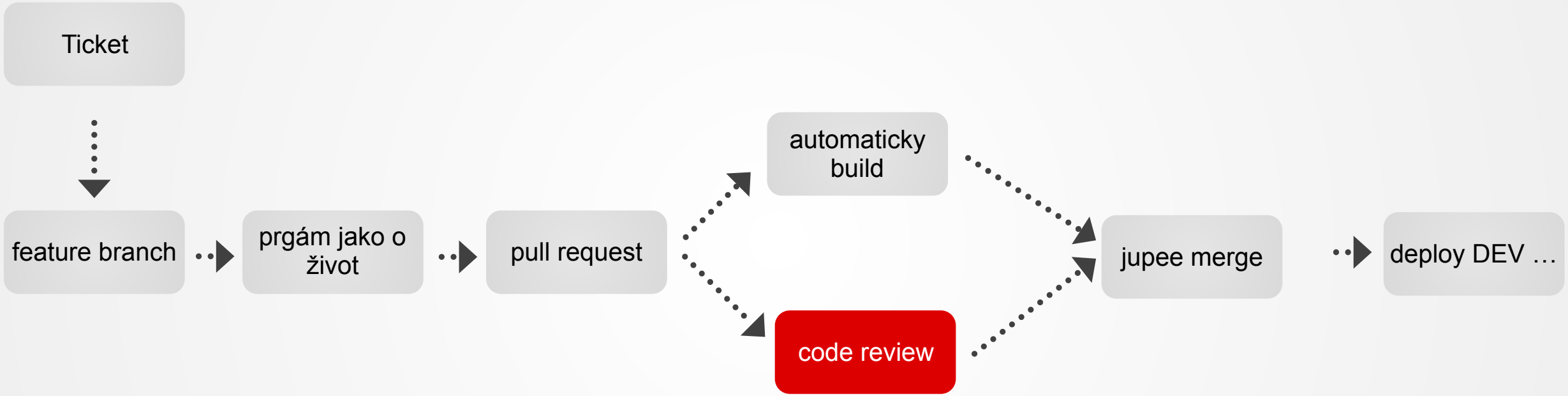
SonarQube

- statická analýza kódu a její zapojení v CI

Babu Červenková
Big Data developer - Java
Fulltext - Robot tým

SEZNAM.CZ

Vývojový proces (zjednodušeně)



Statická analýza = analýza chyb/nekonzistencí kódu bez jeho spuštění

přístup ke statickým parametrům

názvy proměnných

použití lambd místo vložených tříd

nepoužívat třídy ze sun.* balíku

String literál by měl být vlevo při volání equals

standardy

nepoužívat URL.hashCode

zastaralý kód

abstraktní třída by měla začínat Abstract*

deprecated metoda by měla mít Javadoc s vysvětlením

nepoužívat deprecated metody

statické proměnné jsou vždy upper case

podmínka je vždy true/false

nepoužívat octalový zápis čísel

nepoužité proměnné

hlavičky souborů

taby vs mezery

zbytečný cast

public metody mají Javadoc

mrtvý kód

Junit assertion používat jen pro testy

formátování

třída s názvem *Exception nedědí od Exception

zakomentované kusy kódu

nedostupné bloky kódu

bad practices

prázdný řádek na konci souboru

proměnná je vždy null

zapomenuté importy

hvězdičkové * importy

deklarace throws RuntimeException

volání finalize

abstraktní třída nesmí implementovat equals a hashCode

stejné soubory

duplikované parametry ve volání metod

počet znaků na řádek

velká komplexita jedné metody

memory leak

toString() může vrátit null

nepoužívat Thread.sleep v testech

duplicity

čitelnost

chyby

cyklomatická složitost

if else na více řádků

skoro stejné metody

copy&paste bloky

počet parametrů metody nebo konstruktoru

neuzavřená spojení

metoda neloguje exception

switch case max. 10

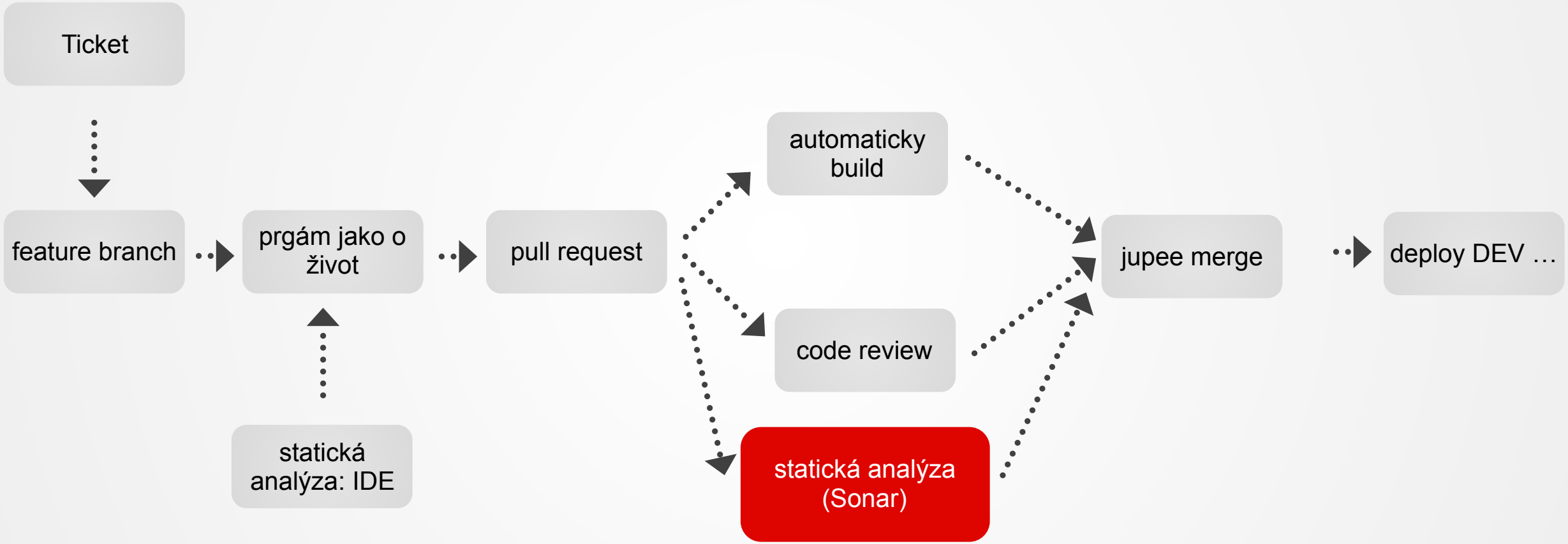
dokumentace pro Class

nepoužívat enum jako kompozitní klíč

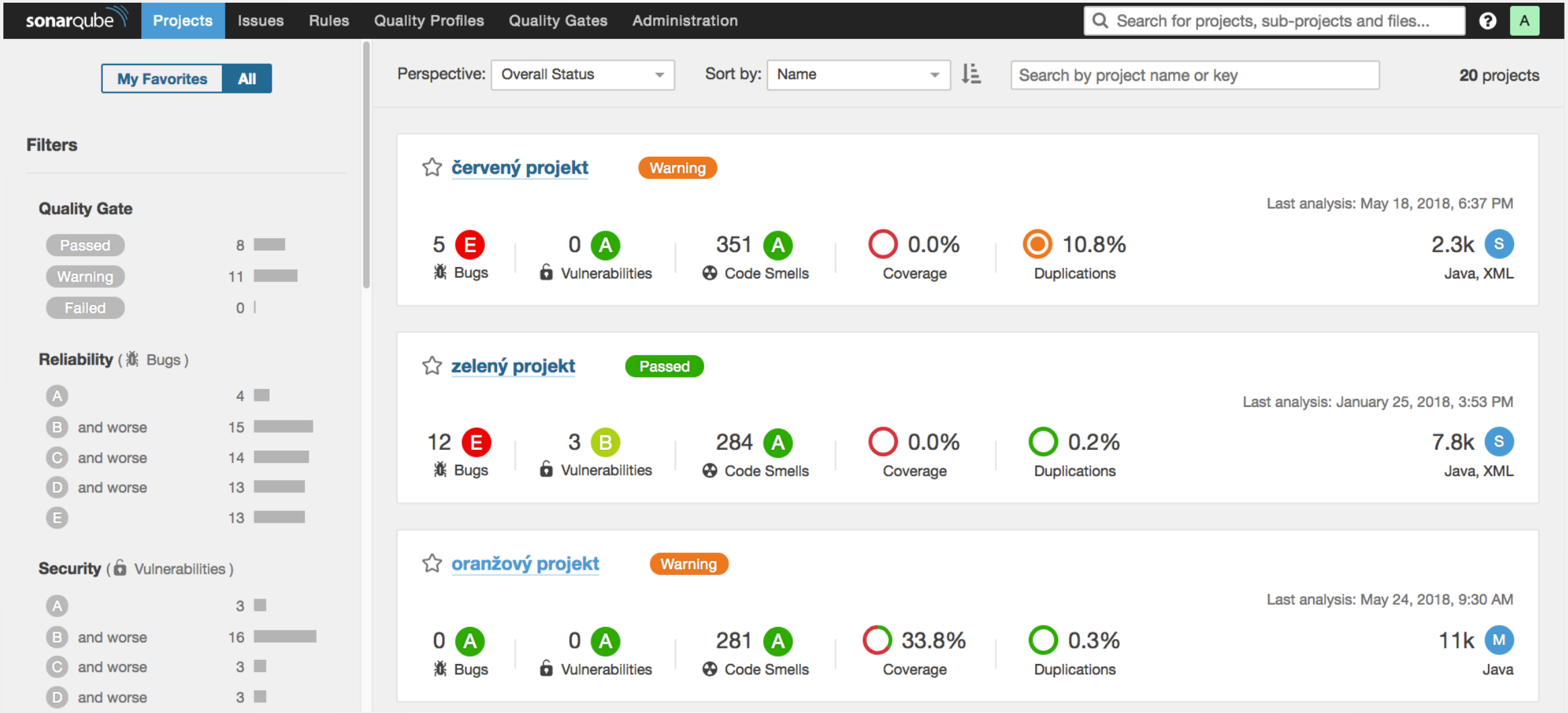
jméno class by nemělo být stejné jako jméno vnitřních proměnných

finally blok nesmí vyhazovat vyjímku

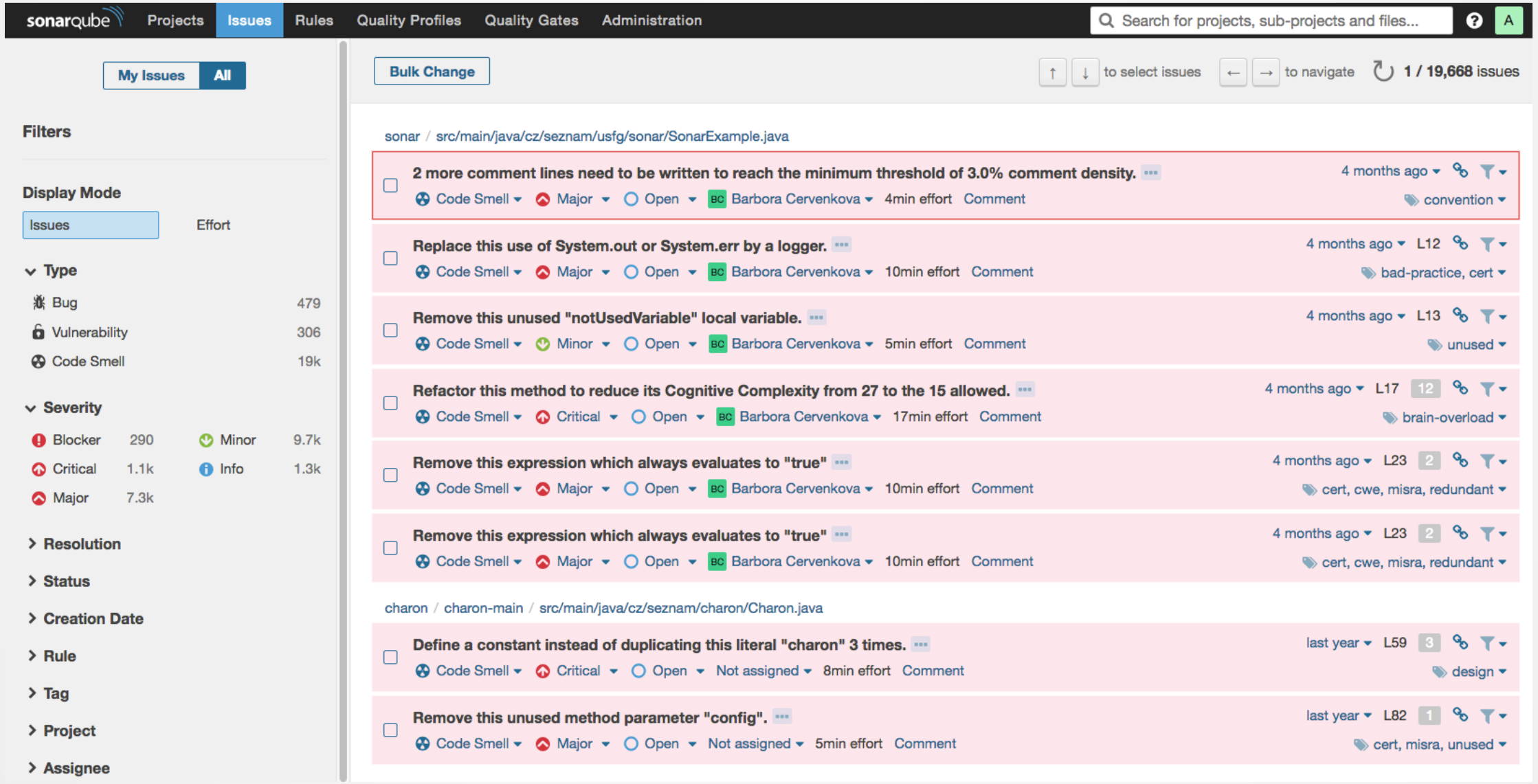
Vývojový proces (zjednodušeně)



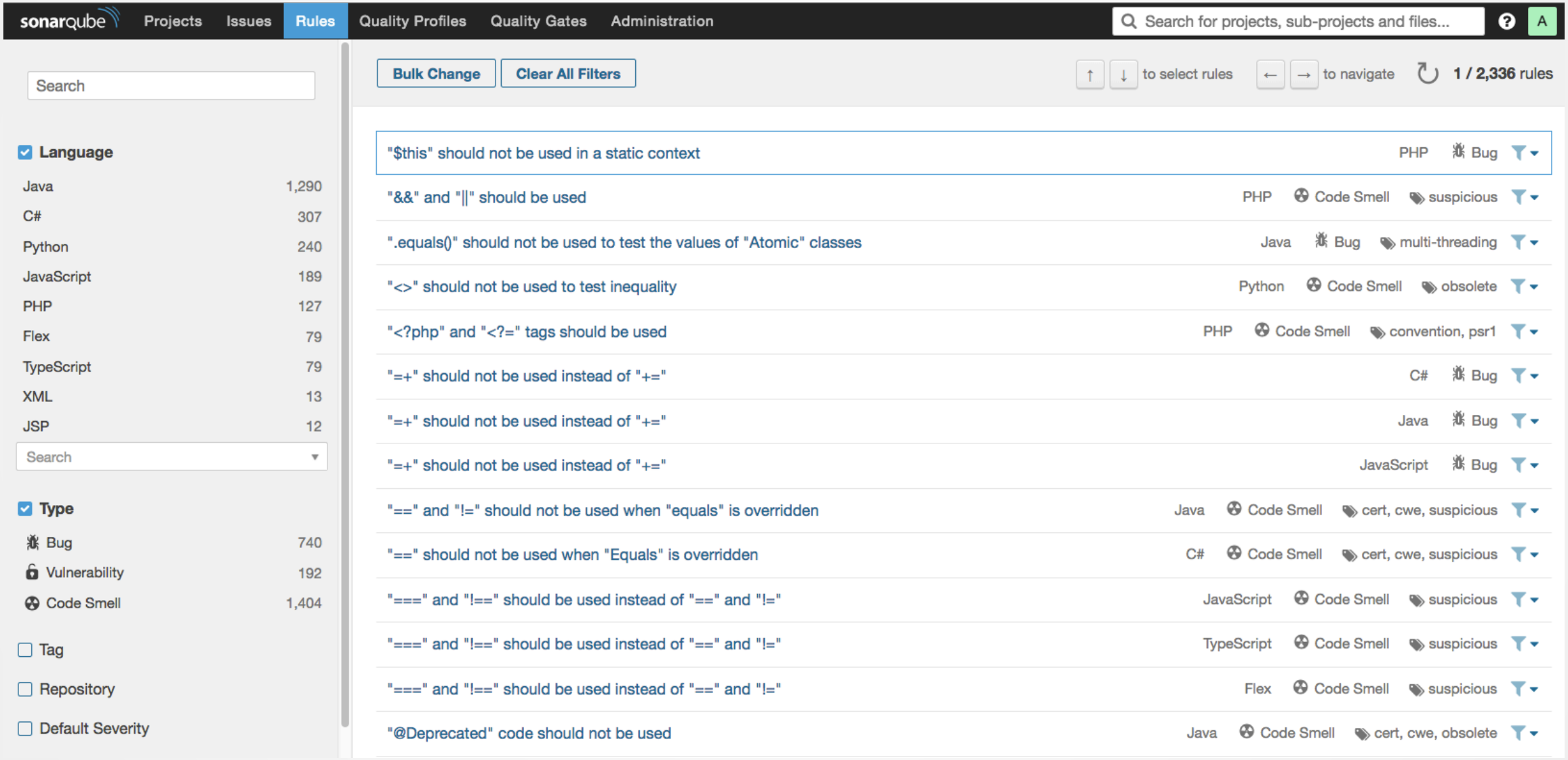
SonarQube


sonarqube
Projects
Issues
Rules
Quality Profiles
Quality Gates
Administration
Search for projects, sub-projects and files...
A
My Favorites
All
Perspective: Overall Status
Sort by: Name
Search by project name or key
20 projects
Filters
Quality Gate
Passed 8
Warning 11
Failed 0
Reliability (Bugs)
A 4
B and worse 15
C and worse 14
D and worse 13
E 13
Security (Vulnerabilities)
A 3
B and worse 16
C and worse 3
D and worse 3
červený projekt
Warning
Last analysis: May 18, 2018, 6:37 PM
5 E Bugs
0 A Vulnerabilities
351 A Code Smells
0.0% Coverage
10.8% Duplications
2.3k S Java, XML
zelený projekt
Passed
Last analysis: January 25, 2018, 3:53 PM
12 E Bugs
3 B Vulnerabilities
284 A Code Smells
0.0% Coverage
0.2% Duplications
7.8k S Java, XML
oranžový projekt
Warning
Last analysis: May 24, 2018, 9:30 AM
0 A Bugs
0 A Vulnerabilities
281 A Code Smells
33.8% Coverage
0.3% Duplications
11k M Java

SonarQube

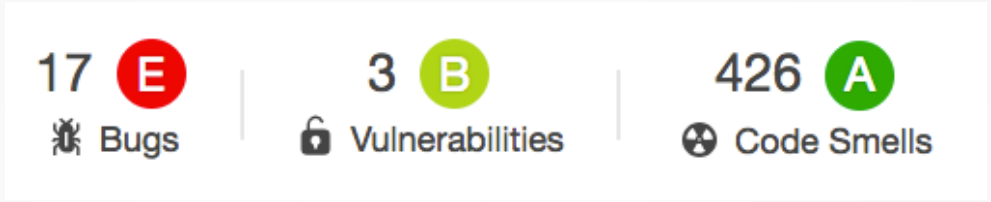

sonarqube
Projects
Issues
Rules
Quality Profiles
Quality Gates
Administration
Search for projects, sub-projects and files...
A
My Issues
All
Filters
Display Mode
Issues
Effort
Type
Bug 479
Vulnerability 306
Code Smell 19k
Severity
Blocker 290
Minor 9.7k
Critical 1.1k
Info 1.3k
Major 7.3k
Resolution
Status
Creation Date
Rule
Tag
Project
Assignee
Bulk Change
to select issues
to navigate
1 / 19,668 issues
sonar / src/main/java/cz/seznam/usfg/sonar/SonarExample.java
2 more comment lines need to be written to reach the minimum threshold of 3.0% comment density.
Code Smell Major Open Barbora Cervenkova 4min effort Comment
4 months ago
convention
Replace this use of System.out or System.err by a logger.
Code Smell Major Open Barbora Cervenkova 10min effort Comment
4 months ago L12
bad-practice, cert
Remove this unused "notUsedVariable" local variable.
Code Smell Minor Open Barbora Cervenkova 5min effort Comment
4 months ago L13
unused
Refactor this method to reduce its Cognitive Complexity from 27 to the 15 allowed.
Code Smell Critical Open Barbora Cervenkova 17min effort Comment
4 months ago L17 12
brain-overload
Remove this expression which always evaluates to "true"
Code Smell Major Open Barbora Cervenkova 10min effort Comment
4 months ago L23 2
cert, cwe, misra, redundant
Remove this expression which always evaluates to "true"
Code Smell Major Open Barbora Cervenkova 10min effort Comment
4 months ago L23 2
cert, cwe, misra, redundant
charon / charon-main / src/main/java/cz/seznam/charon/Charon.java
Define a constant instead of duplicating this literal "charon" 3 times.
Code Smell Critical Open Not assigned 8min effort Comment
last year L59 3
design
Remove this unused method parameter "config".
Code Smell Major Open Not assigned 5min effort Comment
last year L82 1
cert, misra, unused

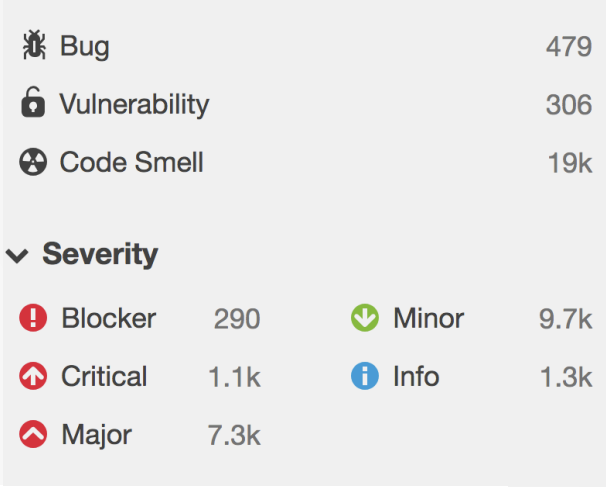
SonarQube

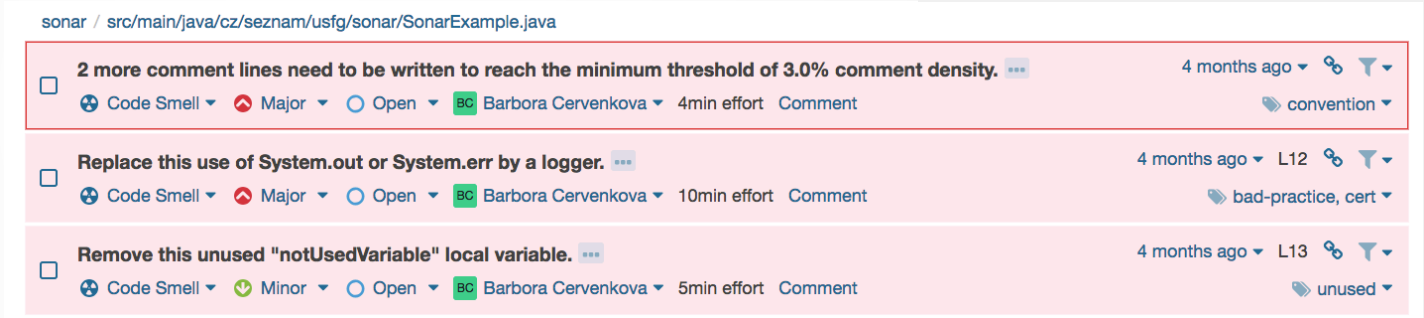

sonarqube
Projects
Issues
Rules
Quality Profiles
Quality Gates
Administration
Search for projects, sub-projects and files...
A
Search
Language
Java 1,290
C# 307
Python 240
JavaScript 189
PHP 127
Flex 79
TypeScript 79
XML 13
JSP 12
Search
Type
Bug 740
Vulnerability 192
Code Smell 1,404
Tag
Repository
Default Severity
Bulk Change
Clear All Filters
to select rules
to navigate
1 / 2,336 rules
"$this" should not be used in a static context PHP Bug
"&&" and "||" should be used PHP Code Smell suspicious
".equals()" should not be used to test the values of "Atomic" classes Java Bug multi-threading
"<>" should not be used to test inequality Python Code Smell obsolete
"<?php" and "<?=" tags should be used PHP Code Smell convention, psr1
"=+" should not be used instead of "+=" C# Bug
"=+" should not be used instead of "+=" Java Bug
"=+" should not be used instead of "+=" JavaScript Bug
"==" and "!=" should not be used when "equals" is overridden Java Code Smell cert, cwe, suspicious
"==" should not be used when "Equals" is overridden C# Code Smell cert, cwe, suspicious
"===" and "!==" should be used instead of "==" and "!=" JavaScript Code Smell suspicious
"===" and "!==" should be used instead of "==" and "!=" TypeScript Code Smell suspicious
"===" and "!==" should be used instead of "==" and "!=" Flex Code Smell suspicious
"@Deprecated" code should not be used Java Code Smell cert, cwe, obsolete

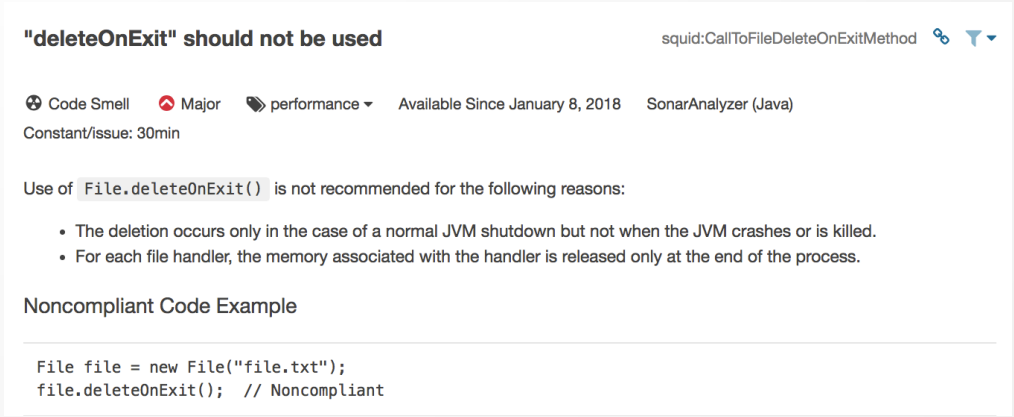
Features

- analýza issues, pravidla



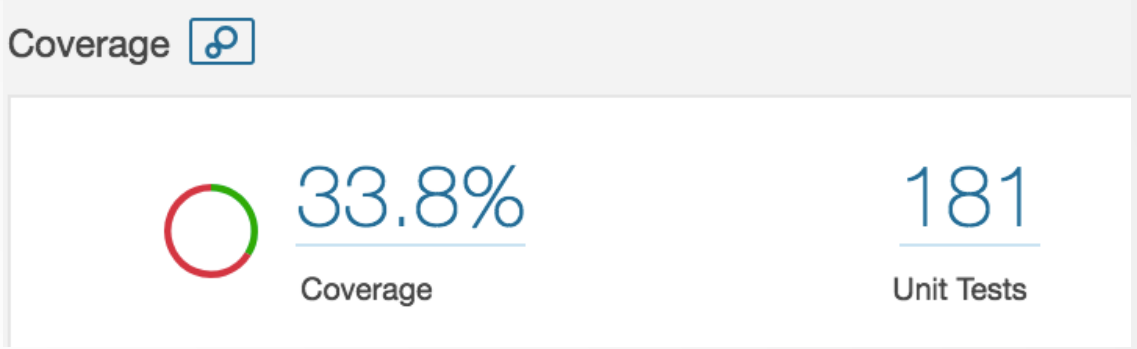




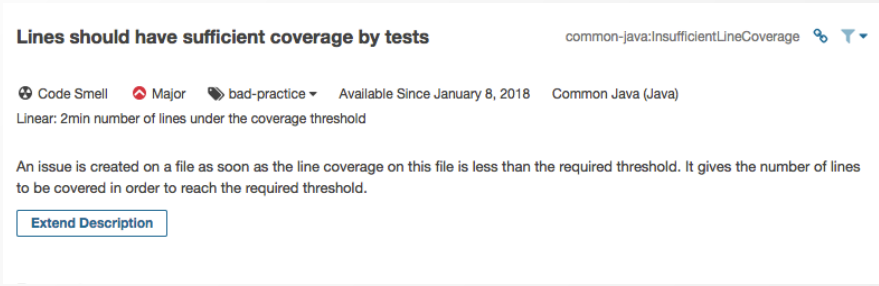


Features

- analýza issues, pravidla
- **zobrazení code coverage**

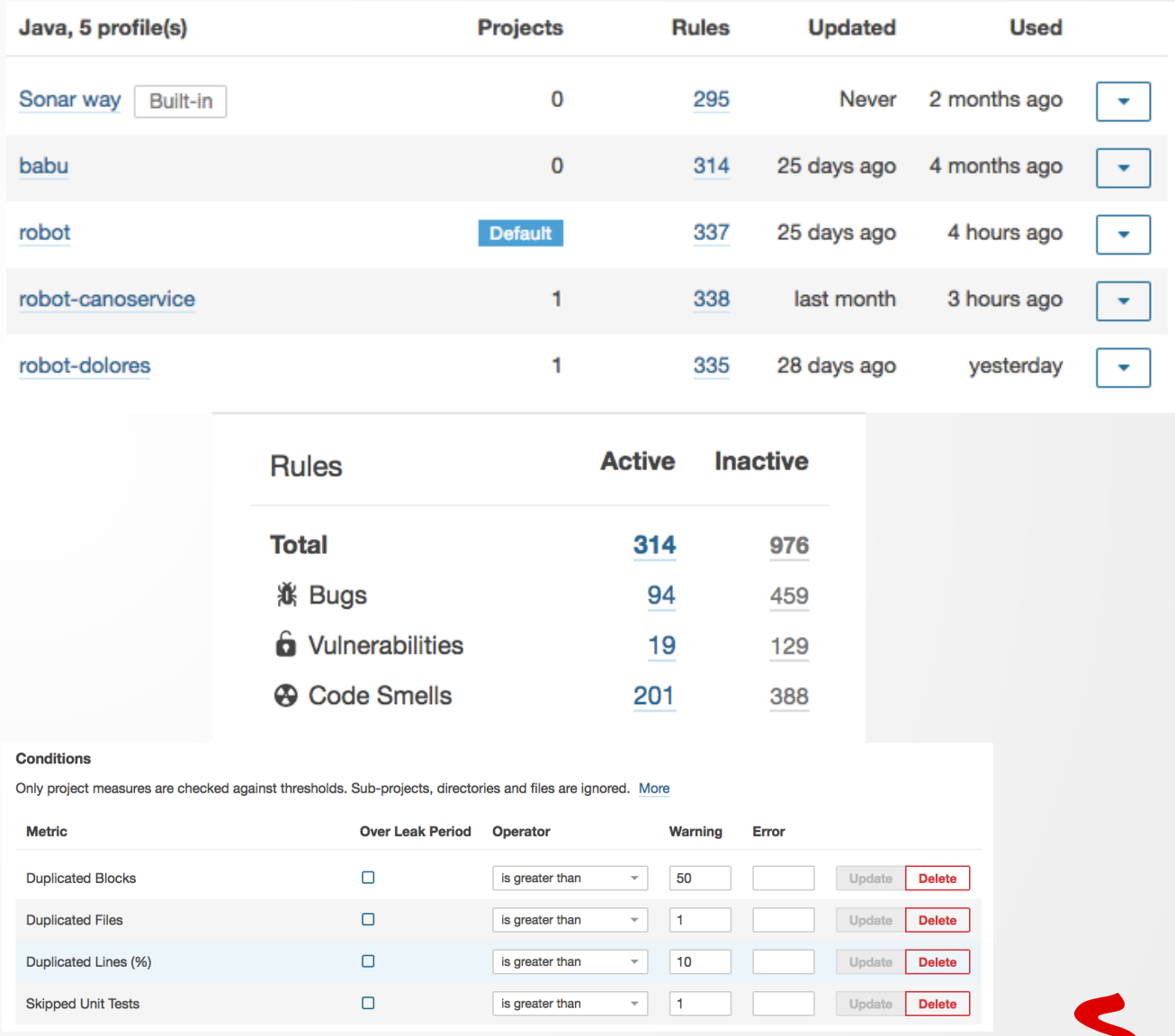



```
122  jind…      if (downloadResponse.hasHttpResponse()) {
123  jind…        log.debug("Robots.txt downloaded, [{}]", robotsTxtTask.getRequest().getNormalizedRequest().getUrl());
124  jind…        try {
125               byte[] gunzip = CompressionUtils.gunzip(downloadResponse.getHttpResponse().getContent().toByteArray())
126               if ((downloadResponse.getHttpResponse().getStatusCodeValue() / 100) != 5) {
127                 // do not cache 500
128                 cacheClient.put(robotsTxtTask, downloadResponse);
129               }
130               return new String(gunzip, Charsets.UTF_8);
131             } catch (IOException e) {
132               log.error("Error when unzipping robots.txt content", e);
133               return ROBOTS_TXT_EMPTY_CONTENT;
134             }
135           }
136           return null;
137         }
```



Features

- analýza issues, pravidla
- zobrazení code coverage
- **quality profile/quality gate per projekt**



Java, 5 profile(s)	Projects	Rules	Updated	Used
Sonar way Built-in	0	295	Never	2 months ago
babu	0	314	25 days ago	4 months ago
robot	Default	337	25 days ago	4 hours ago
robot-canoservice	1	338	last month	3 hours ago
robot-dolores	1	335	28 days ago	yesterday

Rules	Active	Inactive
Total	314	976
Bugs	94	459
Vulnerabilities	19	129
Code Smells	201	388

Conditions

Only project measures are checked against thresholds. Sub-projects, directories and files are ignored. More

Metric	Over Leak Period	Operator	Warning	Error	
Duplicated Blocks	☐	is greater than	50		Update Delete
Duplicated Files	☐	is greater than	1		Update Delete
Duplicated Lines (%)	☐	is greater than	10		Update Delete
Skipped Unit Tests	☐	is greater than	1		Update Delete

Features

- analýza issues, pravidla
- zobrazení code coverage
- quality profile/quality gate per projekt
- **podpora pro 20+ jazyků**

Parent pom for projects specific to fulltext-robot team.

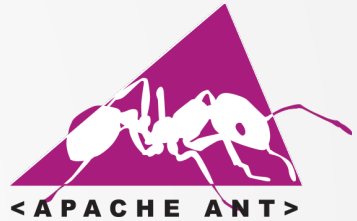
2.3k
Lines of Code

Java	2k
XML	381

Features

- analýza issues, pravidla
- zobrazení code coverage
- quality profile/quality gate per projekt
- podpora pro 20+ jazyků
- **rozsáhlá podpora DevOps**
- **pluginy na integraci do nastroju pro code review (Gitlab, Bitbucket, …)**

Atlassian Bitbucket



Travis CI

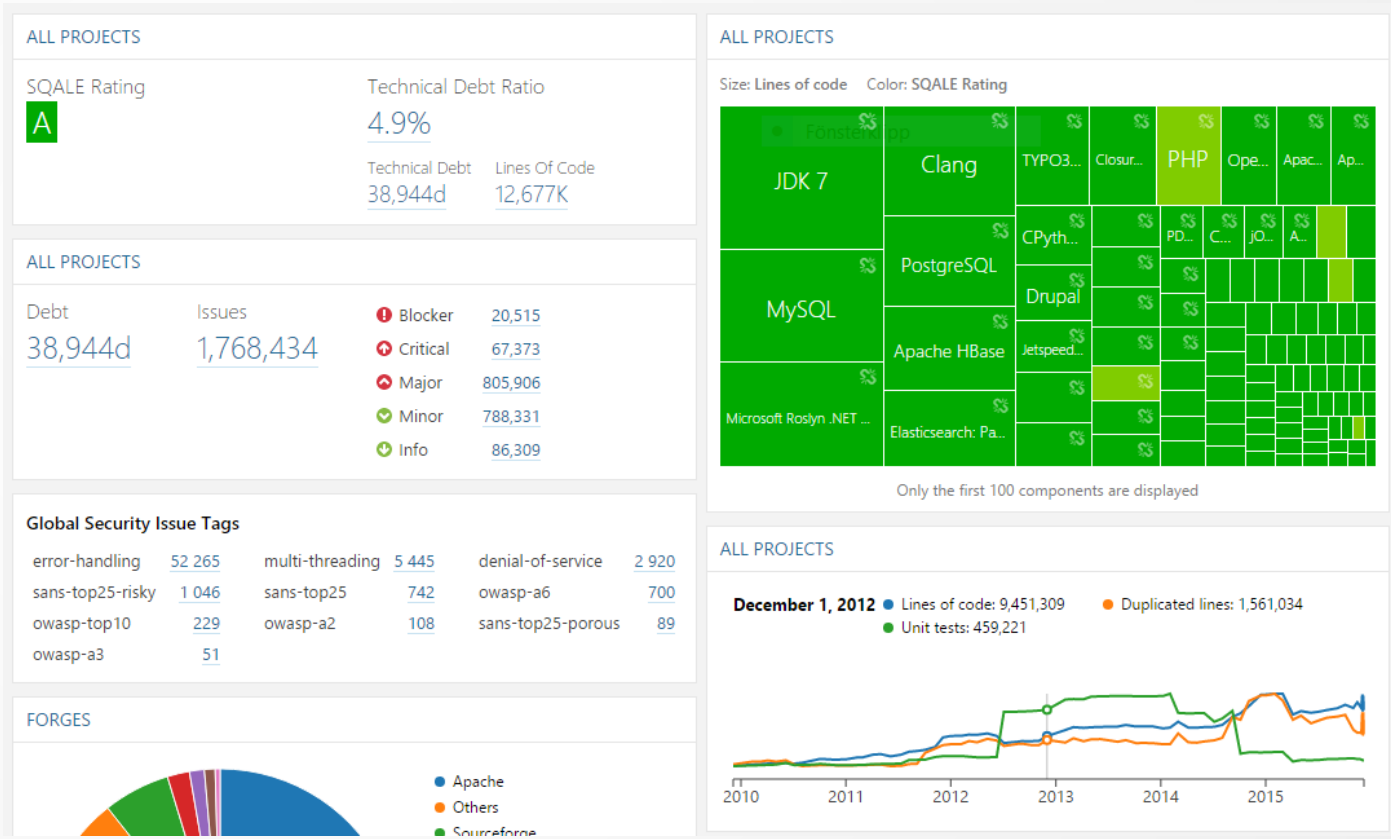
img src: https://gitlab.com/, https://jenkins.io/, https://maven.apache.org/, https://maven.apache.org/, https://gradle.org/ , https://bitbucket.org/, https://travis-ci.org/, https://www.jetbrains.com/teamcity/

Features

- analýza issues, pravidla
- zobrazení code coverage
- quality profile/quality gate per projekt
- podpora pro 20+ jazyků
- rozsáhlá podpora DevOps
- pluginy na integraci do nastroju pro code review (Gitlab, Bitbucket, …)

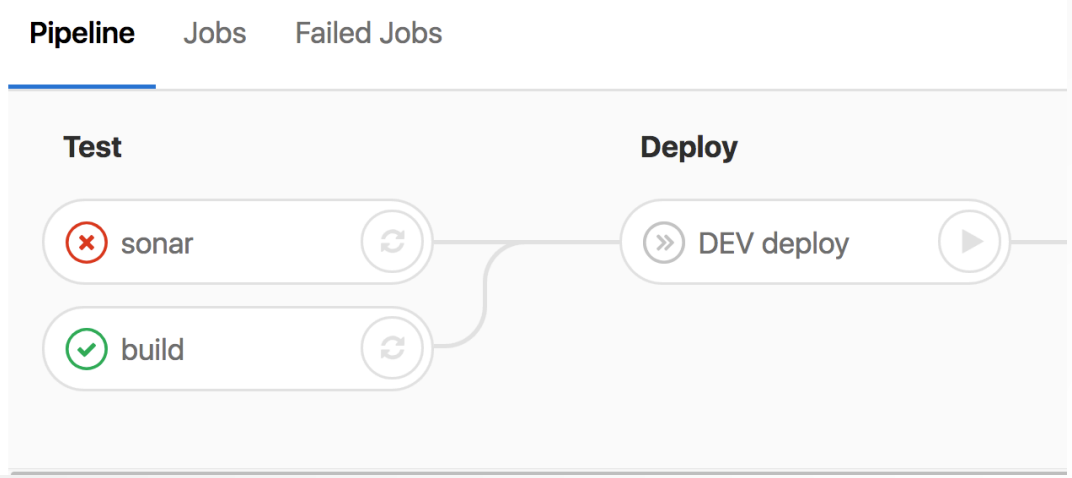
další (+ placené):

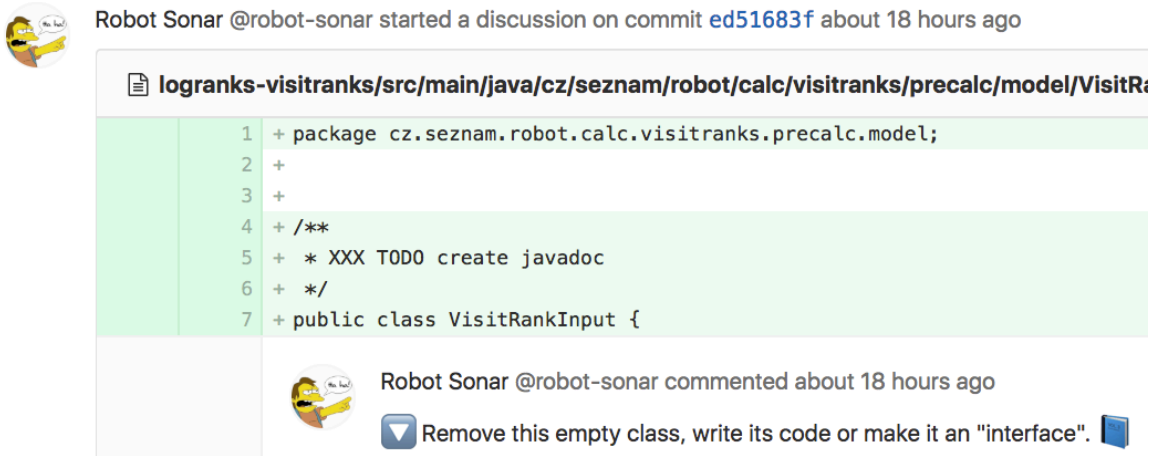
- více dashboardů/reporting
- enterprise edition
- podpora
- SonarCloud - sonar as a service

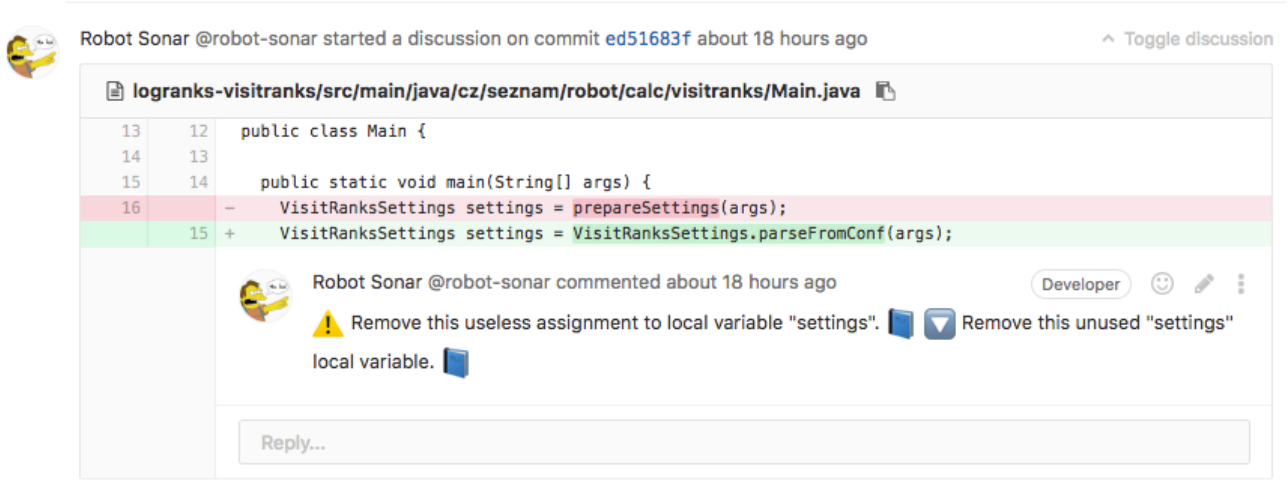


img src: https://www.sonarsource.com/, http://blog.nethouse.se/2015/12/10/fight-technical-debt-with-sonarqube/

Jak to používáme v Robotovi








```
mvn verify sonar:sonar -DskipTests -Dsonar.host.url=$SONAR_URL -Dsonar.analysis.mode=preview
-Dsonar.gitlab.commit_sha=$CI_COMMIT_SHA -Dsonar.gitlab.project_id=$CI_PROJECT_ID -
Dsonar.gitlab.ref_name=$CI_COMMIT_REF_NAME
```

Sonar je dobrý sluha špatný pán

taky souhlasím, akorát se mi nechce opravovat kód po někom jiným

já celkově nesouhlasím s tím, aby mi program kontroloval “human readability”

nemyslím si, že tohle pravidlo má tak hloubkovou analýzu, že se to nepoužívá ani zvenčí, přeci jenom to je public,takže kdo ví odkud to voláš (i když by to byl humus)

jako to pravidlo dává smysl, ale Sonar asi nevidí úplně do completable futures

když si budeš chtít hrát, udělej si profil

`WSRedirectPath` no tfuj 🐷
takhle nemá vypadat konstanta
critical issue na vás

dáš mi admin práva, plíz?

to první rozhodně není ani Javadoc ani “block of commented-out lines of code”,to je to na co tu nadávám

To kontroluje, že všichni píšou konzistentně 👍
a to je důležitý, sorry jako

critical bych opravil, zbytek nech

to vás neomlouvá čuňátka!

nemá no, ale nejlepší je,že to vůbec nepatří k tomu merge requestu

štve mě to, že
* nadává na ”zakomentovanej kód”, který není kód ale komentář
* dožaduje se lambdy v místě, kde lambda moc jednoduše udělat nejde

… aspoň, že ty chyby nejsou kritický 😁

je mi to celkem jedno, ale chce to nastavit si code style, ať všichni jedeme stejně

Kontakt

Babu Červenková
Fulltext robot

E-mail: barbora.cervenkova@firma.seznam.cz
Twitter: @SeznamBot

Odkazy:

- SonarQube: https://www.sonarqube.org/
- sonar-gitlab-plugin: https://gitlab.talanlabs.com/gabriel-allaigre/sonar-gitlab-plugin
- Robot na Twitteru: https://twitter.com/seznambot

SEZNAM.CZ