



# Ferramentas de testes de software

Júlio Werner Z. Koepsel e Rafael J. Camargo

---

# Ferramentas de teste funcional



# PyUnit

- Desenvolvimento e análise de testes unitários para a linguagem Python;
- PyUnit é uma biblioteca de teste unitário desenvolvida para a linguagem de programação Python, fornece um conjunto de ferramentas para testar os códigos escritos. Faz parte da biblioteca padrão do Python desde a versão 2.1 e, portanto, está incluído em todas subsequentes. PyUnit é baseado na popular ferramenta JUnit para Java e fornece um framework similar para testar código Python. Fornece uma estrutura simples, mas poderosa, para testar o código, também tem um rico conjunto de ferramentas para afirmar os resultados de seus testes e para depurar códigos.

```
1 import unittest
2
3 class TestClass(unittest.TestCase):
4
5     def test_meu_metodo(self):
6         self.assertEqual(valor_esperado , valor_real, "mensagem caso o teste falhe")
7
8     if __name__ == "__main__":
9         unittest.main()
```

PyUnit



# QUnit

- Atua na verificação e implantação de testes unitários para a linguagem JavaScript;
- O QUnit é um framework de testes unitários desenvolvido para a linguagem JavaScript, possui uma interface simples e intuitiva que segue os padrões do xUnit, tornando-o familiar e fácil de usar para aqueles que já estão familiarizados com outros frameworks de testes unitários. Além disso, o QUnit é totalmente personalizável através de uma série de plug-ins e tem suporte para testes automatizados, o que o torna ideal para integração contínua e outros ambientes de automação.

```
const add = require('../add.js');

QUnit.module('add');

QUnit.test('two numbers', assert => {
  assert.equal(add(1, 2), 3);
});
```

QUnit

---

# Ferramentas de teste de manutenibilidade



# Complexity Report

- Análise de complexidade de software para projetos JavaScript;
- O Complexity Report é um wrapper de linha de comando baseado em node.js em torno do escomplex, que é a biblioteca que executa o trabalho de análise. O código é passado para o escomplex na forma de árvores de sintaxe que foram geradas com o analisador esprima. O resultado são diversas métricas informando o nível de complexidade do software.



```

{
  maintainability: 171,
  dependencies: [],
  aggregate: {
    sloc: {
      logical: 0,
      physical: 0
    },
    params: 0,
    cyclomatic: 1,
    cyclomaticDensity: 1,
    halstead: {
      vocabulary: 0,
      difficulty: 0,
      volume: 0,
      effort: 0,
      bugs: 0,
      time: 0
    }
  },
},

```

```

functions: [
  {
    name: '',
    line: 0,
    sloc: {
      logical: 0,
      physical: 0
    },
    params: 0,
    cyclomatic: 1,
    cyclomaticDensity: 1,
    halstead: {
      vocabulary: 0,
      difficulty: 0,
      volume: 0,
      effort: 0,
      bugs: 0,
      time: 0
    }
  },
  ...
]
}

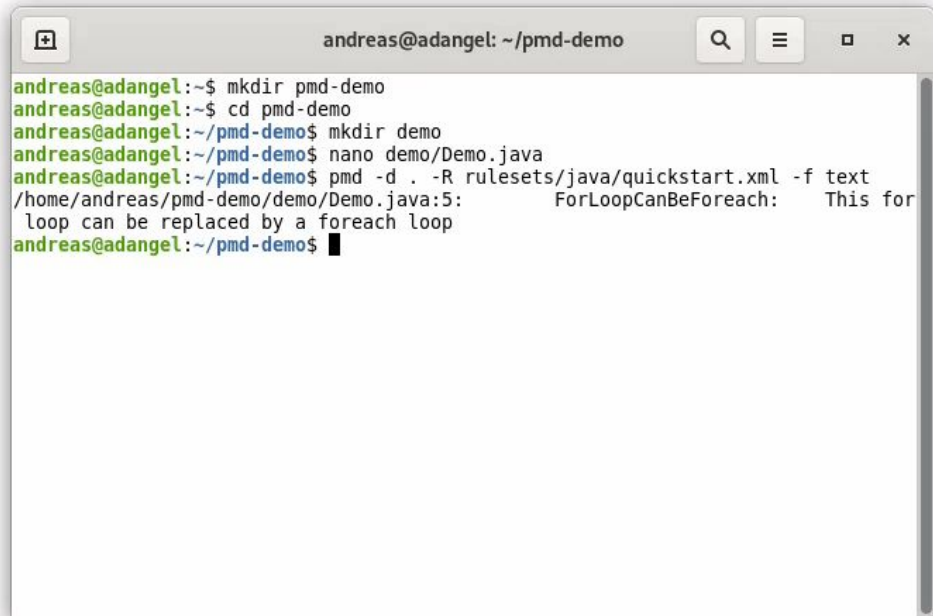
```

## Complexity Report



# PMD

- Analisador de código fonte para Java, JavaScript, Salesforce.com Apex e Visualforce, PLSQL, Apache Velocity, XML, XSL;
- A PMD encontra falhas de programação comuns, como variáveis não utilizadas, blocos *catch* vazios, criação desnecessária de objetos, entre outros. Além disso, ela inclui CPD, um detector de duplicidade. O CPD encontra código duplicado em Java, C, C++, C#, Groovy, PHP, Ruby, Fortran, JavaScript, PLSQL, Apache Velocity, Scala, Objective C, Matlab, Python, Go, Swift e Salesforce.com Apex e Visualforce. A PMD está disponível como plugin em diversas IDEs, facilitando sua implementação.



A terminal window titled "andreas@adangel: ~/pmd-demo" with standard macOS window controls (search, menu, zoom, close). The terminal shows the following commands and output:

```
andreas@adangel:~$ mkdir pmd-demo
andreas@adangel:~$ cd pmd-demo
andreas@adangel:~/pmd-demo$ mkdir demo
andreas@adangel:~/pmd-demo$ nano demo/Demo.java
andreas@adangel:~/pmd-demo$ pmd -d . -R rulesets/java/quickstart.xml -f text
/home/andreas/pmd-demo/demo/Demo.java:5:      ForLoopCanBeForeach:      This for
loop can be replaced by a foreach loop
andreas@adangel:~/pmd-demo$
```

PMD

---

# Ferramentas de teste de usabilidade



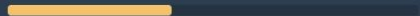
# Website Grader

- Classificação e análise de Search Engine Optimization (SEO);
- O Website Grader é uma ferramenta gratuita que tem por objetivo gerar uma análise de um site, classificando o mesmo em relação a uma série de fatores, incluindo otimização para mecanismos de busca, conteúdo e links. Fornecendo um relatório detalhado de ações que podem ser tomadas para melhorar o site.



sig.ifc.edu.br

DESEMPENHO 12/30



SEO 25/30



MÓVEL 30/30



SEGURANÇA 5/10



Seu site está lhe atrapalhando?

Crie e gerencie sites atraentes que recebem tráfego e convertem leads com o HubSpot CMS gratuito.

Obtenha o CMS gratuito

Sem necessidade de cartão de crédito

HubSpot **TOOLS**  
WEBSITE GRADER

## Esse site é OK

Nada mau! Agora vamos ver como podemos aumentar um pouco essa pontuação. Veja sua pontuação abaixo e obtenha o guia gratuito sobre otimização de sites para melhorá-la.

Obtenha um guia gratuito

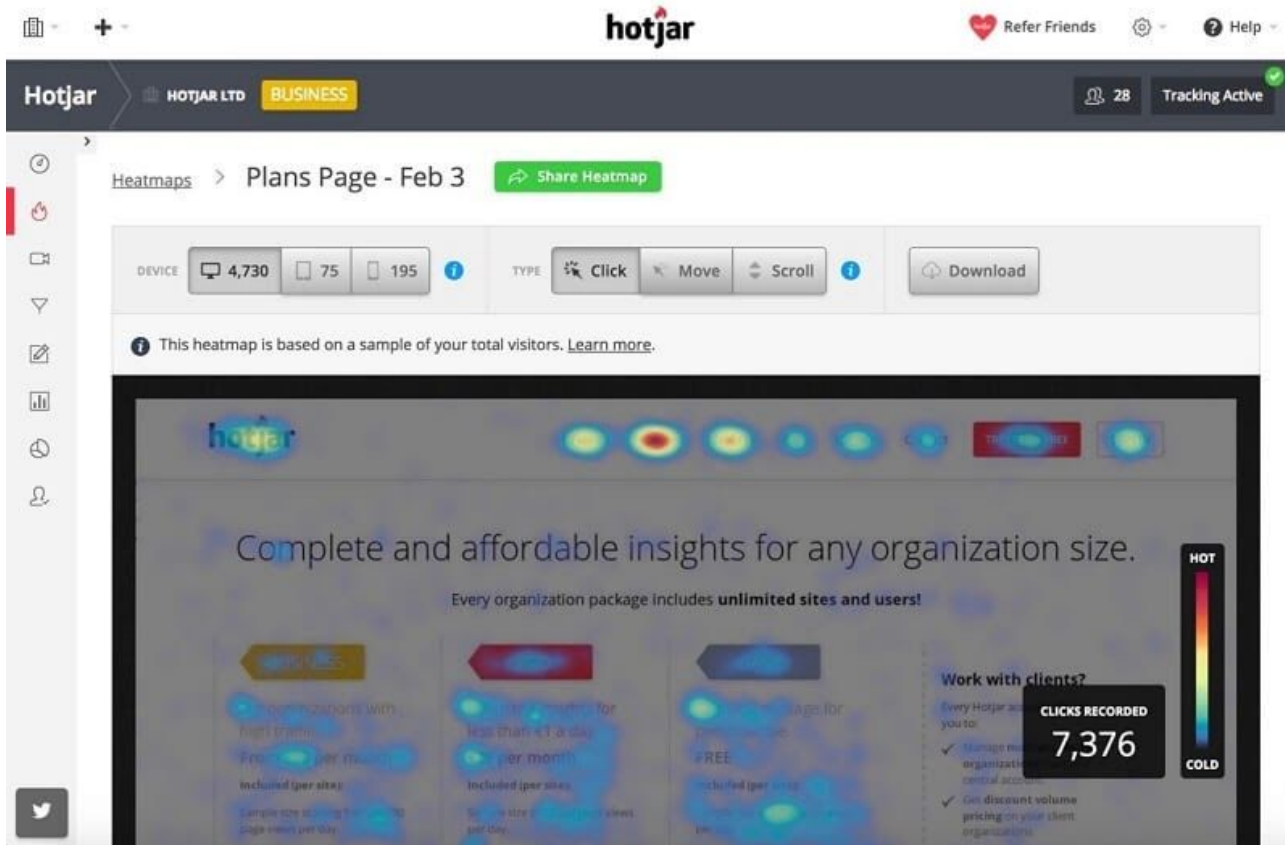


Website Grader



# Hotjar

- Análise comportamental de interações em aplicações WEB;
- Hotjar é uma ferramenta que permite visualizar o comportamento dos usuários em um site. Por meio de um mapa de calor, podemos verificar onde os usuários estão clicando, logo realizando mais interações. A ferramenta também oferece um gravador de sessão que pode ser usado para ver como os usuários estão navegando pelo site. Atua principalmente para o completo entendimento de como o usuário está interagindo com o site, que por sua vez permite identificar problemas de usabilidade, design e navegação.



Hotjar



---

# Ferramentas de teste de segurança



## Google CodeSearchDiggity

- Parte do Google Hacking Diggity Project. Utiliza o Google Code Search para identificar vulnerabilidades em projetos de código aberto hospedados pelo Google Code, MS CodePlex, SourceForge e Github, entre outros;
- A ferramenta proporciona, através da API Code Search do Google, mais de 130 tipos de pesquisa, que identificam SQL injection, cross-site scripting, arquivos remotos e locais inseguros e credenciais embutidas, entre outros. Essencialmente, o Google CodeSearchDiggity fornece uma análise de segurança do código fonte de projetos de código aberto existentes.

GoogleDiggity CodeSearchDiggity BingDiggity LinkFromDomainDiggity DLPDiggity FlashDiggity MalwareDiggity

Advanced Simple

Query Appender

Queries

- ☐ SQL Injection
- ☐ Cross-site Scripting (XS)
- ☐ Filesystem Interaction
- ☐ Handling Sensitive Data
- ☐ Hard-coded Passwords
- ☐ Data Mining
- ☐ Other
- ☐ Remote File Include
- ☐ Remote Code/Command Execution
- ☒ Amazon Keys
  - ☒ EC2
  - ☒ Amazon

SCAN Cancel

Category	Subcategory	Search String	Page Title	URL
Amazon Keys	EC2	ec2[^\d][A-Z0-9]{20}	trunk/simond/js	<a href="http://www.google.com/codesearch/p?hl=en#Kcy">http://www.google.com/codesearch/p?hl=en#Kcy</a>
Amazon Keys	EC2	ec2[^\d][A-Z0-9]{20}	trunk/simond/js	<a href="http://www.google.com/codesearch/p?hl=en#Kcy">http://www.google.com/codesearch/p?hl=en#Kcy</a>
Amazon Keys	EC2	ec2[^\d][A-Z0-9]{20}	trunk/src/chron	<a href="http://www.google.com/codesearch/p?hl=en#CQl">http://www.google.com/codesearch/p?hl=en#CQl</a>
Amazon Keys	EC2	ec2[^\d][A-Z0-9]{20}	trunk/src/chron	<a href="http://www.google.com/codesearch/p?hl=en#CQl">http://www.google.com/codesearch/p?hl=en#CQl</a>
Amazon Keys	EC2	ec2[^\d][A-Z0-9]{20}	chrome/content	<a href="http://www.google.com/codesearch/p?hl=en#ulAl">http://www.google.com/codesearch/p?hl=en#ulAl</a>
Amazon Keys	EC2	ec2[^\d][A-Z0-9]{20}	chrome/content	<a href="http://www.google.com/codesearch/p?hl=en#ulAl">http://www.google.com/codesearch/p?hl=en#ulAl</a>
Amazon Keys	EC2	ec2[^\d][A-Z0-9]{20}	trunk/src/eifaw	<a href="http://www.google.com/codesearch/p?hl=en#aMl">http://www.google.com/codesearch/p?hl=en#aMl</a>
Amazon Keys	EC2	ec2[^\d][A-Z0-9]{20}	trunk/EC2Samp	<a href="http://www.google.com/codesearch/p?hl=en#nfD">http://www.google.com/codesearch/p?hl=en#nfD</a>
Amazon Keys	Amazon	amazon.*[A-Z0-9]{20}	lookups.py	<a href="http://www.google.com/codesearch/p?hl=en#474">http://www.google.com/codesearch/p?hl=en#474</a>

Output Selected Result

```
<pre>    Jec2 ec2 = new J<b>ec2("AK[REDACTED]ZEHQ"</b>, "[REDACTED]n+RCIkuoEeAD6");</pre>
```

Amazon AWS Cloud keys stored in plaintext

Google CodeSearchDiggity



# Veracode

- Plataforma de segurança de aplicativos com foco em segurança integrada ao ambiente de desenvolvimento;
- A plataforma de segurança de software contínua Veracode proporciona várias ferramentas, entre elas: análise estática de mais de 100 linguagens e frameworks; análise dinâmica de aplicativos WEB e APIs; análise de composição de software durante o ciclo de desenvolvimento; gerenciamento de superfície de ataque WEB para descobrir e inventariar todos os aplicativos voltados para o público, dentro e fora do intervalo de IP; teste de penetração manual para encontrar classes de vulnerabilidades que as avaliações automatizadas não conseguem; previsão de vulnerabilidades futuras através da aplicação de aprendizado de máquina e inteligência artificial.

[MY PORTFOLIO](#)
[SCANS & ANALYSIS](#)
[ANALYTICS](#)
[POLICIES](#)
[eLEARNING](#)

Veracode\_Dem

## Security Platform Home

START A SCAN

SCAN RESULTS

ANALYZE PERFORMANCE

LEARN

### Recent Applications

[See All >](#)

<a href="#">Veracode Labs</a> Static Scan: Complete Dynamic Analysis Scan: Complete	Veracode Recommended Very High v1 Veracode Level: 2	<a href="#">View Results</a>
<a href="#">FinTracker</a> Static Scan: Complete	Veracode Recommended Very High v1 Veracode Level: 1	<a href="#">View Results</a>
<a href="#">WebGoat</a> Static Scan: Complete Dynamic Analysis Scan: Complete	Veracode Recommended Very High v1 Veracode Level: 1	<a href="#">View Results</a>
<a href="#">Hadoop</a> Static Scan: Request Incomplete	Veracode Recommended Very High v1 Veracode Level: 1	<a href="#">View Results</a>
<a href="#">Metamail</a> Static Scan: Complete	Veracode Transitional Very High v1 Veracode Level: 1	<a href="#">View Results</a>
<a href="#">midsssh.BB</a> Static Scan: Complete	Veracode Transitional Very High v1 Veracode Level: 3	<a href="#">View Results</a>

### What's New?

[Latest Release Notes](#)
[Hello Center](#)  
Veracode Documentation  
[Integrate and Automate](#)  
Veracode Plugins and APIs  
[Veracode Community](#)  
Engage, Learn, Collaborate

### eLearning

[See All >](#)

Recent Activity

Application Security Training  
Incomplete, latest activity:  
2/7/18

### Connect with Veracode

[Veracode Blog](#)  
Posts on security research and all things security

[Follow Us on Twitter](#)  
Ask questions, get company news, and more.

© Veracode, Inc. 2006 - 2019 [Usage Guidelines](#) [Responsible Disclosure Policy](#) [Hello Center](#) [Contact Support](#)

Last account activity on 11/26/19 3:05 PM EST from IP: 172.22.103.1. For use under U.S. Pat. Nos. 8,072,035, 8,043,800, 8,402,906, 9,236,063, 9,207,820, 9,190,833, 8,565,155, 7,792,609, and 8,804,904, and patents pending.

Veracode

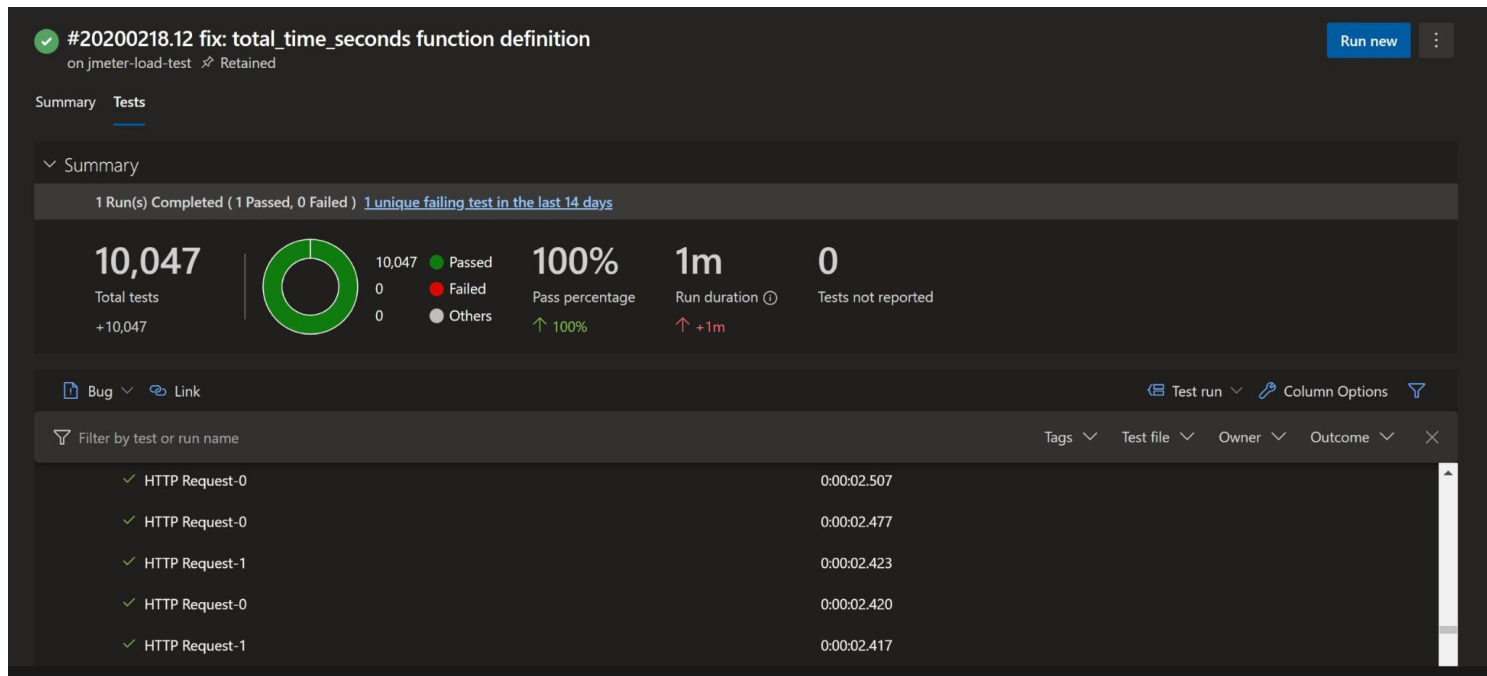
---

# Ferramentas de teste de desempenho



# Apache JMeter

- Teste de carga de aplicações e serviços WEB;
- Apache JMeter é um software de teste de carga open source, gratuito e de código aberto. Ele foi criado para permitir que os usuários testem a funcionalidade e o desempenho de aplicativos web e outros serviços de rede. Ele fornece um conjunto de ferramentas para criar testes de carga sintéticos e monitorar o desempenho de aplicativos web e outros serviços de rede. Ele pode ser usado para simular um grande número de usuários que acessam um aplicativo ou um site. Também pode ser usado para medir a capacidade do servidor de lidar com um grande número de conexões simultâneas.



Apache JMeter





# Open STA

- Teste de carga WEB de estresse e desempenho HTTP/HTTPS;
- Open STA é um software livre que fornece um ambiente de teste automatizado para aplicativos Web. Ele pode ser usado para automatizar testes funcionais e de stress com carga pesada em HTTP e HTTPS, bem como para criar cenários de teste complexos por meio da utilização de scripts, gerando um benchmarking com base nos testes executados.



---

# Ferramentas de verificação e validação contínuas



# Kiuwan

- Plataforma de segurança de aplicativos de ponta a ponta;
- A plataforma de segurança de aplicativos Kiuwan suporta mais de 30 linguagens de programação e proporciona dois produtos: teste de segurança de aplicativos estáticos, capaz de escanear código e identificar vulnerabilidades, sendo compatível com padrões de segurança rigorosos, incluindo CWE, OWASP, PCI, CERT e SANS; análise de composição de software, para redução do risco de componentes de terceiros, corrigindo vulnerabilidades e garantindo a conformidade com as licenças, sendo alinhado com o banco de dados NIST.

Not grouped

Sample » Analysis ✓ 2019/10/02 10:07

Sample

Sample2

⊕ New

## SUMMARY

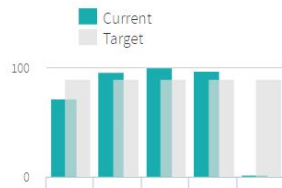
RISK INDEX

17.77



GLOBAL INDICATOR

70.63



EFFORT TO TARGET

14h 24

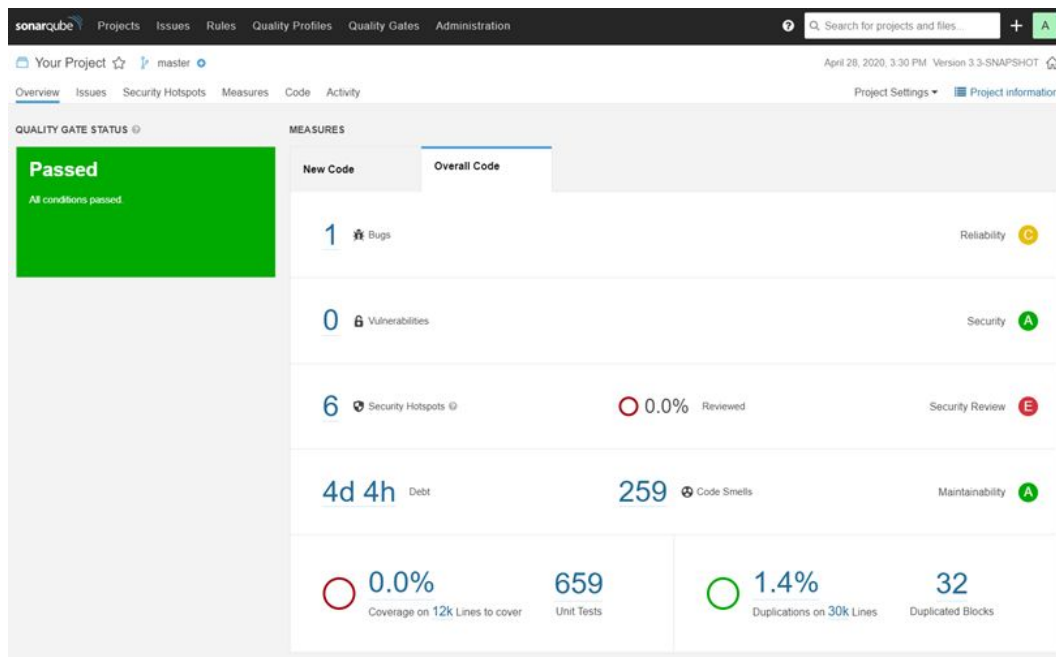


Kiuwan



# SonarQube

- Plataforma de código aberto para inspeção contínua da qualidade do código;
- A plataforma SonarQube oferece ferramentas de inspeção de código estático e análise de código com suporte para 29 linguagens de programação. Algumas das ferramentas são: Quality Gate, para verificação de erros e vulnerabilidades no código e em commits, Maintainability analysis para garantir código limpo e manutenível e Security Analysis para verificar erros de segurança no código.



SonarQube



# Ferramentas de testes de software

Júlio Werner Z. Koepsel e Rafael J. Camargo