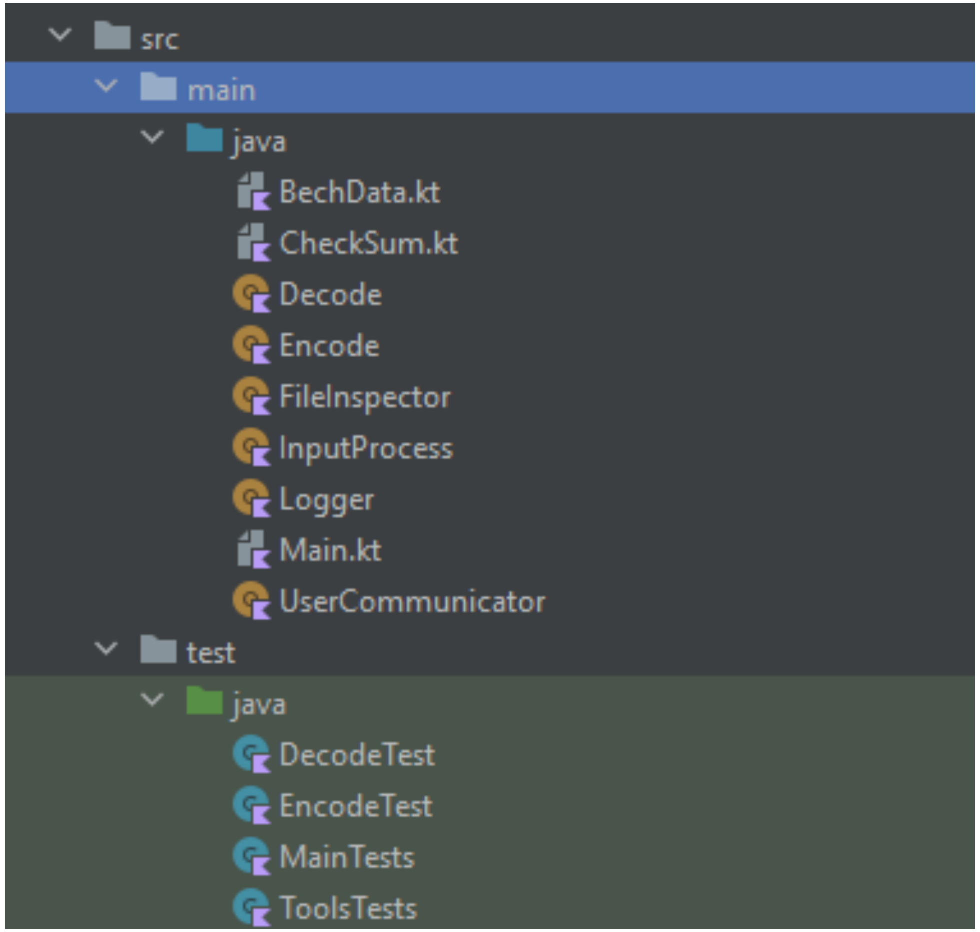
MUNI
FI

super_Bech32m

Mikita Valatovich, Illia Kostenko, Kamil Fňukal

https://github.com/NikitaVolotovich/super_bech32m

Structure of the project



```
src
  main
    java
      BechData.kt
      CheckSum.kt
      Decode
      Encode
      FileInspector
      InputProcess
      Logger
      Main.kt
      UserCommunicator
  test
    java
      DecodeTest
      EncodeTest
      MainTests
      ToolsTests
```

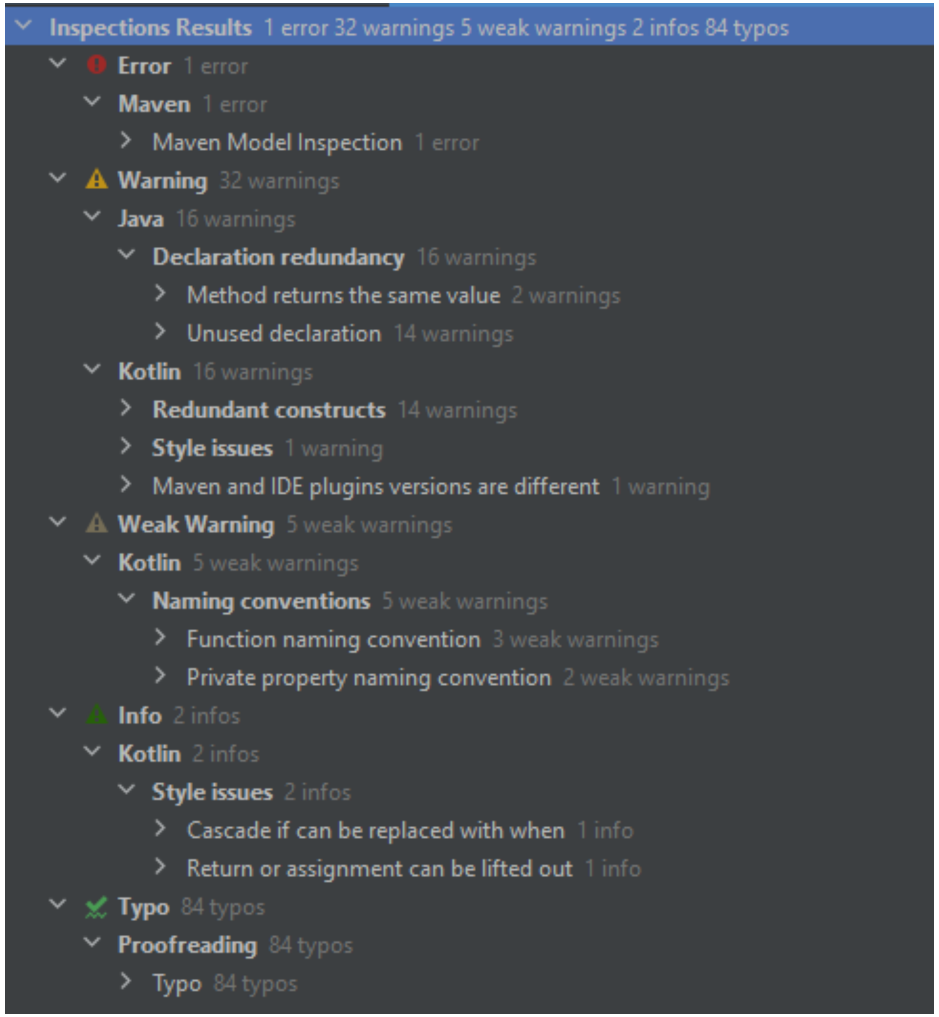
Encountered obstacles

- user friendly and intuitive interface
- prevent incorect inputs
- creating fuzzer for ArrayList<String> with jazzer

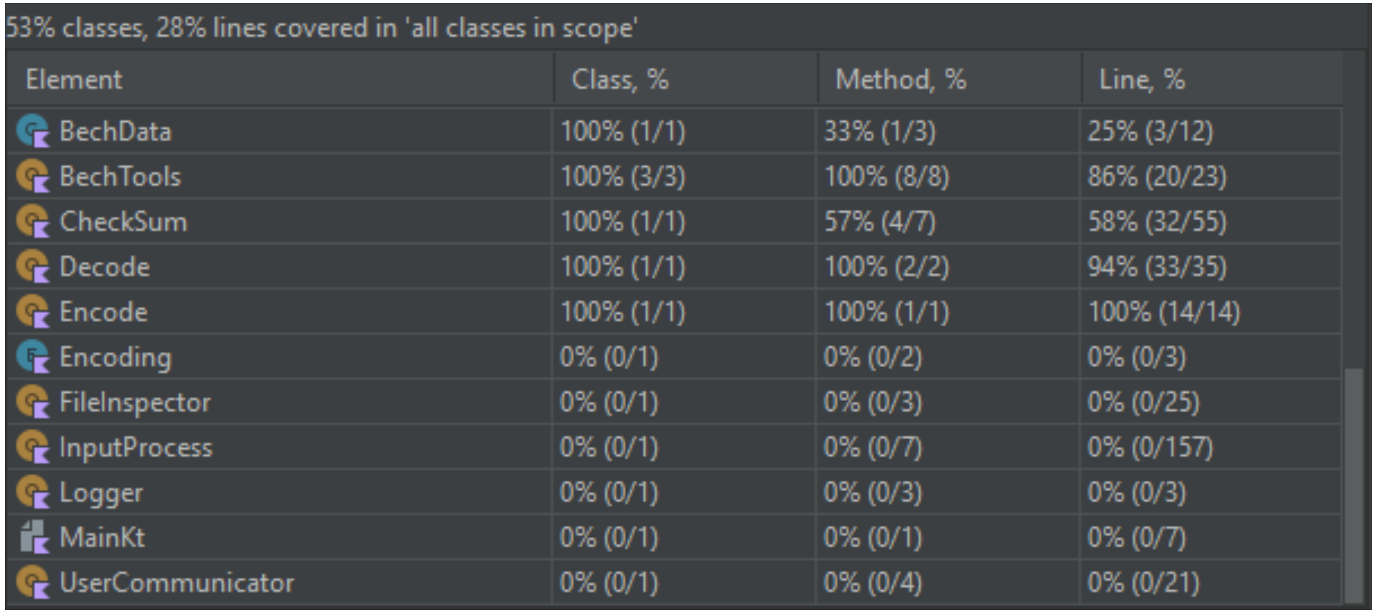
Used analysis tools

- Built-in Intellij analyzer
- SonarQube
- Ktlint
- Snyk
- YourKit Java Profiler

Built-in Intellij analyzer and code coverage



```
Inspections Results 1 error 32 warnings 5 weak warnings 2 infos 84 typos
  Error 1 error
    Maven 1 error
      Maven Model Inspection 1 error
  Warning 32 warnings
    Java 16 warnings
      Declaration redundancy 16 warnings
        Method returns the same value 2 warnings
        Unused declaration 14 warnings
    Kotlin 16 warnings
      Redundant constructs 14 warnings
      Style issues 1 warning
      Maven and IDE plugins versions are different 1 warning
  Weak Warning 5 weak warnings
    Kotlin 5 weak warnings
      Naming conventions 5 weak warnings
        Function naming convention 3 weak warnings
        Private property naming convention 2 weak warnings
  Info 2 infos
    Kotlin 2 infos
      Style issues 2 infos
        Cascade if can be replaced with when 1 info
        Return or assignment can be lifted out 1 info
  Typo 84 typos
    Proofreading 84 typos
      Typo 84 typos
```

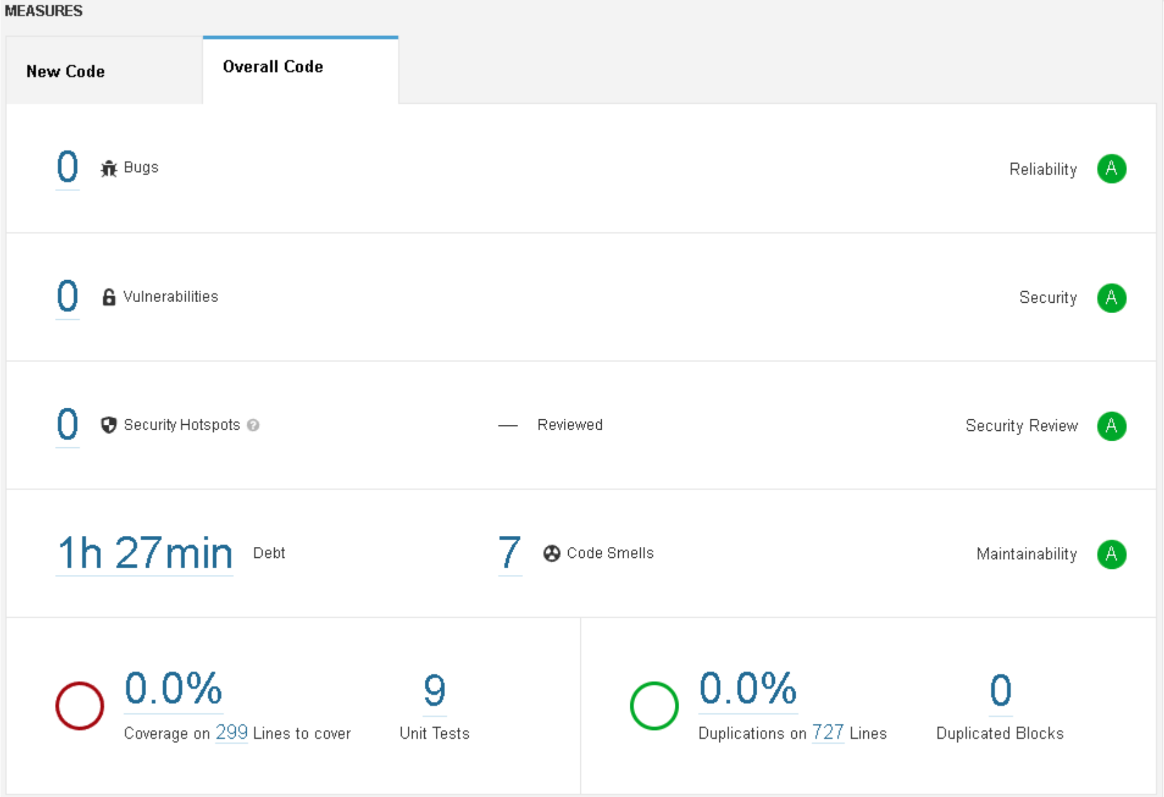


53% classes, 28% lines covered in 'all classes in scope'

Element	Class, %	Method, %	Line, %
BechData	100% (1/1)	33% (1/3)	25% (3/12)
BechTools	100% (3/3)	100% (8/8)	86% (20/23)
CheckSum	100% (1/1)	57% (4/7)	58% (32/55)
Decode	100% (1/1)	100% (2/2)	94% (33/35)
Encode	100% (1/1)	100% (1/1)	100% (14/14)
Encoding	0% (0/1)	0% (0/2)	0% (0/3)
FileInspector	0% (0/1)	0% (0/3)	0% (0/25)
InputProcess	0% (0/1)	0% (0/7)	0% (0/157)
Logger	0% (0/1)	0% (0/3)	0% (0/3)
MainKt	0% (0/1)	0% (0/1)	0% (0/7)
UserCommunicator	0% (0/1)	0% (0/4)	0% (0/21)

Html export in ./CoverageTest.7z

SonarQube



MEASURES

New Code | Overall Code

0 Bugs — Reliability A

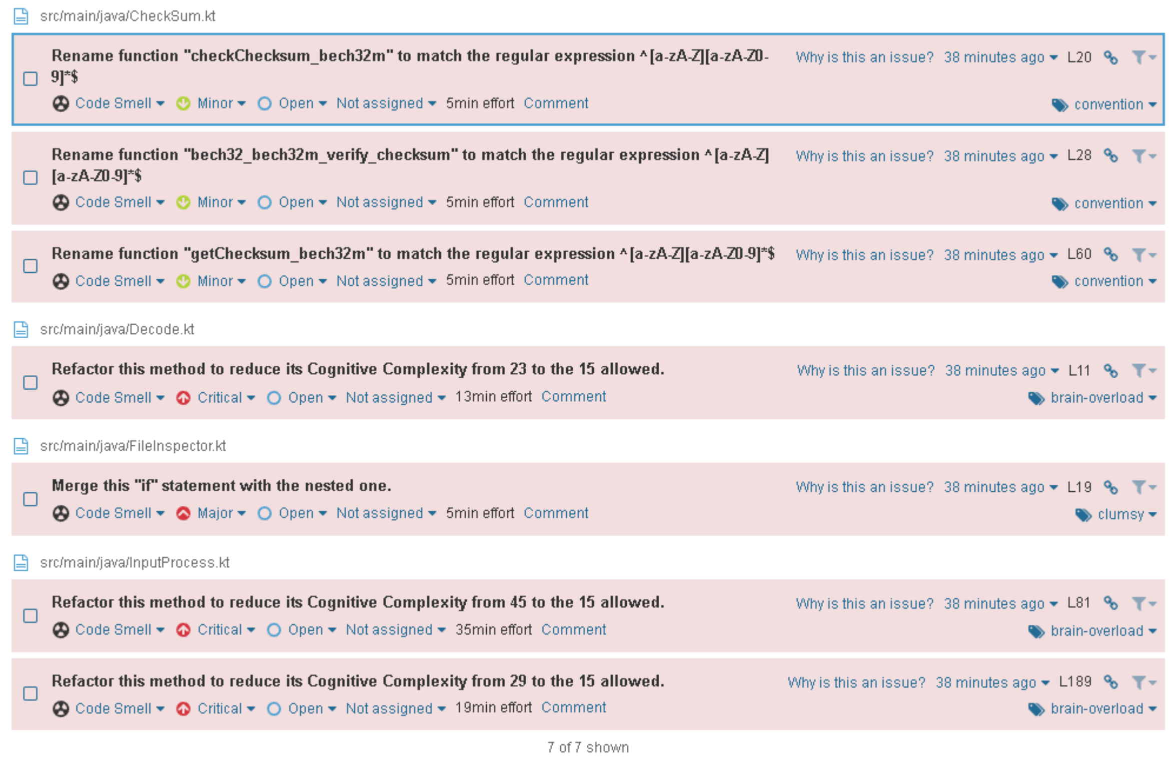
0 Vulnerabilities — Security A

0 Security Hotspots — Reviewed — Security Review A

1h 27min Debt — 7 Code Smells — Maintainability A

0.0% Coverage on 299 Lines to cover — 9 Unit Tests

0.0% Duplications on 727 Lines — 0 Duplicated Blocks



src/main/java/CheckSum.kt

□ Rename function "checkChecksum_bech32m" to match the regular expression ^[a-zA-Z][a-zA-Z0-9]*$ — Why is this an issue? 38 minutes ago L20
Code Smell · Minor · Open · Not assigned · 5min effort · Comment · convention

□ Rename function "bech32_bech32m_verify_checksum" to match the regular expression ^[a-zA-Z][a-zA-Z0-9]*$ — Why is this an issue? 38 minutes ago L28
Code Smell · Minor · Open · Not assigned · 5min effort · Comment · convention

□ Rename function "getChecksum_bech32m" to match the regular expression ^[a-zA-Z][a-zA-Z0-9]*$ — Why is this an issue? 38 minutes ago L60
Code Smell · Minor · Open · Not assigned · 5min effort · Comment · convention

src/main/java/Decode.kt

□ Refactor this method to reduce its Cognitive Complexity from 23 to the 15 allowed. — Why is this an issue? 38 minutes ago L11
Code Smell · Critical · Open · Not assigned · 13min effort · Comment · brain-overload

src/main/java/FileInspector.kt

□ Merge this "if" statement with the nested one. — Why is this an issue? 38 minutes ago L19
Code Smell · Major · Open · Not assigned · 5min effort · Comment · clumsy

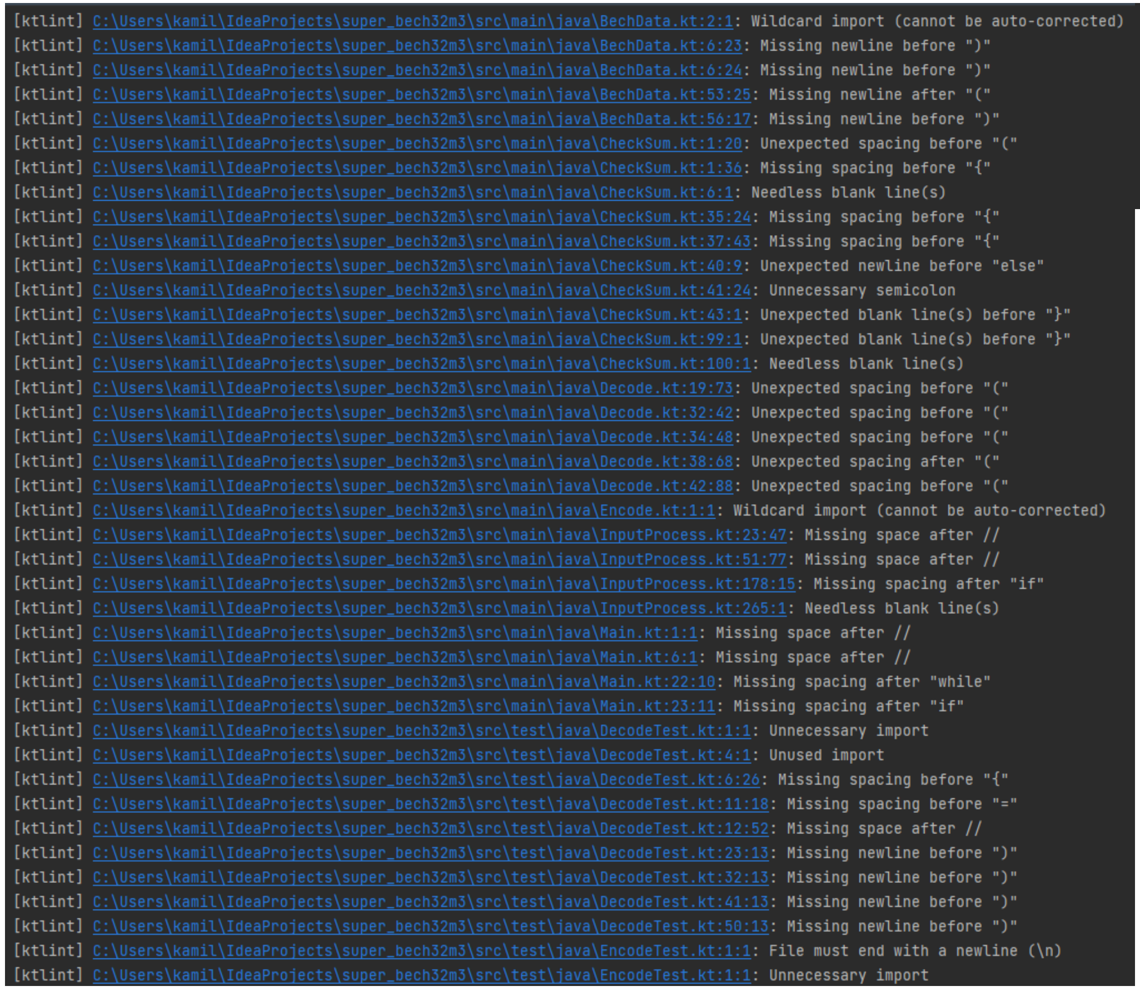
src/main/java/InputProcess.kt

□ Refactor this method to reduce its Cognitive Complexity from 45 to the 15 allowed. — Why is this an issue? 38 minutes ago L81
Code Smell · Critical · Open · Not assigned · 35min effort · Comment · brain-overload

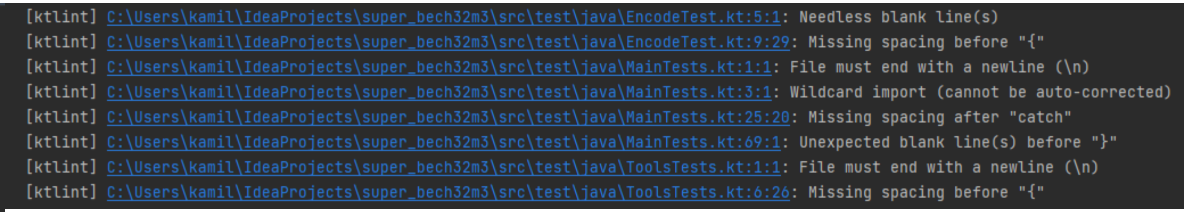
□ Refactor this method to reduce its Cognitive Complexity from 29 to the 15 allowed. — Why is this an issue? 38 minutes ago L189
Code Smell · Critical · Open · Not assigned · 19min effort · Comment · brain-overload

7 of 7 shown

ktlint

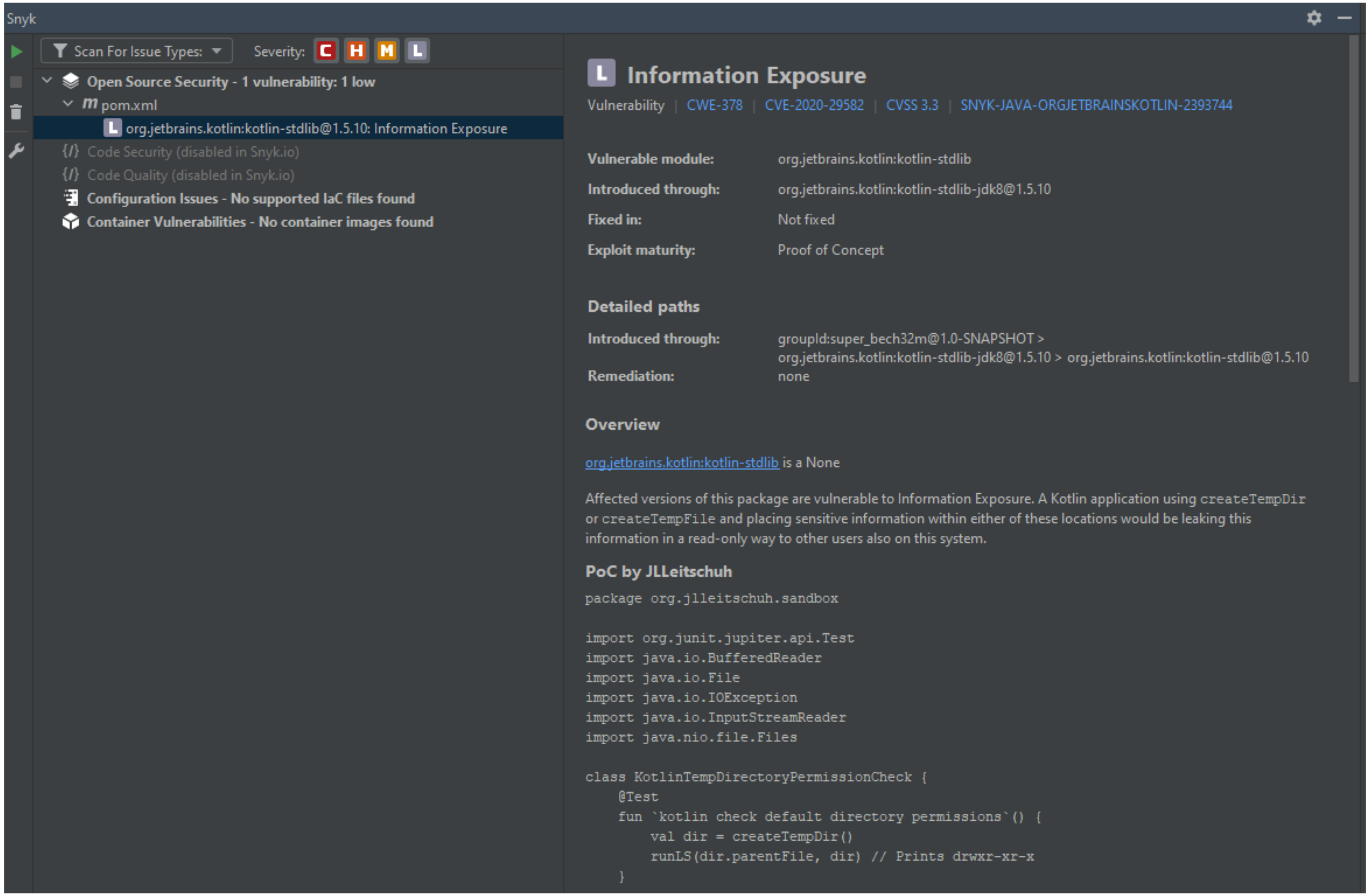


```
[ktlint] C:\Users\kamil\IdeaProjects\super_bech32m3\src\main\java\BechData.kt:2:1: Wildcard import (cannot be auto-corrected)
[ktlint] C:\Users\kamil\IdeaProjects\super_bech32m3\src\main\java\BechData.kt:6:23: Missing newline before ")"
[ktlint] C:\Users\kamil\IdeaProjects\super_bech32m3\src\main\java\BechData.kt:6:24: Missing newline before ")"
[ktlint] C:\Users\kamil\IdeaProjects\super_bech32m3\src\main\java\BechData.kt:53:25: Missing newline after "("
[ktlint] C:\Users\kamil\IdeaProjects\super_bech32m3\src\main\java\BechData.kt:56:17: Missing newline before ")"
[ktlint] C:\Users\kamil\IdeaProjects\super_bech32m3\src\main\java\CheckSum.kt:1:20: Unexpected spacing before "("
[ktlint] C:\Users\kamil\IdeaProjects\super_bech32m3\src\main\java\CheckSum.kt:1:36: Missing spacing before "{"
[ktlint] C:\Users\kamil\IdeaProjects\super_bech32m3\src\main\java\CheckSum.kt:6:1: Needless blank line(s)
[ktlint] C:\Users\kamil\IdeaProjects\super_bech32m3\src\main\java\CheckSum.kt:35:24: Missing spacing before "{"
[ktlint] C:\Users\kamil\IdeaProjects\super_bech32m3\src\main\java\CheckSum.kt:37:43: Missing spacing before "{"
[ktlint] C:\Users\kamil\IdeaProjects\super_bech32m3\src\main\java\CheckSum.kt:40:9: Unexpected newline before "else"
[ktlint] C:\Users\kamil\IdeaProjects\super_bech32m3\src\main\java\CheckSum.kt:41:24: Unnecessary semicolon
[ktlint] C:\Users\kamil\IdeaProjects\super_bech32m3\src\main\java\CheckSum.kt:43:1: Unexpected blank line(s) before "}"
[ktlint] C:\Users\kamil\IdeaProjects\super_bech32m3\src\main\java\CheckSum.kt:99:1: Unexpected blank line(s) before "}"
[ktlint] C:\Users\kamil\IdeaProjects\super_bech32m3\src\main\java\CheckSum.kt:100:1: Needless blank line(s)
[ktlint] C:\Users\kamil\IdeaProjects\super_bech32m3\src\main\java\Decode.kt:19:73: Unexpected spacing before "("
[ktlint] C:\Users\kamil\IdeaProjects\super_bech32m3\src\main\java\Decode.kt:32:42: Unexpected spacing before "("
[ktlint] C:\Users\kamil\IdeaProjects\super_bech32m3\src\main\java\Decode.kt:34:48: Unexpected spacing before "("
[ktlint] C:\Users\kamil\IdeaProjects\super_bech32m3\src\main\java\Decode.kt:38:68: Unexpected spacing after "("
[ktlint] C:\Users\kamil\IdeaProjects\super_bech32m3\src\main\java\Decode.kt:42:88: Unexpected spacing before "("
[ktlint] C:\Users\kamil\IdeaProjects\super_bech32m3\src\main\java\Encode.kt:1:1: Wildcard import (cannot be auto-corrected)
[ktlint] C:\Users\kamil\IdeaProjects\super_bech32m3\src\main\java\InputProcess.kt:23:47: Missing space after //
[ktlint] C:\Users\kamil\IdeaProjects\super_bech32m3\src\main\java\InputProcess.kt:51:77: Missing space after //
[ktlint] C:\Users\kamil\IdeaProjects\super_bech32m3\src\main\java\InputProcess.kt:178:15: Missing spacing after "if"
[ktlint] C:\Users\kamil\IdeaProjects\super_bech32m3\src\main\java\InputProcess.kt:265:1: Needless blank line(s)
[ktlint] C:\Users\kamil\IdeaProjects\super_bech32m3\src\main\java\Main.kt:1:1: Missing space after //
[ktlint] C:\Users\kamil\IdeaProjects\super_bech32m3\src\main\java\Main.kt:6:1: Missing space after //
[ktlint] C:\Users\kamil\IdeaProjects\super_bech32m3\src\main\java\Main.kt:22:10: Missing spacing after "while"
[ktlint] C:\Users\kamil\IdeaProjects\super_bech32m3\src\main\java\Main.kt:23:11: Missing spacing after "if"
[ktlint] C:\Users\kamil\IdeaProjects\super_bech32m3\src\test\java\DecodeTest.kt:1:1: Unnecessary import
[ktlint] C:\Users\kamil\IdeaProjects\super_bech32m3\src\test\java\DecodeTest.kt:4:1: Unused import
[ktlint] C:\Users\kamil\IdeaProjects\super_bech32m3\src\test\java\DecodeTest.kt:6:26: Missing spacing before "{"
[ktlint] C:\Users\kamil\IdeaProjects\super_bech32m3\src\test\java\DecodeTest.kt:11:18: Missing spacing before "="
[ktlint] C:\Users\kamil\IdeaProjects\super_bech32m3\src\test\java\DecodeTest.kt:12:52: Missing space after //
[ktlint] C:\Users\kamil\IdeaProjects\super_bech32m3\src\test\java\DecodeTest.kt:23:13: Missing newline before ")"
[ktlint] C:\Users\kamil\IdeaProjects\super_bech32m3\src\test\java\DecodeTest.kt:32:13: Missing newline before ")"
[ktlint] C:\Users\kamil\IdeaProjects\super_bech32m3\src\test\java\DecodeTest.kt:41:13: Missing newline before ")"
[ktlint] C:\Users\kamil\IdeaProjects\super_bech32m3\src\test\java\DecodeTest.kt:50:13: Missing newline before ")"
[ktlint] C:\Users\kamil\IdeaProjects\super_bech32m3\src\test\java\EncodeTest.kt:1:1: File must end with a newline (\n)
[ktlint] C:\Users\kamil\IdeaProjects\super_bech32m3\src\test\java\EncodeTest.kt:1:1: Unnecessary import
```



```
[ktlint] C:\Users\kamil\IdeaProjects\super_bech32m3\src\test\java\EncodeTest.kt:5:1: Needless blank line(s)
[ktlint] C:\Users\kamil\IdeaProjects\super_bech32m3\src\test\java\EncodeTest.kt:9:29: Missing spacing before "{"
[ktlint] C:\Users\kamil\IdeaProjects\super_bech32m3\src\test\java\MainTests.kt:1:1: File must end with a newline (\n)
[ktlint] C:\Users\kamil\IdeaProjects\super_bech32m3\src\test\java\MainTests.kt:3:1: Wildcard import (cannot be auto-corrected)
[ktlint] C:\Users\kamil\IdeaProjects\super_bech32m3\src\test\java\MainTests.kt:25:20: Missing spacing after "catch"
[ktlint] C:\Users\kamil\IdeaProjects\super_bech32m3\src\test\java\MainTests.kt:69:1: Unexpected blank line(s) before "}"
[ktlint] C:\Users\kamil\IdeaProjects\super_bech32m3\src\test\java\ToolsTests.kt:1:1: File must end with a newline (\n)
[ktlint] C:\Users\kamil\IdeaProjects\super_bech32m3\src\test\java\ToolsTests.kt:6:26: Missing spacing before "{"
```

Snyk



Open Source Security - 1 vulnerability: 1 low
- pom.xml
  - L org.jetbrains.kotlin:kotlin-stdlib@1.5.10: Information Exposure

Code Security (disabled in Snyk.io)

Code Quality (disabled in Snyk.io)

Configuration Issues - No supported IaC files found

Container Vulnerabilities - No container images found

L Information Exposure

Vulnerability | CWE-378 | CVE-2020-29582 | CVSS 3.3 | SNYK-JAVA-ORGJETBRAINSKOTLIN-2393744

Vulnerable module:	org.jetbrains.kotlin:kotlin-stdlib
Introduced through:	org.jetbrains.kotlin:kotlin-stdlib-jdk8@1.5.10
Fixed in:	Not fixed
Exploit maturity:	Proof of Concept

Detailed paths

Introduced through:	groupId:super_bech32m@1.0-SNAPSHOT > org.jetbrains.kotlin:kotlin-stdlib-jdk8@1.5.10 > org.jetbrains.kotlin:kotlin-stdlib@1.5.10
Remediation:	none

Overview

org.jetbrains.kotlin:kotlin-stdlib is a None

Affected versions of this package are vulnerable to Information Exposure. A Kotlin application using `createTempDir` or `createTempFile` and placing sensitive information within either of these locations would be leaking this information in a read-only way to other users also on this system.

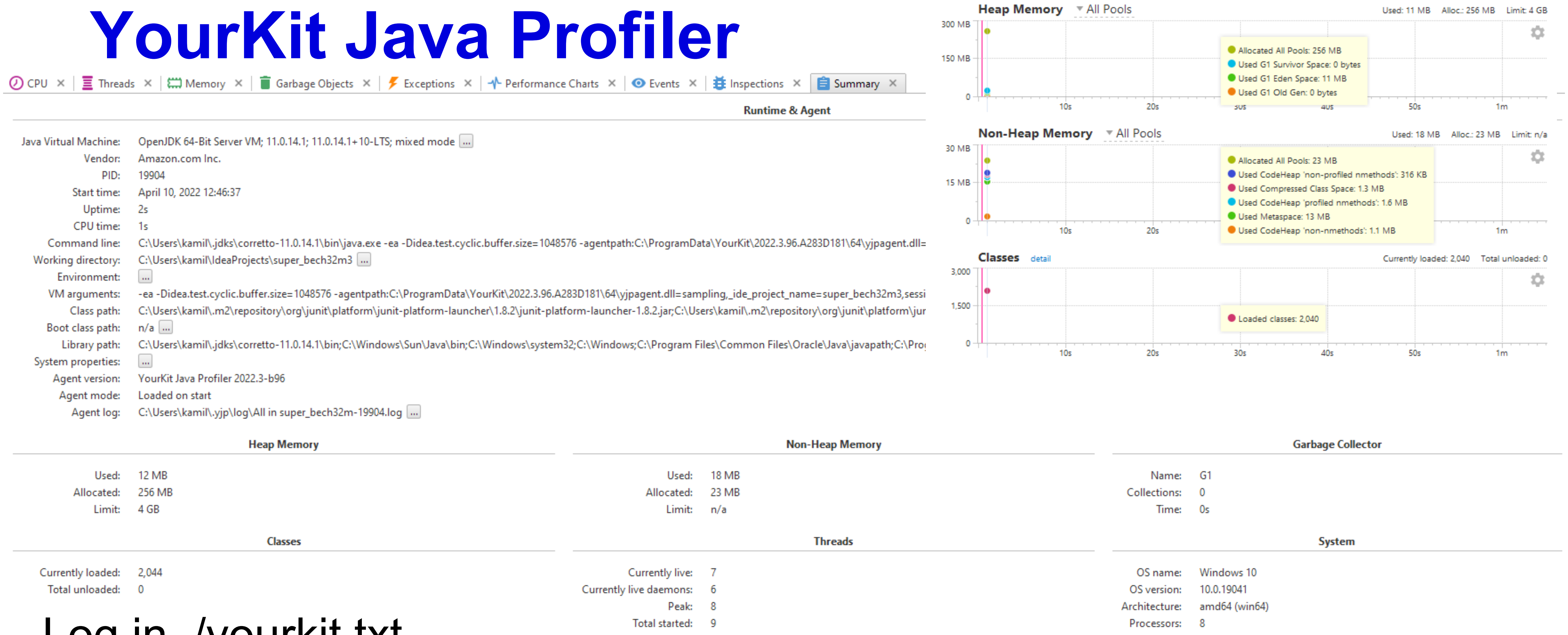
PoC by JLLeitschuh

```
package org.jlleitschuh.sandbox

import org.junit.jupiter.api.Test
import java.io.BufferedReader
import java.io.File
import java.io.IOException
import java.io.InputStreamReader
import java.nio.file.Files

class KotlinTempDirectoryPermissionCheck {
    @Test
    fun `kotlin check default directory permissions`() {
        val dir = createTempDir()
        runLS(dir.parentFile, dir) // Prints drwxr-xr-x
    }
```

Vulnerability:

Opening temporary files without appropriate measures or controls can leave the file, its contents and any function that it impacts vulnerable to attack.

YourKit Java Profiler



CPU ×
Threads ×
Memory ×
Garbage Objects ×
Exceptions ×
Performance Charts ×
Events ×
Inspections ×
Summary ×
Heap Memory
All Pools
Used: 11 MB Alloc.: 256 MB Limit: 4 GB
300 MB
150 MB
0
10s
20s
30s
40s
50s
1m
● Allocated All Pools: 256 MB
● Used G1 Survivor Space: 0 bytes
● Used G1 Eden Space: 11 MB
● Used G1 Old Gen: 0 bytes
Non-Heap Memory
All Pools
Used: 18 MB Alloc.: 23 MB Limit: n/a
30 MB
15 MB
0
10s
20s
1m
● Allocated All Pools: 23 MB
● Used CodeHeap 'non-profiled nmethods': 316 KB
● Used Compressed Class Space: 1.3 MB
● Used CodeHeap 'profiled nmethods': 1.6 MB
● Used Metaspace: 13 MB
● Used CodeHeap 'non-nmethods': 1.1 MB
Classes
detail
Currently loaded: 2,040 Total unloaded: 0
3,000
1,500
0
10s
20s
30s
40s
50s
1m
● Loaded classes: 2,040

Runtime & Agent

Java Virtual Machine:	OpenJDK 64-Bit Server VM; 11.0.14.1; 11.0.14.1+10-LTS; mixed mode ...
Vendor:	Amazon.com Inc.
PID:	19904
Start time:	April 10, 2022 12:46:37
Uptime:	2s
CPU time:	1s
Command line:	C:\Users\kamil\.jdks\corretto-11.0.14.1\bin\java.exe -ea -Didea.test.cyclic.buffer.size=1048576 -agentpath:C:\ProgramData\YourKit\2022.3.96.A283D181\64\yjpagent.dll=
Working directory:	C:\Users\kamil\IdeaProjects\super_bech32m3 ...
Environment:	...
VM arguments:	-ea -Didea.test.cyclic.buffer.size=1048576 -agentpath:C:\ProgramData\YourKit\2022.3.96.A283D181\64\yjpagent.dll=sampling,_ide_project_name=super_bech32m3,sessi
Class path:	C:\Users\kamil\.m2\repository\org\junit\platform\junit-platform-launcher\1.8.2\junit-platform-launcher-1.8.2.jar;C:\Users\kamil\.m2\repository\org\junit\platform\jur
Boot class path:	n/a ...
Library path:	C:\Users\kamil\.jdks\corretto-11.0.14.1\bin;C:\Windows\Sun\Java\bin;C:\Windows\system32;C:\Windows;C:\Program Files\Common Files\Oracle\Java\javapath;C:\Pro
System properties:	...
Agent version:	YourKit Java Profiler 2022.3-b96
Agent mode:	Loaded on start
Agent log:	C:\Users\kamil\.yjp\log\All in super_bech32m-19904.log ...

Heap Memory

Used:	12 MB
Allocated:	256 MB
Limit:	4 GB

Non-Heap Memory

Used:	18 MB
Allocated:	23 MB
Limit:	n/a

Garbage Collector

Name:	G1
Collections:	0
Time:	0s

Classes

Currently loaded:	2,044
Total unloaded:	0

Threads

Currently live:	7
Currently live daemons:	6
Peak:	8
Total started:	9

System

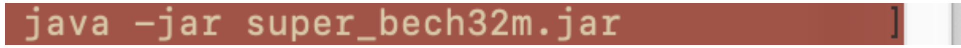
OS name:	Windows 10
OS version:	10.0.19041
Architecture:	amd64 (win64)
Processors:	8

Log in ./yourkit.txt

Usage of the tool

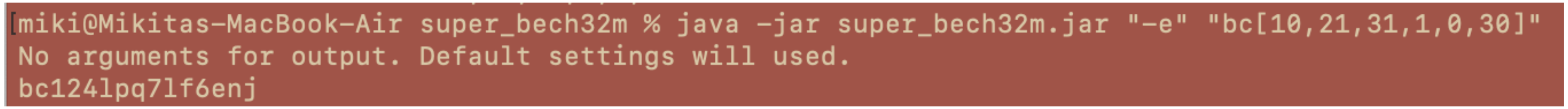
Provided file: super_bech32m.jar

It can be executed using terminal:



```
java -jar super_bech32m.jar
```

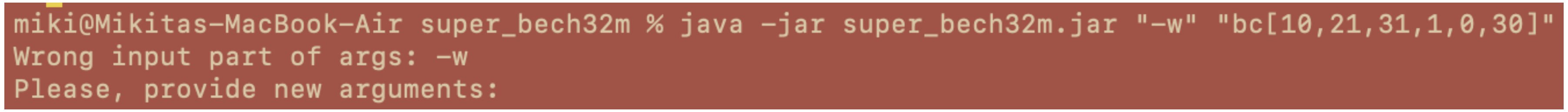
It can be run also with input arguments (listed with ““):



```
[miki@Mikitas-MacBook-Air super_bech32m % java -jar super_bech32m.jar "-e" "bc[10,21,31,1,0,30]"
No arguments for output. Default settings will used.
bc124lpq7lf6enj
```

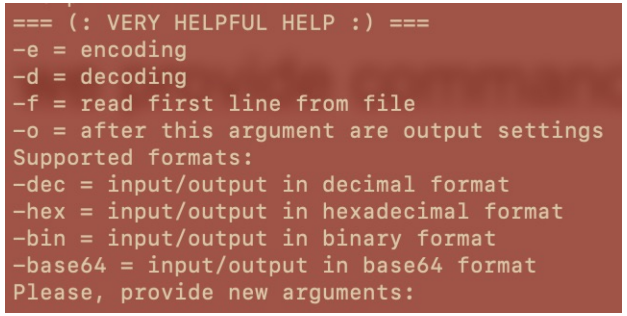
Usage of the tool

In case when no arguments provided program shows examples of usage and if something wrong print this part what is incorrect. And then ask for a new input.

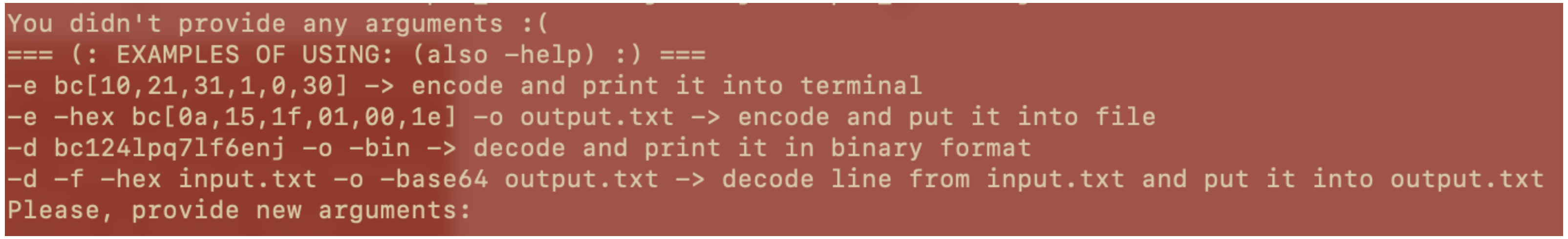


```
miki@Mikitas-MacBook-Air super_bech32m % java -jar super_bech32m.jar "-w" "bc[10,21,31,1,0,30]"
Wrong input part of args: -w
Please, provide new arguments:
```

Also we provide command –help which show list of all commands.



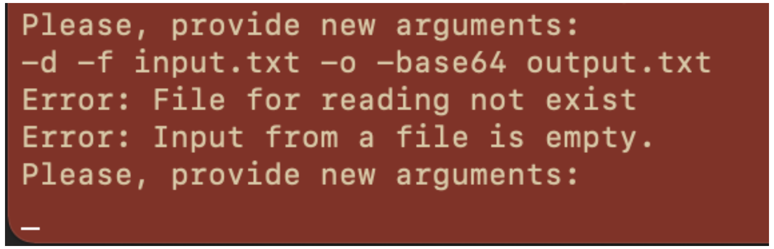
```
=== (: VERY HELPFUL HELP :) ===
-e = encoding
-d = decoding
-f = read first line from file
-o = after this argument are output settings
Supported formats:
-dec = input/output in decimal format
-hex = input/output in hexadecimal format
-bin = input/output in binary format
-base64 = input/output in base64 format
Please, provide new arguments:
```



```
You didn't provide any arguments :(
=== (: EXAMPLES OF USING: (also -help) :) ===
-e bc[10,21,31,1,0,30] -> encode and print it into terminal
-e -hex bc[0a,15,1f,01,00,1e] -o output.txt -> encode and put it into file
-d bc124lpq7lf6enj -o -bin -> decode and print it in binary format
-d -f -hex input.txt -o -base64 output.txt -> decode line from input.txt and put it into output.txt
Please, provide new arguments:
```

Usage of the tool

Logically program divide input into two parts which corresponds to input part and output part.



```
Please, provide new arguments:
-d -f input.txt -o -base64 output.txt
Error: File for reading not exist
Error: Input from a file is empty.
Please, provide new arguments:
_
```

For example, first part here:

–d (decode) –f (read first line from a file) input.txt (path to file or input string)

Seconds part (not compulsory):

-o (arguments for output) –base64 (format for output) output.txt (filepath for output)

Usage of the tool

For encoding request should look like:

HRP[data]

Example:

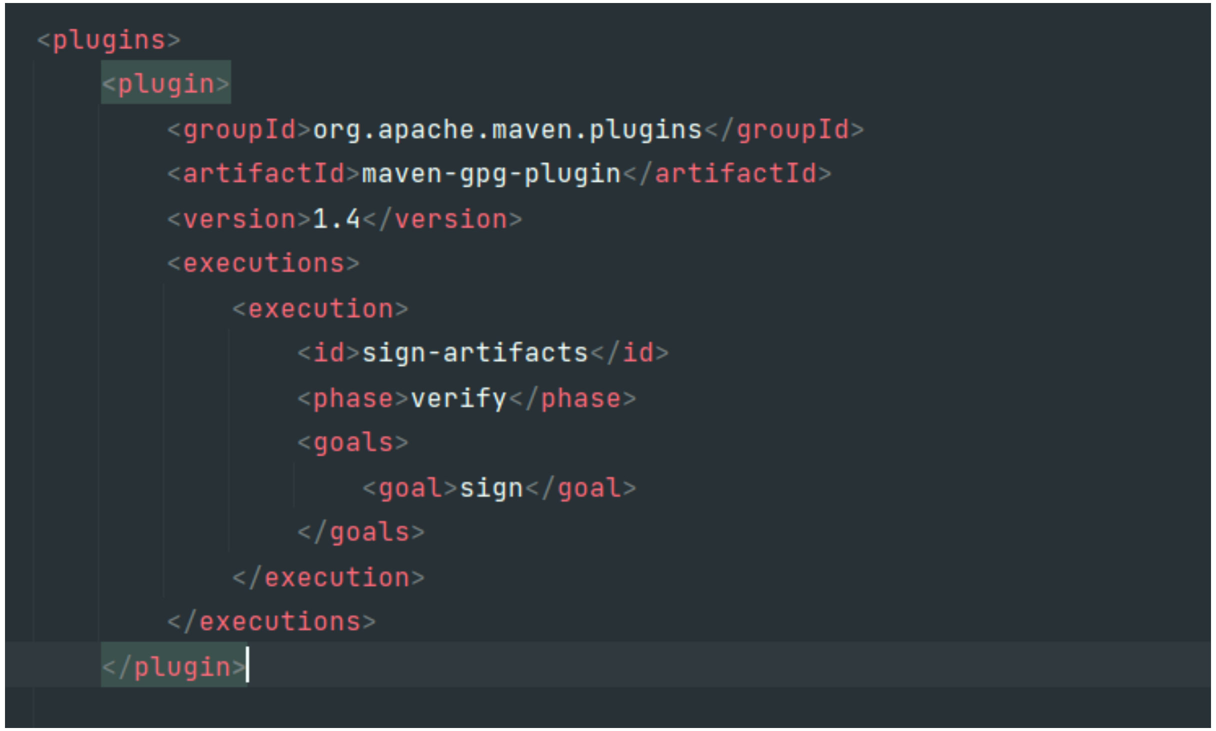
In dec : -e bc[10,20,31,0,1,2,3] (without spaces between data) (can be without flag –dec, because its by default)

In hex: -e -hex bc[0a,15,1f,01,00,1e]

In bin: -e -bin bc[01010,10101,11111,00001,00000,11110]

Release build with a GPG signature

- For signing final binary build was used maven plugin maven-gpg-plugin. These part has been added to the pom.xml file:



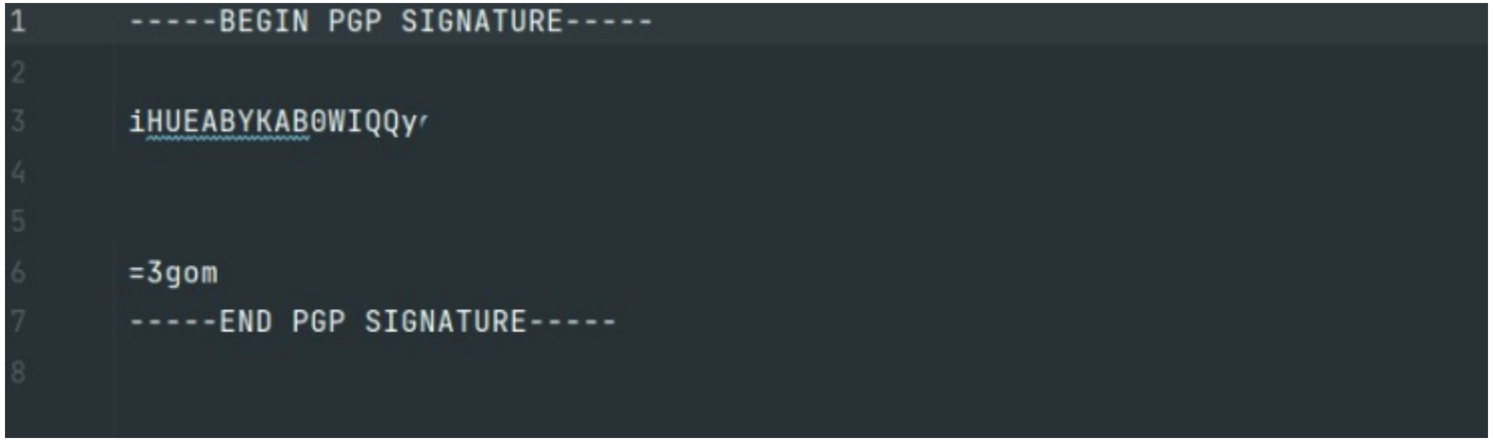
```xml
<plugins>
    <plugin>
        <groupId>org.apache.maven.plugins</groupId>
        <artifactId>maven-gpg-plugin</artifactId>
        <version>1.4</version>
        <executions>
            <execution>
                <id>sign-artifacts</id>
                <phase>verify</phase>
                <goals>
                    <goal>sign</goal>
                </goals>
            </execution>
        </executions>
    </plugin>
```

Release build with a GPG signature

- For creating signed binary build (.jar) is enough to call:

  mvn clean install

  Part of created GPG key (in .asc format).



```
-----BEGIN PGP SIGNATURE-----

iHUEABYKAB0WIQQy


=3gom
-----END PGP SIGNATURE-----

```