

[toc]

General

1. Group members

张望 11811026
王超逸 11811014
唐润哲 11710418
何宗翰 11812917
杨浩滨 11810816
张峻程 11810721

2. Group name and GitHub repository

Group name: WuYanGroup

Github repository URL: <https://github.com/cs304-spring2021/project-proposal-wuyangroup>

3. Project selection

Project chosen:

- JSONassert: <https://github.com/skyscreamer/JSONassert>
- JsonPath: <https://github.com/json-path/JsonPath>

Project Specification

JSONassert

Ease of use

Yes , screenshot as follows:

```
package hzh_test;

import org.json.JSONException;
import org.skyscreamer.jsonassert.JSONAssert;

public class HZH_A {
    public static void main(String[] args) throws JSONException {
        JSONAssert.assertEquals( expectedStr: "{a:12, b:34}", actualStr: "{b:34, a:12}", strict: true);
        JSONAssert.assertEquals( expectedStr: "{a:12, b:34}", actualStr: "{b:34, a:12}", strict: false);
        JSONAssert.assertEquals( expectedStr: "{a:12, b:34}", actualStr: "{b:34, a:33332}", strict: false);
    }
}
```

Run: HZH_A

"D:\2 Software\2 Software Install\20180904 jdk\bin\java.exe" "-javaagent:D:\2 Software\2 Software Install\2020103001_IDEA\IntelliJ IDEA 2020.2.3\lib\i
Exception in thread "main" java.lang.AssertionError: a
Expected: 12
got: 33332

at org.skyscreamer.jsonassert.JSONAssert.assertEquals(JSONAssert.java:417)
at org.skyscreamer.jsonassert.JSONAssert.assertEquals(JSONAssert.java:394)
at org.skyscreamer.jsonassert.JSONAssert.assertEquals(JSONAssert.java:336)
at hzh_test.HZH_A.main(HZH_A.java:10)

Process finished with exit code 1

The red-marked exception is the assertion by JSONassert, which indicates that the two JSON strings differ in field "a". And it is the case that JSONassert is put into use.

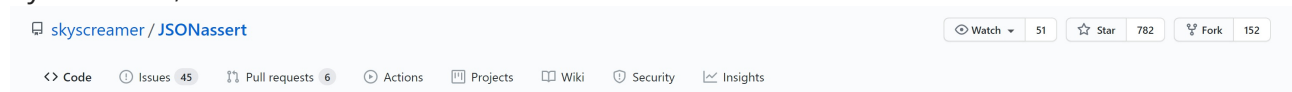
Existing Tests

Yes, there are some test cases in

<https://github.com/skyscreamer/JSONassert/tree/master/src/test>

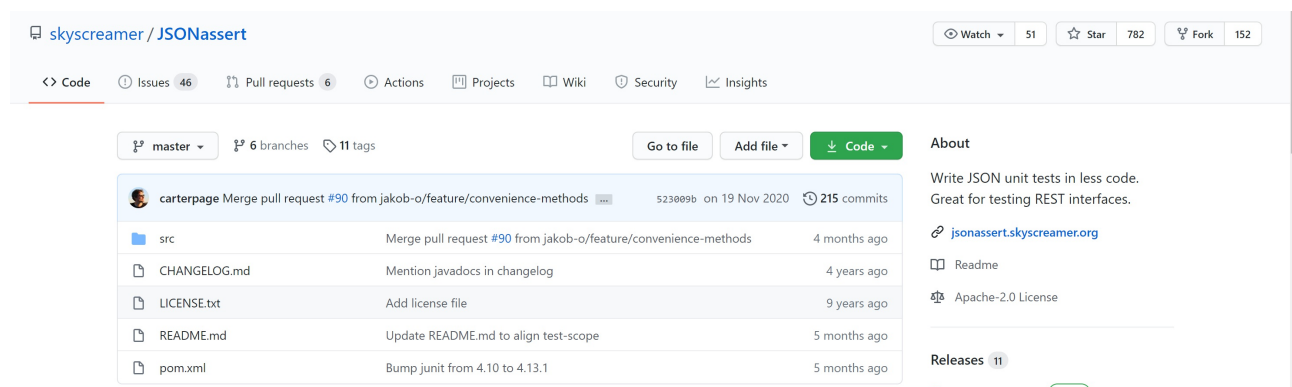
Popularity

By 2021/3/12, there has been 782 stars.



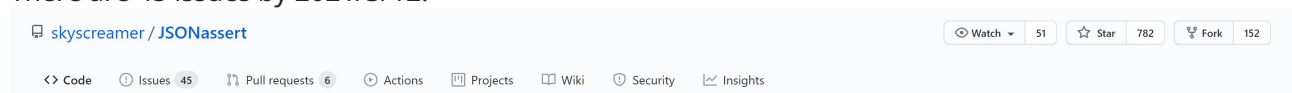
Actively Maintained

The latest commit is on Nov 19, 2020.



Number of open GitHub issues

There are 45 issues by 2021/3/12.



Contributing Guidelines

Yes, available at <http://jsonassert.skyscreamer.org/>

Contact

This is open source so if you want to help out whether by submitting code, design, suggestions, feedback, or feature requests, we appreciate whatever you can contribute. Contact us at jsonassert-dev@skyscreamer.org with questions or ideas.

Diversity of team members

Name	Role
王超逸	Leader
张望	Developer
唐润哲	Developer
何宗翰	Developer (Contribution guidelines & code review)

杨浩滨 Tester

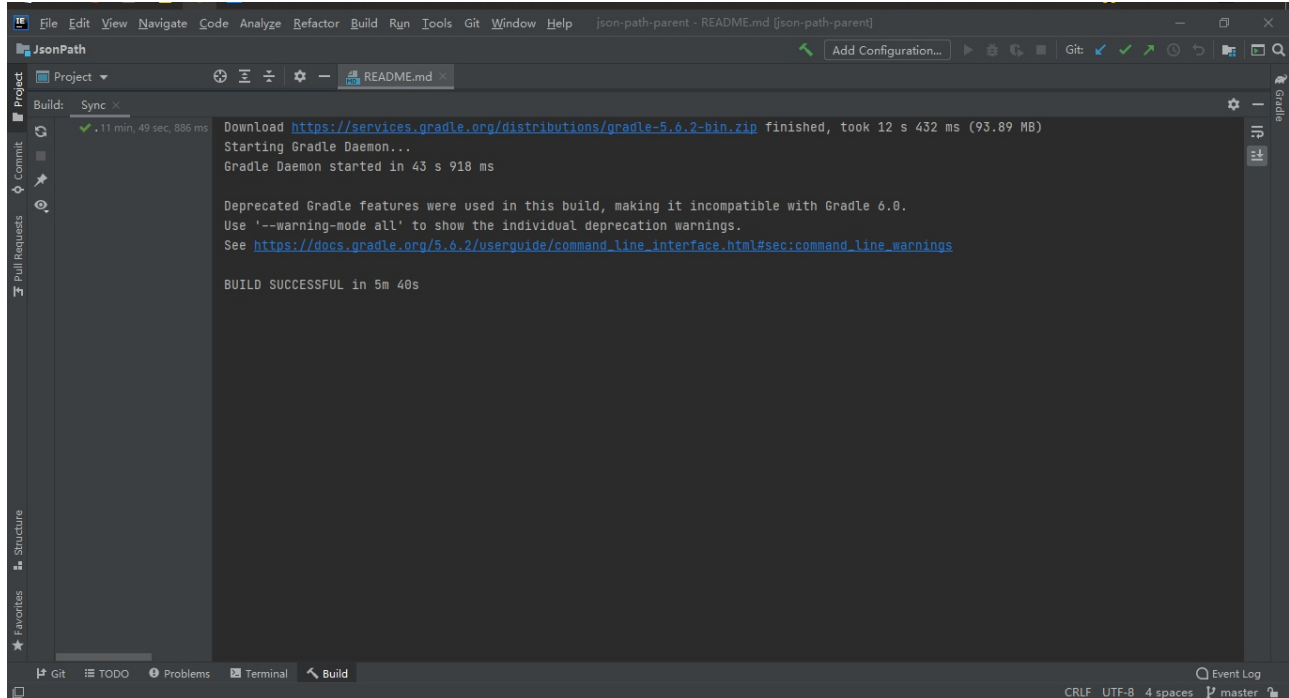
张峻程 Developer & Documentation (JavaDoc)

Link to issues	Type of issue (Bug/Feature)	Estimated Time to fix each issue	Number of people for fix this issue	Estimated Difficulty
https://github.com/skyscreamer/JSONassert/issues/130	Bug	3	2	4
https://github.com/skyscreamer/JSONassert/issues/127	Bug	3	2	4
https://github.com/skyscreamer/JSONassert/issues/113	Bug	3	2	4
https://github.com/skyscreamer/JSONassert/issues/114	Feature	2	2	2
https://github.com/skyscreamer/JSONassert/issues/115	Bug	2	2	2
https://github.com/skyscreamer/JSONassert/issues/107	Bug	2	2	2
https://github.com/skyscreamer/JSONassert/issues/108	Bug	3	2	3
https://github.com/skyscreamer/JSONassert/issues/106	Feature	3	2	3
https://github.com/skyscreamer/JSONassert/issues/85	Bug	5	1	3
https://github.com/skyscreamer/JSONassert/issues/75	Feature	2	2	2

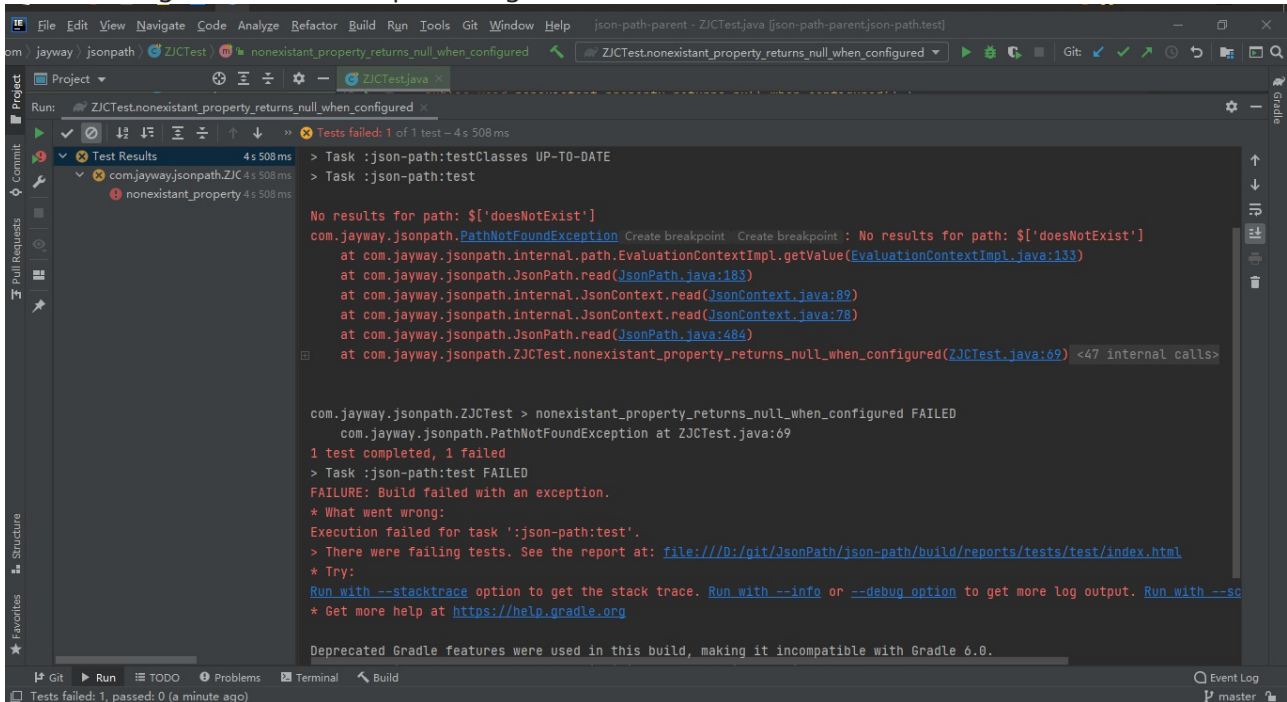
JSONPath

Ease of use

Yes , screenshot as follows:



The following is the result of reproducing an issue.



The screenshot shows an IDE window with a test run failure. The test is `com.jayway.jsonpath.ZJCTest.nonexistent_property_returns_null_when_configured`. The failure message is:

```
No results for path: $['doesNotExist']
com.jayway.jsonpath.PathNotFoundException: No results for path: $['doesNotExist']
    at com.jayway.jsonpath.internal.path.EvaluationContextImpl.getValue(EvaluationContextImpl.java:133)
    at com.jayway.jsonpath.JsonPath.read(JsonPath.java:183)
    at com.jayway.jsonpath.internal.JsonContext.read(JsonContext.java:82)
    at com.jayway.jsonpath.internal.JsonContext.read(JsonContext.java:78)
    at com.jayway.jsonpath.JsonPath.read(JsonPath.java:484)
    at com.jayway.jsonpath.ZJCTest.nonexistent_property_returns_null_when_configured(ZJCTest.java:69) <47 internal calls>
```

The test results summary shows:

```
com.jayway.jsonpath.ZJCTest > nonexistent_property_returns_null_when_configured FAILED
com.jayway.jsonpath.PathNotFoundException at ZJCTest.java:69
1 test completed, 1 failed
> Task :json-path:test FAILED
FAILURE: Build failed with an exception.
* What went wrong:
Execution failed for task ':json-path:test'.
> There were failing tests. See the report at: file:///D:/git/JsonPath/json-path/build/reports/tests/test/index.html
* Try:
Run with --stacktrace option to get the stack trace. Run with --info or --debug option to get more log output. Run with --sc
* Get more help at https://help.gradle.org
```

At the bottom, a message states: "Deprecated Gradle features were used in this build, making it incompatible with Gradle 6.0."

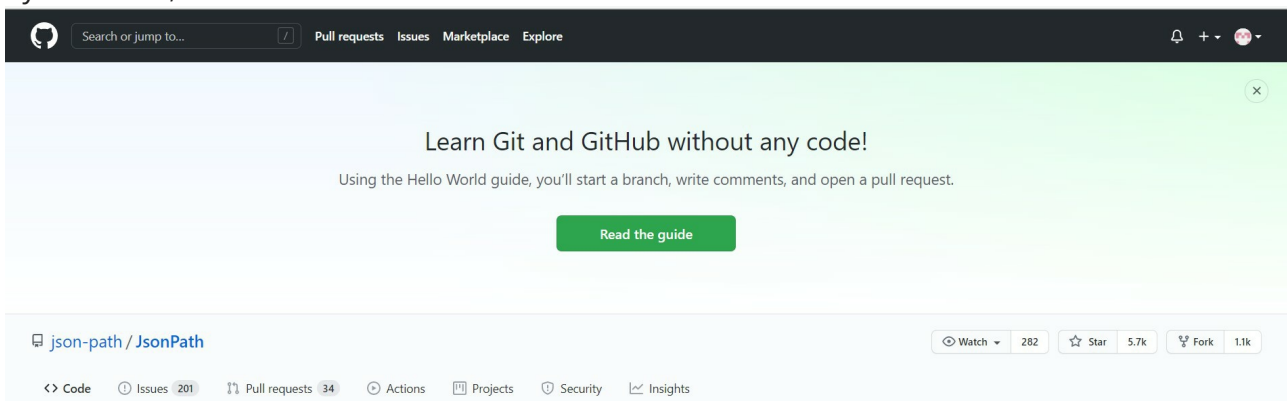
Existing Tests

Yes , there are some test cases in

<https://github.com/json-path/JsonPath/tree/master/json-path-web-test>

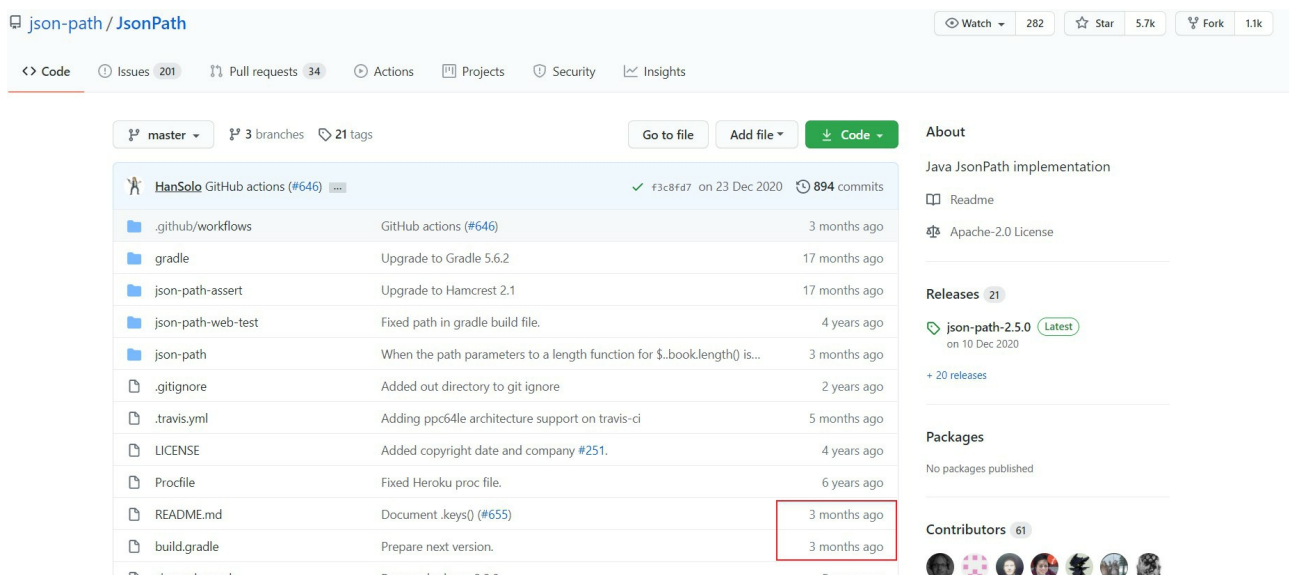
Popularity

By 2021/3/12,there has been 5.7k stars.



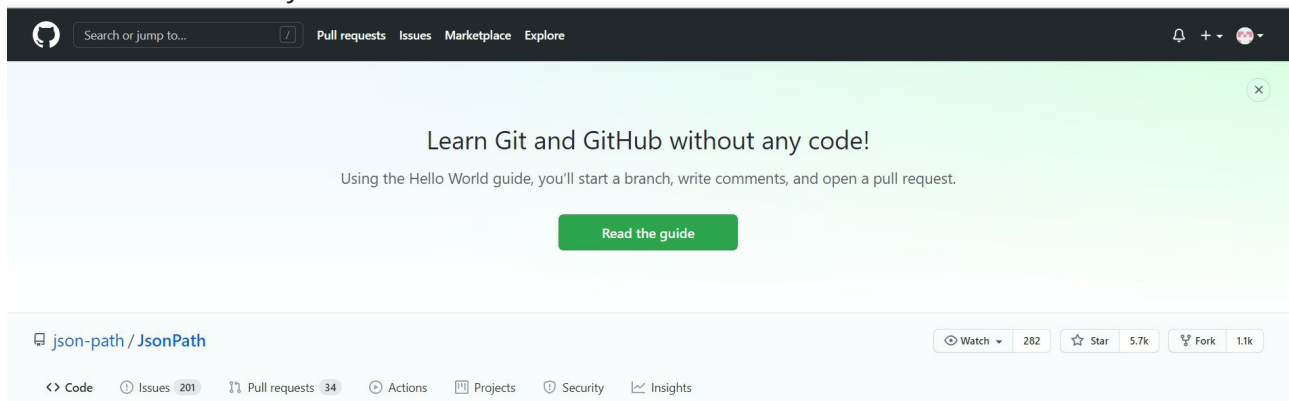
Actively Maintained

The latest commit is on Dec 23, 2020.



Number of open GitHub issues

There are 201 issues by 2021/3/12.



Contributing Guidelines

No, it does not have contributing guidelines.

Diversity of team members

Name	Role
王超逸	Leader
张望	Developer
唐润哲	Developer
何宗翰	Developer (Contribution guidelines & code review)
杨浩滨	Tester
张峻程	Developer & Documentation (JavaDoc)

Link to issues	Type of issue (Bug/Feature)	Estimated Time to fix each issue	Number of people for fix this issue	Estimated Difficulty
https://github.com/json-path/JsonPath/issues/628	Bug	3	2	3
https://github.com/json-path/JsonPath/issues/526	Bug	3	2	3

https://github.com/json-path/JsonPath/issues/620	Bug	3	2	3
https://github.com/json-path/JsonPath/issues/395	Bug	3	2	3
https://github.com/json-path/JsonPath/issues/356	Bug	3	2	3
https://github.com/json-path/JsonPath/issues/273	Bug	3	2	3
https://github.com/json-path/JsonPath/issues/174	Bug	3	2	3
https://github.com/json-path/JsonPath/issues/629	Bug	3	2	3
https://github.com/json-path/JsonPath/issues/623	Feature	3	2	3

backup

find-sec-bugs

Ease of use

Yes , screenshot as follows:

The screenshot shows the Eclipse IDE interface. The top part displays the 'XmlDecodeUtil.java' file with the following code:

```
1 package testcode.xmldecoder;
2
3 import java.beans.XMLDecoder;
4
5 public class XmlDecodeUtil {
6
7     public static Object handleXml(InputStream in) {
8         XMLDecoder d = new XMLDecoder(in);
9         try {
10             Object result = d.readObject();
11             return result;
12         } finally {
13             d.close();
14         }
15     }
16 }
```

The 'Bug Explorer' on the left shows a list of bugs. The selected bug is 'Its not safe to use an XMLDecoder to p...'. The 'Bug Info' tab on the right shows the 'Vulnerable Code' and the 'Solution'.

Vulnerable Code:

```
XMLDecoder d = new XMLDecoder(in);
try {
    Object result = d.readObject();
}
[...]
```

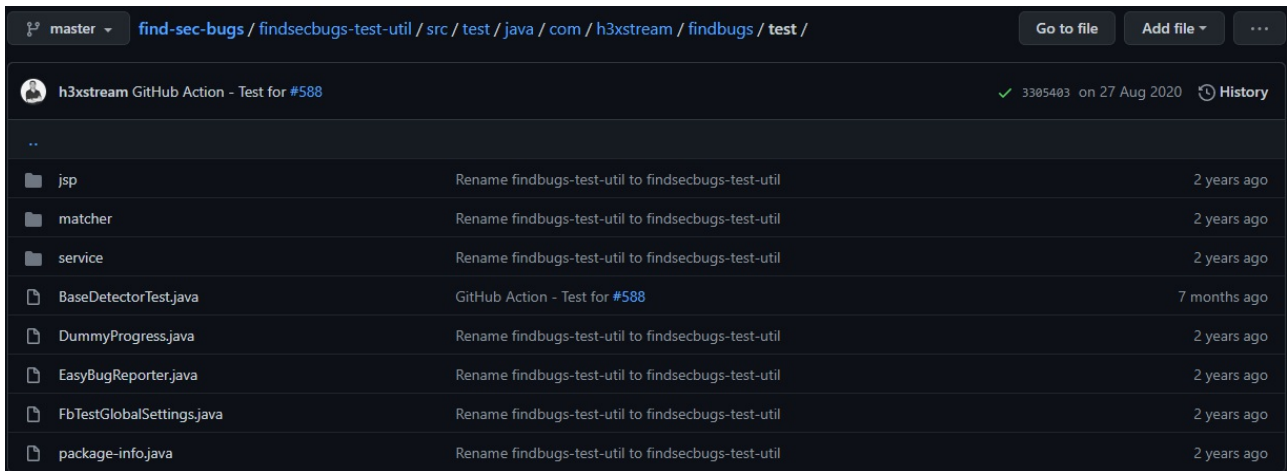
Solution:
The solution is to avoid using XMLDecoder to parse content from an untrusted source.

The bottom part of the screenshot shows a terminal window with the following output:

```
[INFO] Tests run: 327, Failures: 0, Errors: 0, Skipped: 0, Time elapsed: 226.046 s - in TestSuite
[INFO] Results:
[INFO] Tests run: 327, Failures: 0, Errors: 0, Skipped: 0
[INFO] --- maven-antrun-plugin:1.3:run (ant-magic) @ findsecbugs-plugin ---
[INFO] Executing tasks
[copy] Copying 4 files to /home/younge/Desktop/find-sec-bugs/findsecbugs-plugin/target/classes
[INFO] Executed tasks
[INFO] --- maven-jar-plugin:3.0.2:jar (default-jar) @ findsecbugs-plugin ---
[INFO] Building jar: /home/younge/Desktop/find-sec-bugs/findsecbugs-plugin/target/findsecbugs-plugin-1.12.0-SNAPSHOT.jar
[INFO] --- license-maven-plugin:2.11:check (regen_lgpl) @ findsecbugs-plugin ---
[INFO] Checking licenses...
[INFO] --- maven-install-plugin:2.4:install (default-install) @ findsecbugs-plugin ---
[INFO] Installing /home/younge/Desktop/find-sec-bugs/findsecbugs-plugin/target/findsecbugs-plugin-1.12.0-SNAPSHOT.jar
[INFO] Installing /home/younge/Desktop/find-sec-bugs/findsecbugs-plugin/pom.xml to /home/younge/.m2/repository/org/owasp/findsecbugs-plugin/1.12.0-SNAPSHOT/pom.xml
[INFO] -----
[INFO] Reactor Summary for OWASP Find Security Bugs root 1.12.0-SNAPSHOT:
[INFO] OWASP Find Security Bugs root ..... SUCCESS [ 0.743 s]
[INFO] FindSecBugs Test Utility ..... SUCCESS [ 2.048 s]
[INFO] Find Security Bugs Samples Dependencies ..... SUCCESS [ 1.389 s]
[INFO] Find Security Bugs Samples Kotlin ..... SUCCESS [ 5.060 s]
[INFO] Find Security Bugs Samples Java ..... SUCCESS [ 1.475 s]
[INFO] Find Security Bugs Samples JSP ..... SUCCESS [ 1.513 s]
[INFO] OWASP Find Security Bugs Plugin ..... SUCCESS [03:49 min]
[INFO] -----
[INFO] BUILD SUCCESS
[INFO] -----
[INFO] Total time: 04:01 min
[INFO] Finished at: 2021-03-11T07:56:32-08:00
[INFO] -----
```

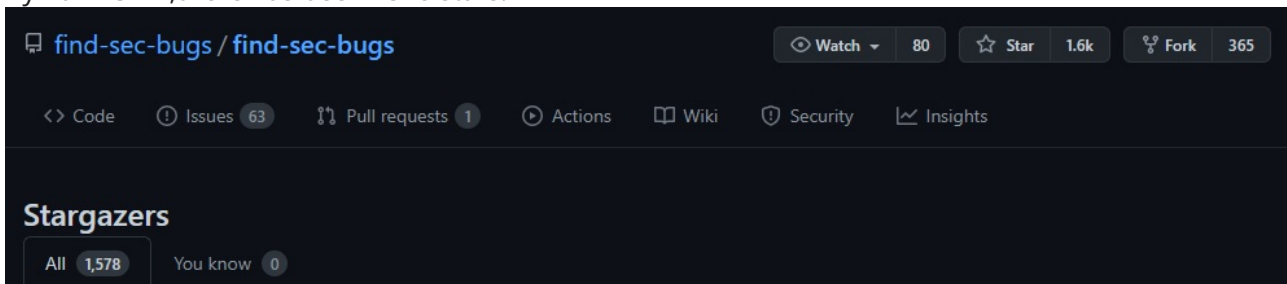
Existing Tests

Yes, there are some test cases in <https://github.com/find-sec-bugs/find-sec-bugs/tree/master/findsecbugs-test-util/src/test/java/com/h3xstream/findbugs/test>, as the screenshot:
























Popularity

By 2021/3/11, there has been 1578 stars.



Actively Maintained

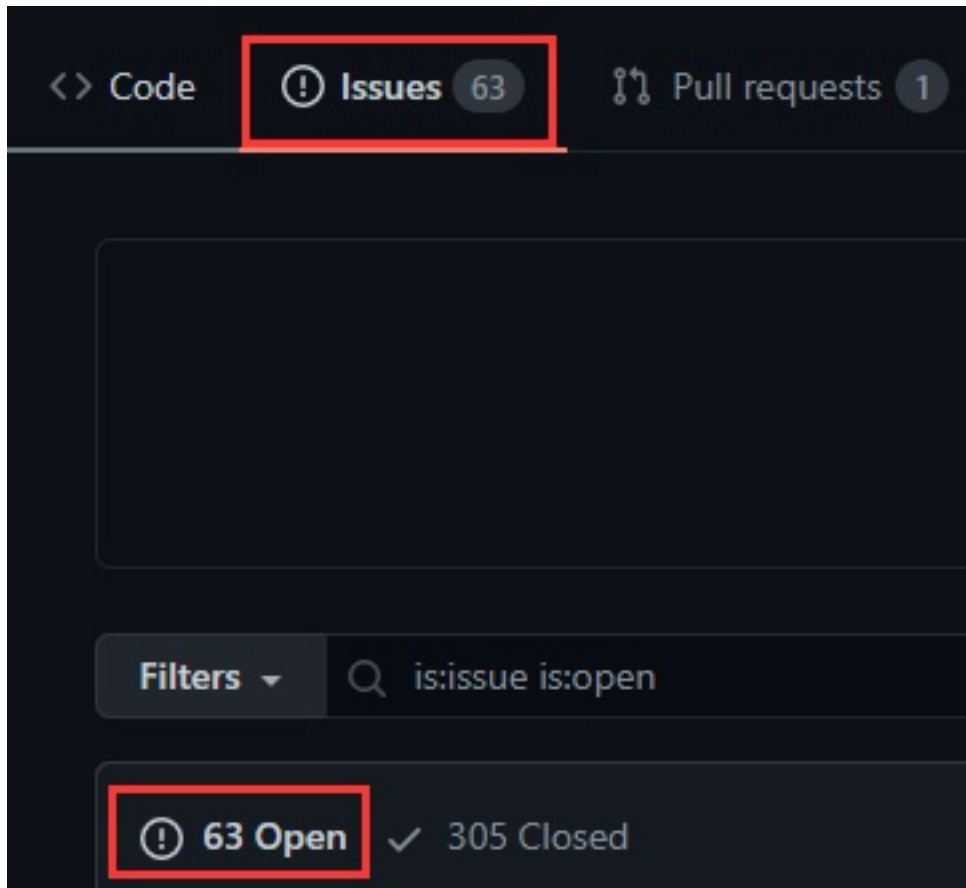
The latest commit is on 2 Feb.

	h3xstream Merge pull request #621 from pmlopes/feature/add-vertx-oauth-and-csrf ...		 fa7f7c4 on 2 Feb	 1,246 commits
	.github	Update codeql-analysis.yml		5 months ago
	cli	Change --version-list to -V to support busybox version of the sort co...		7 months ago
	findsebugs-plugin	Add support for Vert.x web Oauth2 + CSRF handlers		last month
	findsebugs-samples-deps	Add support for Vert.x web Oauth2 + CSRF handlers		last month
	findsebugs-samples-java	Add support for Vert.x web Oauth2 + CSRF handlers		last month
	findsebugs-samples-jsp	Preparing the next working version		4 months ago
	findsebugs-samples-kotlin	Preparing the next working version		4 months ago
	findsebugs-test-util	Preparing the next working version		4 months ago
	website	Update JQuery to 3.5.1 (Make dependabot happy)		9 months ago
	.gitignore	added EnabledExtensionsInApacheXmlRpcDetector and mocks		2 years ago
	.travis.yml	This should speed up the build process.		17 months ago
	CHANGELOG.md	Update auto-generated CHANGELOG..		4 years ago
	CONTRIBUTING.md	Minor change to contribution file		4 years ago
	LGPL-3.0-header.txt	Remove the year in the file header. 2015+ compliant		6 years ago
	LGPL-3.0.txt	License files		9 years ago
	LICENSE	License file added (duplicate)		4 years ago
	README.md	Move the badges lower to avoid overflow		17 months ago
	pom.xml	Preparing the next working version		4 months ago

Number of open GitHub issues

There are 63 issues, 18 tags of bugs by 2021/3/11.

Issue:



Labeled as bug:

18 Open ✓ 76 Closed

Filter by label

Filter labels

Unlabeled

✓ bug

blocker

canceled

description

duplicate

enhancement

false-negative

false-positive

Use **alt** + **click/return** to exclude labels.

Interface sinks not working? **bug** **false-negative**
#611 opened on 21 Oct 2020 by Quiark

Not able to run findSecBugs via CLI on macOS **blocker** **bug**
#606 opened on 12 Oct 2020 by hiteshgargavid ↗ version-1.11.0

Hibernate SQLi not discovered **bug** **false-negative**
#597 opened on 4 Sep 2020 by pauser0000001

findsecbugs threads hang in java.util.WeakHashMap.get(WeakHashMapV
#595 opened on 3 Sep 2020 by mhn0t

SSRF issue link doesn't exist **bug**
#564 opened on 27 Jun 2020 by davewichers

CorsRegistryCORSDescriptor crashes with NullPointerException **bug**
#540 opened on 16 Jan 2020 by simon-greatrix

There are numerous flags in the cli that do not work **bug**
#533 opened on 17 Nov 2019 by ghost

Random chance of detection for some files in Juliet 1.3 CWE89 SQL Injection
#456 opened on 28 Feb 2019 by mamik95

[1.8.0] INFORMATION_EXPOSURE_THROUGH_AN_ERROR_MESSAGE false positive **bug** **false-positive**
#411 opened on 29 Jun 2018 by boris-petrov

Android SQL Injection detection not working **bug** **question**
#366 opened on 1 Feb 2018 by jyotigajrani

SECRD ReDOS false-positive **bug** **false-positive** **good first issue** **hacktoberfest**
#335 opened on 23 Aug 2017 by archmageirvine

invokedynamic from lambdas produces wrong missing class warnings **bug**
#332 opened on 21 Aug 2017 by Vampire

UnvalidatedRedirectDetector "Location" LDC issue **bug** **false-negative**
#249 opened on 30 Dec 2016 by plr0man

False positive if XML parser is configured in separate method **bug**
#245 opened on 20 Dec 2016 by eoftedal

INSECURE_COOKIE detector can be fooled by creating two or more cookies **bug** **false-positive**
#182 opened on 16 Mar 2016 by jborgland

find-sec-bugs plugin generates many exceptions when hitting a lengthy method **bug**
#175 opened on 16 Feb 2016 by mkienerb

False positive for INSECURE_COOKIE **bug** **false-positive**
#164 opened on 12 Jan 2016 by kutzi

WEAK_FILENAMEUTILS does not check context **bug** **false-positive**
#141 opened on 14 Dec 2015 by agabrys

Contributing Guidelines

<https://github.com/find-sec-bugs/find-sec-bugs/blob/master/CONTRIBUTING.md>

Diversity of team members 分工 这个讨论一下

Name	Role
王超逸	Leader
张望	Developer
唐润哲	Developer
何宗翰	Developer (Contribution guidelines & code review)
杨浩滨	Tester
张峻程	Developer & Documentation (JavaDoc)

找想fix的issue

Link to issues	Type of issues(Bug/Feature)	Estimated Time to fix each issue	Number of people for fix this issue members for each issue	Estimated Difficulty(in a scale of 1-5, 1 means very easy to fix and 5 means very difficult to fix)
----------------	-----------------------------	----------------------------------	--	---

querydsl

Ease of use: Have you successfully compile?

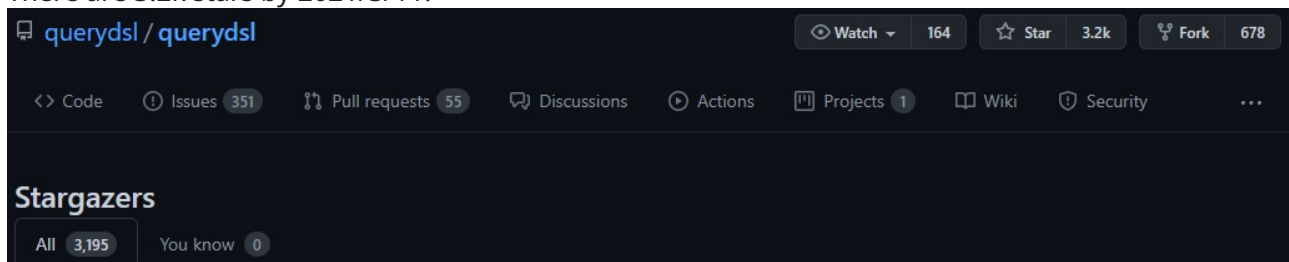
Yes , it is very easy to get Querydsl releases releases via public Maven repositories.

Existing Tests: Do the project contain some test case?

Yes , there are some test case in <https://github.com/querydsl/querydsl/tree/master/querydsl-sql/src/test>

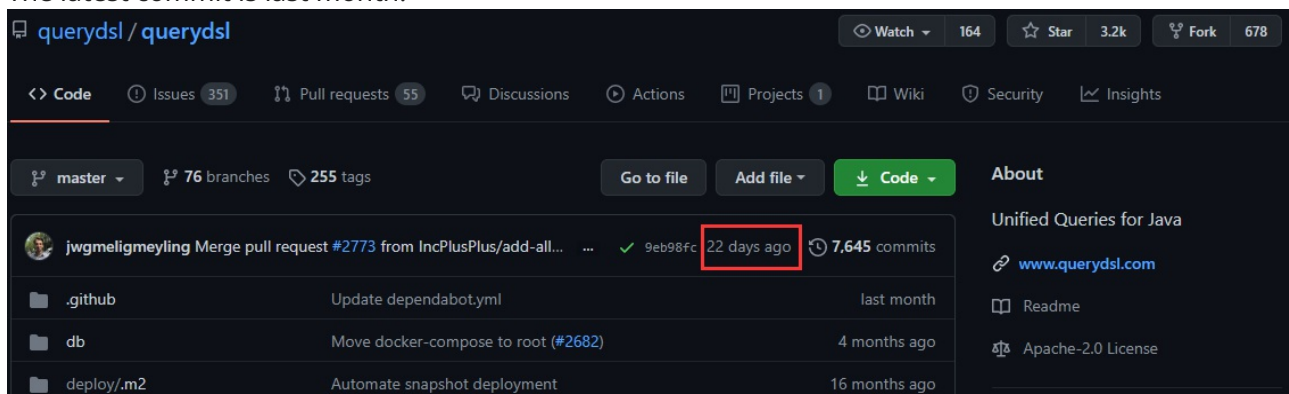
Popularity: How many stars does the project have in GitHub? (2 points)

There are 3.2k stars by 2021/3/11.



Actively Maintained: When is the latest commits to the project? Please make sure that the latest commits were within a year

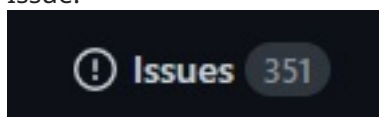
The latest commit is last month.



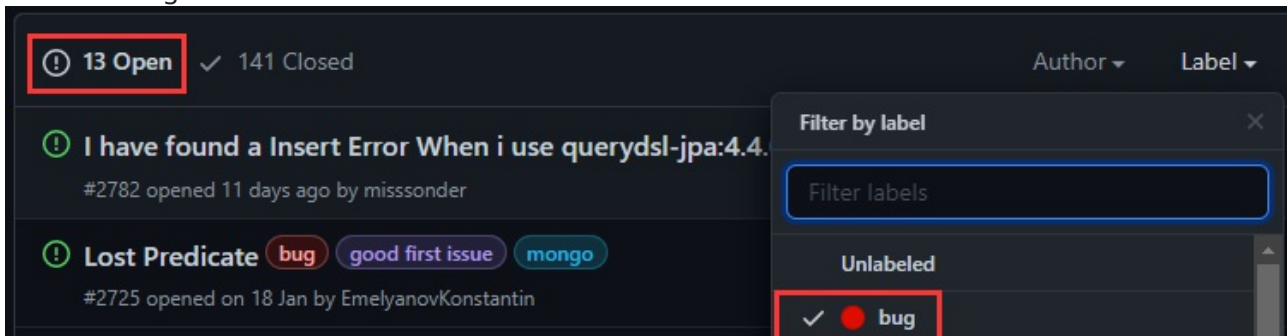
Number of open GitHub issues: How many open issues the project have?

there are 351 issues, 13 tags of bugs, 43 tags of feature by 2021/3/11.

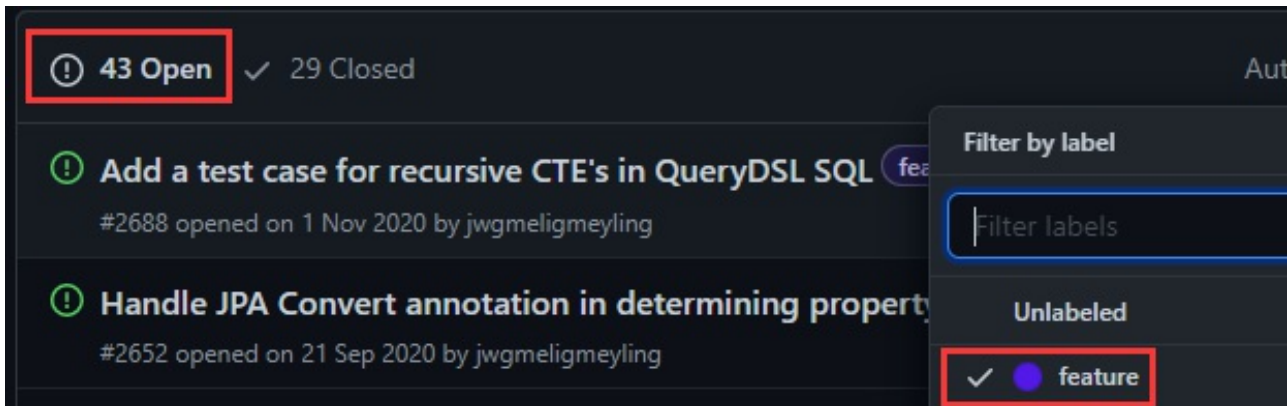
Issue:



Labled as bug:



Labled as feature:



Does the project have any contributing guidelines?

No, but how to contribute is mentioned in README.md

Link to issues	Type of issues(Bug/Feature)	Estimated Time to fix each issue	Number of people for fix this issue members for each issue	Estimated Difficulty(in a scale of 1-5, 1 means very easy to fix and 5 means very difficult to fix)
----------------	-----------------------------	----------------------------------	--	---