ZAD2

Branch : main

VERSION 1.0-SNAPSHOT

Code analysis

By: Administrator

2024-12-18

zad2

CONTENT

INTRODUCTION

This document contains results of the code analysis of zad2.

CONFIGURATION

- Quality Profiles

  o Names: Sonar way [Java]; Sonar way [XML];

  o Files: 9c24d35f-16b0-4bd2-b4bc-e96fc1c76e3f.json; 4b086136-2149-4783-8ff9-9189c963009a.json;

- Quality Gate

  o Name: Sonar way

  o File: Sonar way.xml

zad2

SYNTHESIS

ANALYSIS STATUS

Reliability	Security	Security Review	Maintainability
E	A	E	A

QUALITY GATE STATUS

Quality Gate Status	Failed

Metric	Value
Coverage on New Code	ERROR (0.0% is less than 80%)
Duplicated Lines (%) on New Code	OK
Security Hotspots Reviewed on New Code	ERROR (0.0% is less than 100%)
New Issues	ERROR (2 is greater than 0)

METRICS

Coverage	Duplication	Comment density	Median number of lines of code per file	Adherence to coding standard
0.0 %	0.0 %	9.1 %	182.0	99.8 %

TESTS

Total	Success Rate	Skipped	Errors	Failures
19	100.0 %	0	0	0

zad2

DETAILED TECHNICAL DEBT

Reliability	Security	Maintainability	Total
0d 0h 30min	-	0d 2h 59min	**0d 3h 29min**

zad2

METRICS RANGE						
	Cyclomatic Complexity	Cognitive Complexity	Lines of code per file	Comment density (%)	Coverage	Duplication (%)
Min	6.0	0.0	50.0	3.6	0.0	0.0
Max	155.0	152.0	739.0	13.8	0.0	0.0

| VOLUME	
Language	**Number**
Java	739
XML	81
Total	820

zad2

CHARTS

Number of issues by severity

0% 0%

10%

10%

80%

- BLOCKER
- CRITICAL
- MAJOR
- MINOR
- INFO

Number of issues by type

0%

10%

90%

- BUG
- VULNERABILITY
- CODE_SMELL

6

Evolution of number of issues

Evolution of technical debt ratio (%)
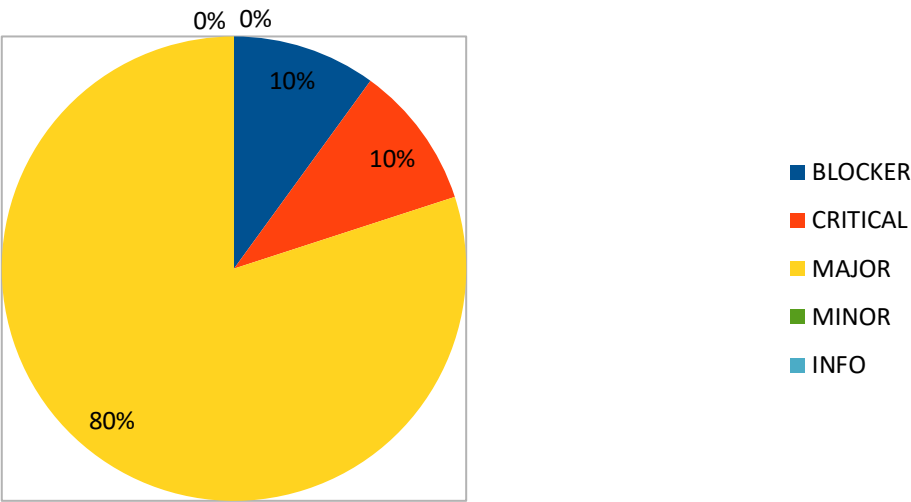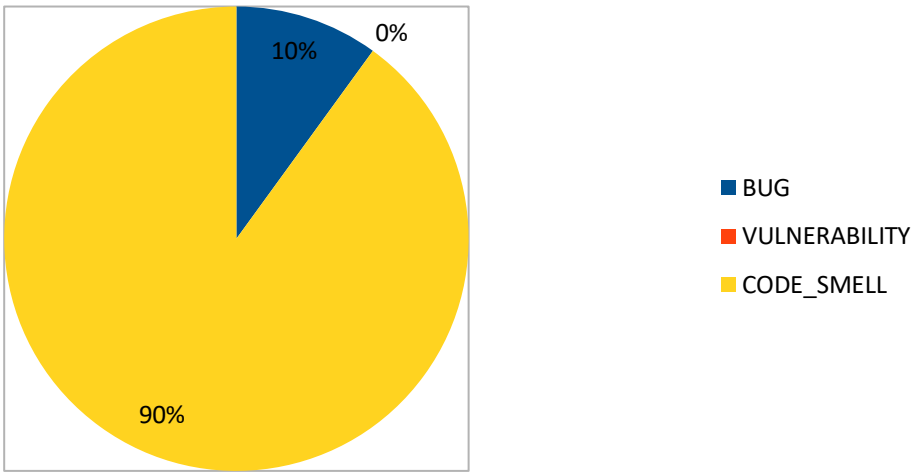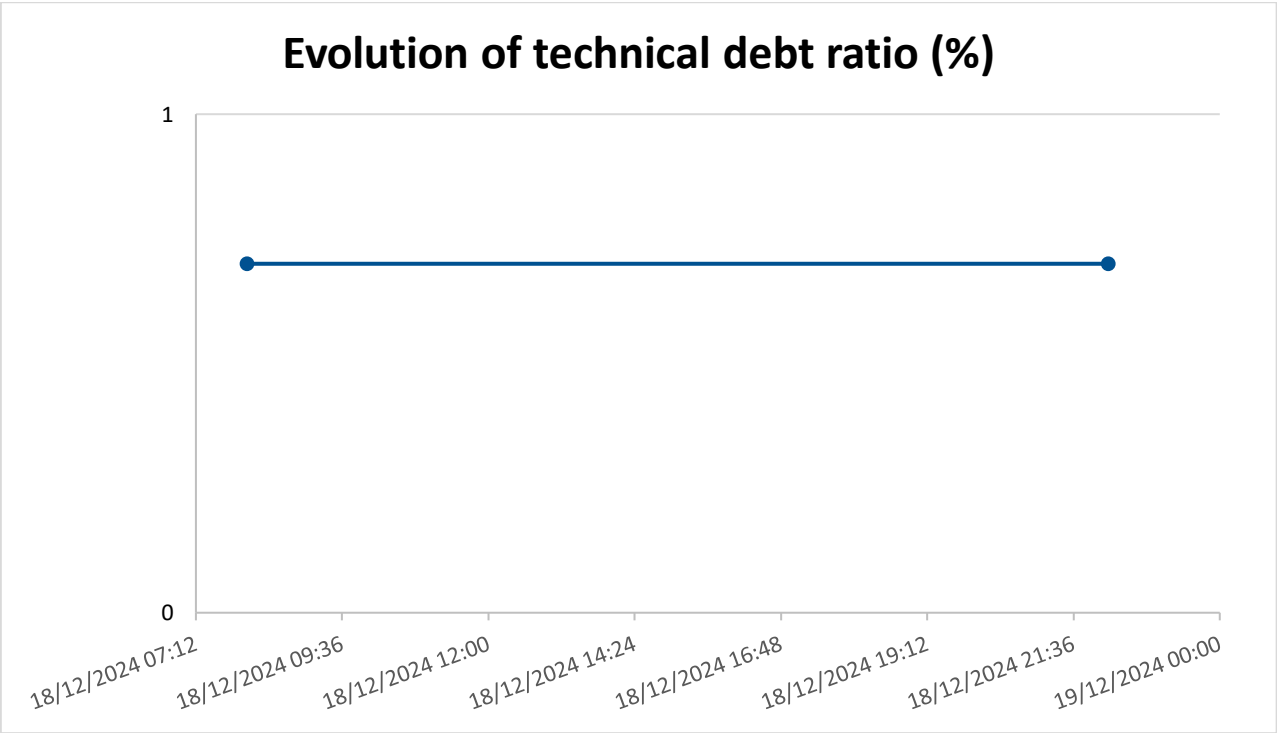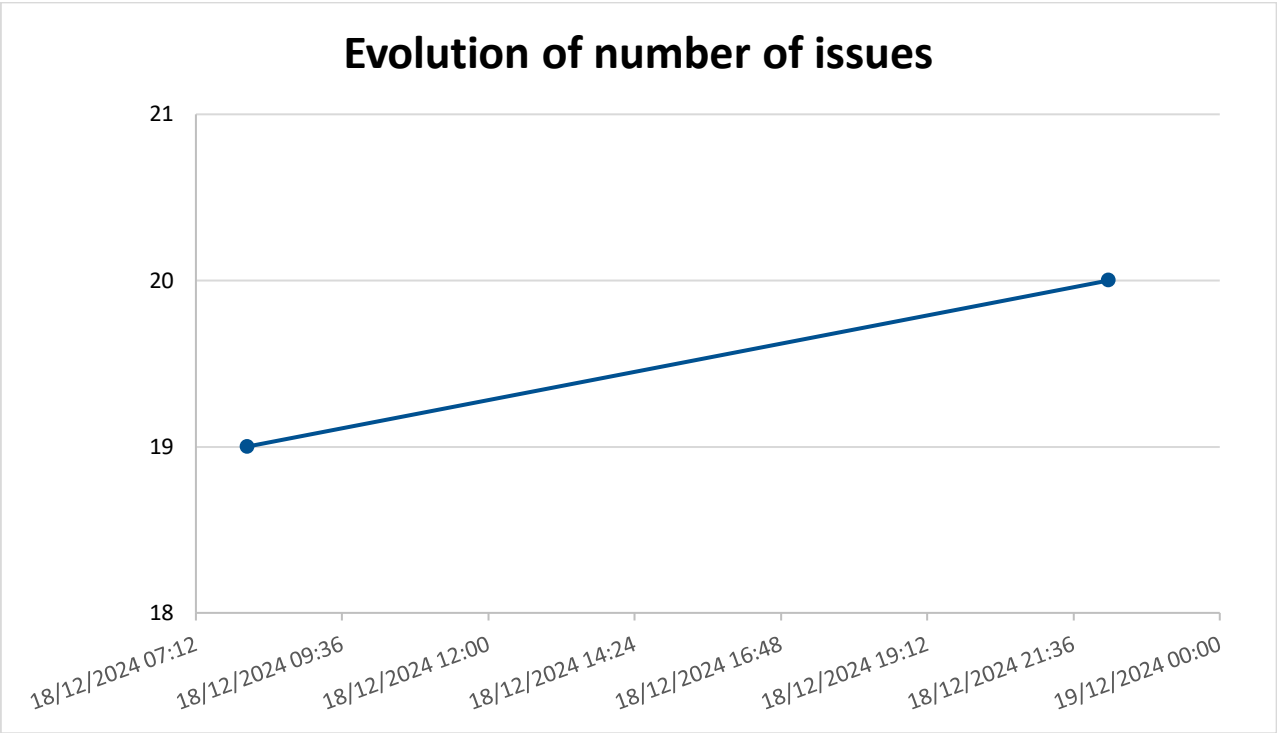
zad2

ISSUES COUNT BY SEVERITY AND TYPE

Type / Severity	INFO	MINOR	MAJOR	CRITICAL	BLOCKER
BUG	0	0	0	0	2
VULNERABILITY	0	0	0	0	0
CODE_SMELL	0	0	16	2	0

ISSUES LIST

Name	Description	Type	Severity	Number
Loops should not be infinite		BUG	BLOCKER	2
Cognitive Complexity of methods should not be too high		CODE_SMELL	CRITICAL	2
Standard outputs should not be used directly to log anything		CODE_SMELL	MAJOR	16

zad2

SECURITY HOTSPOTS

SECURITY HOTSPOTS COUNT BY CATEGORY AND PRIORITY

Category / Priority	LOW	MEDIUM	HIGH
LDAP Injection	0	0	0
Object Injection	0	0	0
Server-Side Request Forgery (SSRF)	0	0	0
XML External Entity (XXE)	0	0	0
Insecure Configuration	1	0	0
XPath Injection	0	0	0
Authentication	0	0	0
Weak Cryptography	0	1	0
Denial of Service (DoS)	0	0	0
Log Injection	0	0	0
Cross-Site Request Forgery (CSRF)	0	0	0
Open Redirect	0	0	0
Permission	0	0	0
SQL Injection	0	0	0
Encryption of Sensitive Data	0	0	0
Traceability	0	0	0
Buffer Overflow	0	0	0
File Manipulation	0	0	0
Code Injection (RCE)	0	0	0

Cross-Site Scripting (XSS)	0	0	0
Command Injection	0	0	0
Path Traversal Injection	0	0	0
HTTP Response Splitting	0	0	0
Others	0	0	0

SECURITY HOTSPOTS LIST

Category	Name	Priority	Severity	Count
Insecure Configuration	Delivering code in production with debug features activated is security-sensitive	LOW	MINOR	1
Weak Cryptography	Using pseudorandom number generators (PRNGs) is security-sensitive	MEDIUM	CRITICAL	1