Table A: The selected test cases of the Juliet test suite.

Test Case	LOC	Total number of vulnerabilities
CWE319_Cleartext_Tx_Sensitive_Info__connect_tcp_driverManager.	391	7
CWE570_Expression_Always_False__class_getClass_equal.	54	1
CWE690_NULL_Deref_From_Return__Class_String.	86	4
CWE253_Incorrect_Check_of_Function_Return_Value__FileInputStream.	146	1
CWE252_Unchecked_Return_Value__FileInputStream.	208	2
CWE571_Expression_Always_True__class_getClass_not_equal.	54	1
CWE191_Integer_Underflow__byte_console_readLine_multiply.	208	4
CWE481_Assigning_Instead_of_Comparing__basic.	108	2
CWE563_Unused_Variable__unused_init_variable_int.	68	2
CWE390_Error_Without_Action__mkdirs.	129	2
CWE197_Numeric_Truncation_Error__int_connect_tcp_to_byte.	148	3
CWE476_NULL_Pointer_Dereference__binary_if.	96	2
CWE134_Uncontrolled_Format_String__connect_tcp_format.	221	4
CWE835_Infinite_Loop__do.	57	1
CWE478_Missing_Default_Case_in_Switch__basic.	85	1
CWE483_Incorrect_Block_Delimitation__if_without_braces_multiline.	68	1
CWE395_Catch_NullPointerException__basic.	106	2
CWE382_Use_of_System_Exit__Servlet_Runtime.	55	1
CWE15_External_Control_of_System_or_Configuration_Setting__connect_tcp.	191	3
CWE78_OS_Command_Injection__connect_tcp.	162	3
CWE643_Xpath_Injection_connect_tcp.	312	3
CWE89_SQL_Injection_database_executeQuery.	398	4
CWE23_Relative_Path_Traversal_connect_tcp.	280	3
CWE90_LDAP_Injection_connect_tcp.	155	3
CWE113_HTTP_Response_Splitting_connect_tcp_addCookieServerlet.	76	1

Table B: The selected heuristics guidelines.

Please select one of the following SAST tools which you have previous experience with to evaluate:

○ Fortify SCA

○ Sparrow SAST

○ PVS-Studio

No	Heuristic	Description	Yes/No	Issues if "Yes"
1	Visibility of System Status	The system should always keep the user informed about what is going on through appropriate feedback within a reasonable time.		
2	Match Between System and the Real World	The system should speak the user’s language, with words, phrases, and concepts familiar to the user, rather than system-oriented terms. Follow real-world conventions, making information appear in a natural and logical order.		
3	Help and Documentation	Even though it is better if the system can be used without documentation, it may be necessary to provide help and documentation. Any such information should be easy to search, focused on the user’s task, list concrete steps to be carried out, and not be too large.		
4	Flexibility and efficiency of use	Accelerators — unseen by the novice user — may often speed up the interaction for the expert user such that the system can cater to both inexperienced and experienced users. Allow users to tailor frequent actions.		
5	Understanding Alternative Fixes & Approaches	Information about alternative ways to achieve the same functionality securely.		
6	Relationship Between Vulnerabilities	Information about how co-occurring vulnerabilities relate to each other.		

7	Locating Information	Information that satisfies "where" questions. Searching for information in the code.		
8	Code Background & Functionality	Information about the history and the functionality of the potentially vulnerable code.		
9	End-User Interaction	Information about sanitization/validation and input coming from users. Does the tool help show where input to the application is coming from?		
10	Understanding Concepts	Information about unfamiliar concepts that appear in the code or in the tool.		
11	Notification Text	Textual information that an analysis tool provides and how that text relates to the potentially vulnerable code.		
12	Vulnerability Severity & Rank	Information about the potential impact of vulnerabilities, including which vulnerabilities are potentially most impactful.		
13	Confirming Expectations	Does the tool behave as expected?		

Table C: System Usability Scale (SUS) items.

No	SUS Items
1	I believe I will use this product on a regular basis.
2	I thought the system was very complicated.
3	I found the system to be simple to use.
4	To utilize this system, I believe I would need the assistance of a technical expert.
5	The many functionalities of this system were properly integrated, in my opinion.
6	This method, I believed, had much too much irregularity.
7	Most individuals, I believe, would soon pick up on how to utilize this method.
8	I found the system to be really inconvenient to utilize.
9	I had a lot of confidence in the system.
10	Before I could get started with this technique, I had to study a lot of things.

Table D: Acceptability ranges of SUS score.

SUS Score	Interpretation
Less than 50	Not Acceptable
From 50 to 70	Marginal
Greater than 70	Acceptable