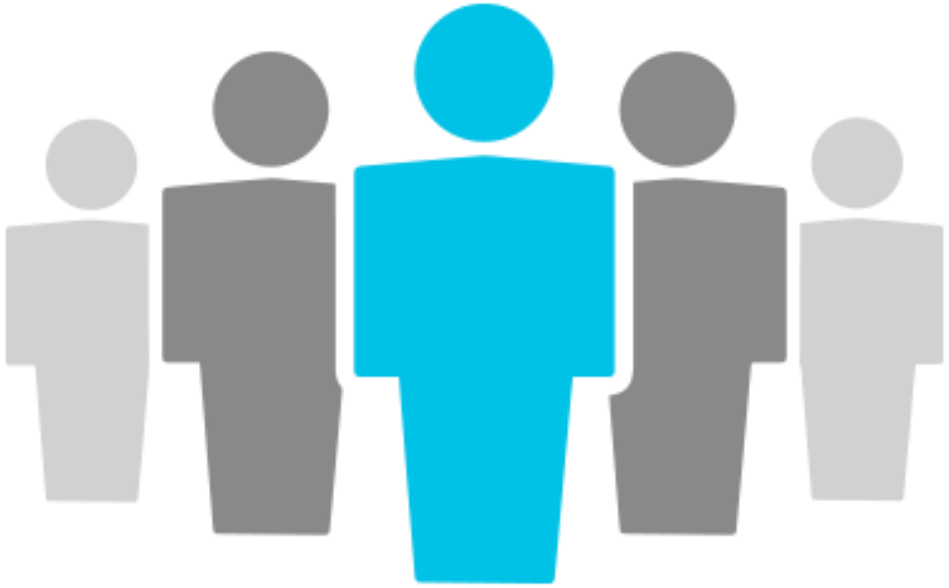
- Analysis View
- Code View
- UX 1 Scalability

- Improvisations for next UX cycle:
  - UX 2 Scalability
  - + new sub RQ’s

UX Design Cycle 3

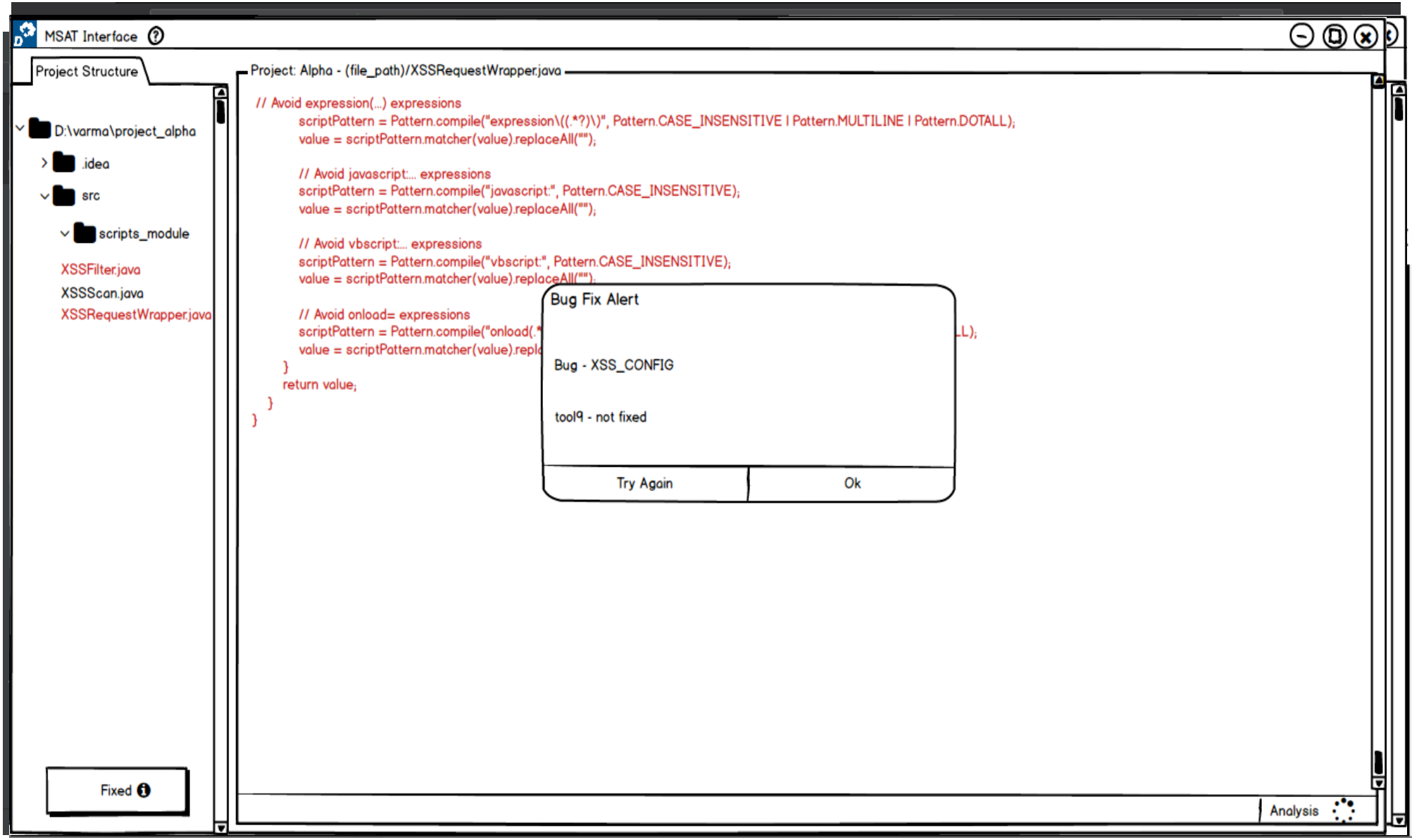
UX 3

- Users: 5
- Sub research questions: 13
- Each session: ~ 120 minutes



UX 3	Analysis View	Code View
RQ 1 (display)		• Next • List view • Bug icons • Table view • Vertical view • Horizontal view • Similar boxes • Similar list
RQ 2 (feedback)	• Animated Icons • Progress Bar • Popup	• Toasts (alerts) • Spinner (status)
RQ 3 (trace)		• Before/After • Table view

[RQ 2.1]


MSAT Interface
Project Structure
D:\varma\project_alpha
.idea
src
scripts_module
XSSFilter.java
XSSScan.java
XSSRequestWrapper.java
Fixed
Project: Alpha - (file_path)/XSSRequestWrapper.java
// Avoid expression(...) expressions
scriptPattern = Pattern.compile("expression\((.*?)\)", Pattern.CASE_INSENSITIVE | Pattern.MULTILINE | Pattern.DOTALL);
value = scriptPattern.matcher(value).replaceAll("");
// Avoid javascript:... expressions
scriptPattern = Pattern.compile("javascript:", Pattern.CASE_INSENSITIVE);
value = scriptPattern.matcher(value).replaceAll("");
// Avoid vbscript:... expressions
scriptPattern = Pattern.compile("vbscript:", Pattern.CASE_INSENSITIVE);
value = scriptPattern.matcher(value).replaceAll("");
// Avoid onload= expressions
scriptPattern = Pattern.compile("onload(.*
value = scriptPattern.matcher(value).repl
}
return value;
}
}
Bug Fix Alert
Bug - XSS_CONFIG
tool9 - not fixed
Try Again
Ok
Analysis

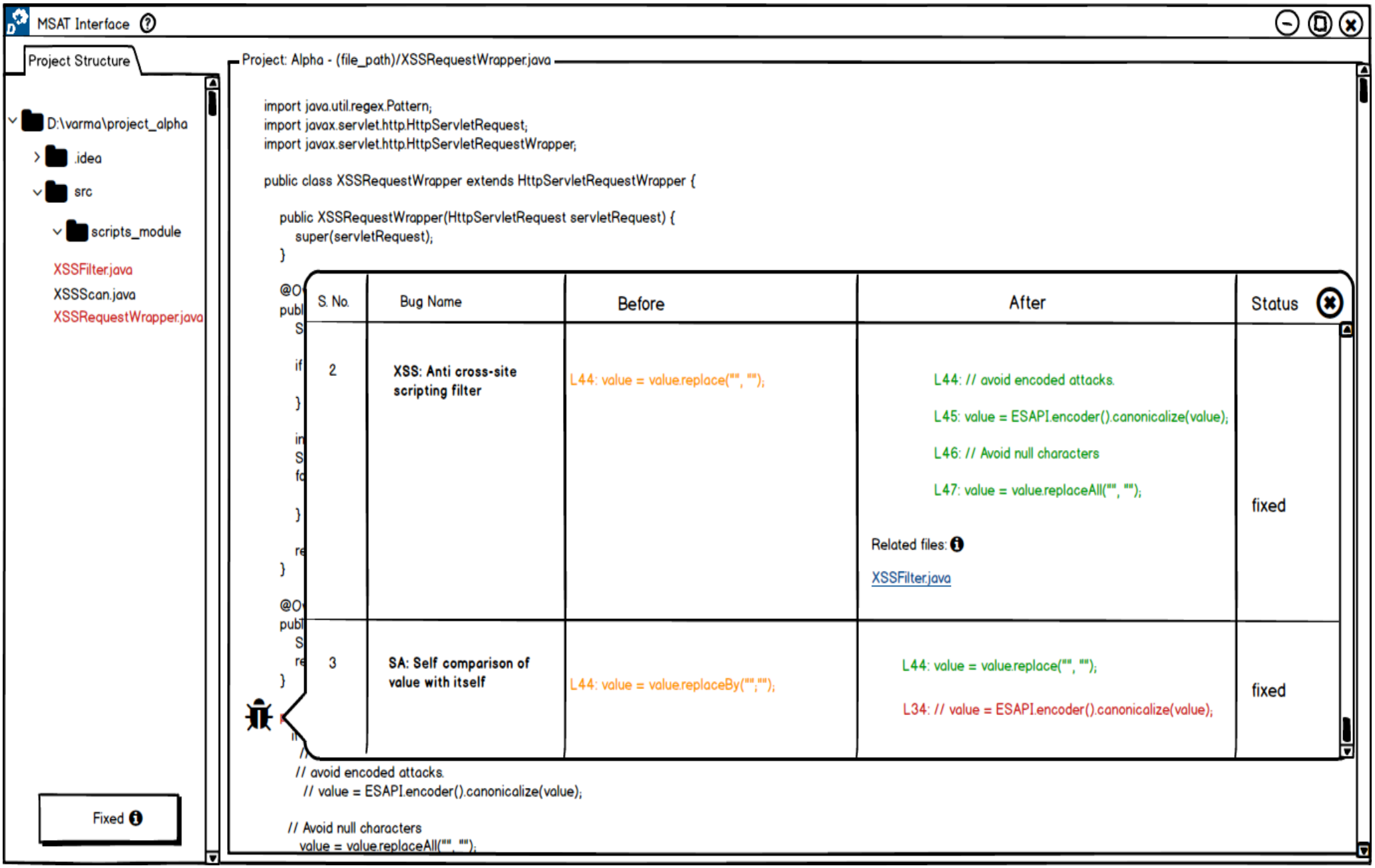
[RQ 2.1]

How usable are each feedback functionality compared to the scenario of using unified UI to native UIs?

Result	MSAT-UI*	Native UIs
Animated Icons	8.4	0
Progress Bar	7.6	0.8
Pending Status Popup	7.8	0
Alerts	9.2	0
Status	8.8	4

Almost all users agreed the ideas being novel and hardly present with native UIs.

*Multiple Static Analysis Tools – User Interface


MSAT Interface
Project Structure
Project: Alpha - (file_path)/XSSRequestWrapper.java
D:\varma\project_alpha
.idea
src
scripts_module
XSSFilter.java
XSSScan.java
XSSRequestWrapper.java
Fixed
import java.util.regex.Pattern;
import javax.servlet.http.HttpServletRequest;
import javax.servlet.http.HttpServletRequestWrapper;
public class XSSRequestWrapper extends HttpServletRequestWrapper {
public XSSRequestWrapper(HttpServletRequest servletRequest) {
super(servletRequest);
}
// avoid encoded attacks.
// value = ESAPI.encoder().canonicalize(value);
// Avoid null characters
value = value.replaceAll("", "");
S. No.
Bug Name
Before
After
Status
2
XSS: Anti cross-site scripting filter
L44: value = value.replace("", "");
L44: // avoid encoded attacks.
L45: value = ESAPI.encoder().canonicalize(value);
L46: // Avoid null characters
L47: value = value.replaceAll("", "");
Related files:
XSSFilter.java
fixed
3
SA: Self comparison of value with itself
L44: value = value.replaceBy("","");
L44: value = value.replace("", "");
L34: // value = ESAPI.encoder().canonicalize(value);
fixed

Findings

	Analysis View	Code View
RQ 1 (display)	• Single list	• List view • Single icon • Table view • Similar list
RQ 2 (feedback)	• Animated Icons • Progress Bar • Popup	• Toasts (alerts)
RQ 3 (trace)	• Adjectives	• Table view

Limitations

- Number of participants: > 5

- UX 1 – 5
- UX 2 – 7
- UX 3 – 5

- Priming, Recency bias: Latin Square partition

- Closed Study, Design Tool

balsamiq®

- Why You Only Need to Test with 5 Users. url: https://www.nngroup.com/articles/why-you-only-need-to-test-with-5-users
- Balsamiq – Rapid, effective and fun wireframing software. url: https://balsamiq.com/

Future Work

- Q. Would having tabs help scale the tools visibility with bugs results?
- Q. Do graphs help in understanding the bugs reported?
- RQ 4: How is teamwork facilitated in bug fixing in context of multiple tools?

… many more!

Summary

- Importance of Static Analysis tools
- Usage of Multiple Static Analysis tools

- Need for a single user interface for multiple tools

- This thesis work followed UX Design Cycle to achieve usable prototypes focussing on primary research questions such as,

  - How to display results of the same codebase from different analysis tools?
  - What feedback works to know that bug fixing is on-going?
  - How to carry traceability of bug fixing?