

FIAP

FIAP

SLIDER



COMPLIANCE & QUALITY ASSURANCE

Prof. M.Sc. Felipe Desiglo Ferrare
proffelipe.ferrare@fiap.com.br

Exemplos de Análise Estática

Aula 3

Análise Estática

Foco em Segurança - Dependabot

es [Pull requests](#) [Actions](#) [Projects](#) [Wiki](#) [Security](#) [Insights](#) [Settings](#)

[Overview](#)

Reporting

[Policy](#)

[Advisories](#)

Vulnerability alerts

[Dependabot](#)

[Code scanning](#)

[Secret scanning](#)

Dependabot alerts

[Give feedback](#)

Confi

Auto-triage your alerts

Control how Dependabot opens pull requests, ignores false positives and snoozes alerts. Rules can be enforced at the organization level. Free for open source and available for private repos through [GitHub Advanced Security](#).

[Learn more about auto-triage](#)



Generate fix
for custom
pattern



Ignore for
manifest



Dependabot alerts are disabled.

To receive Dependabot alerts, you must first enable Dependabot alerts in [this repository's settings](#).

Análise Estática

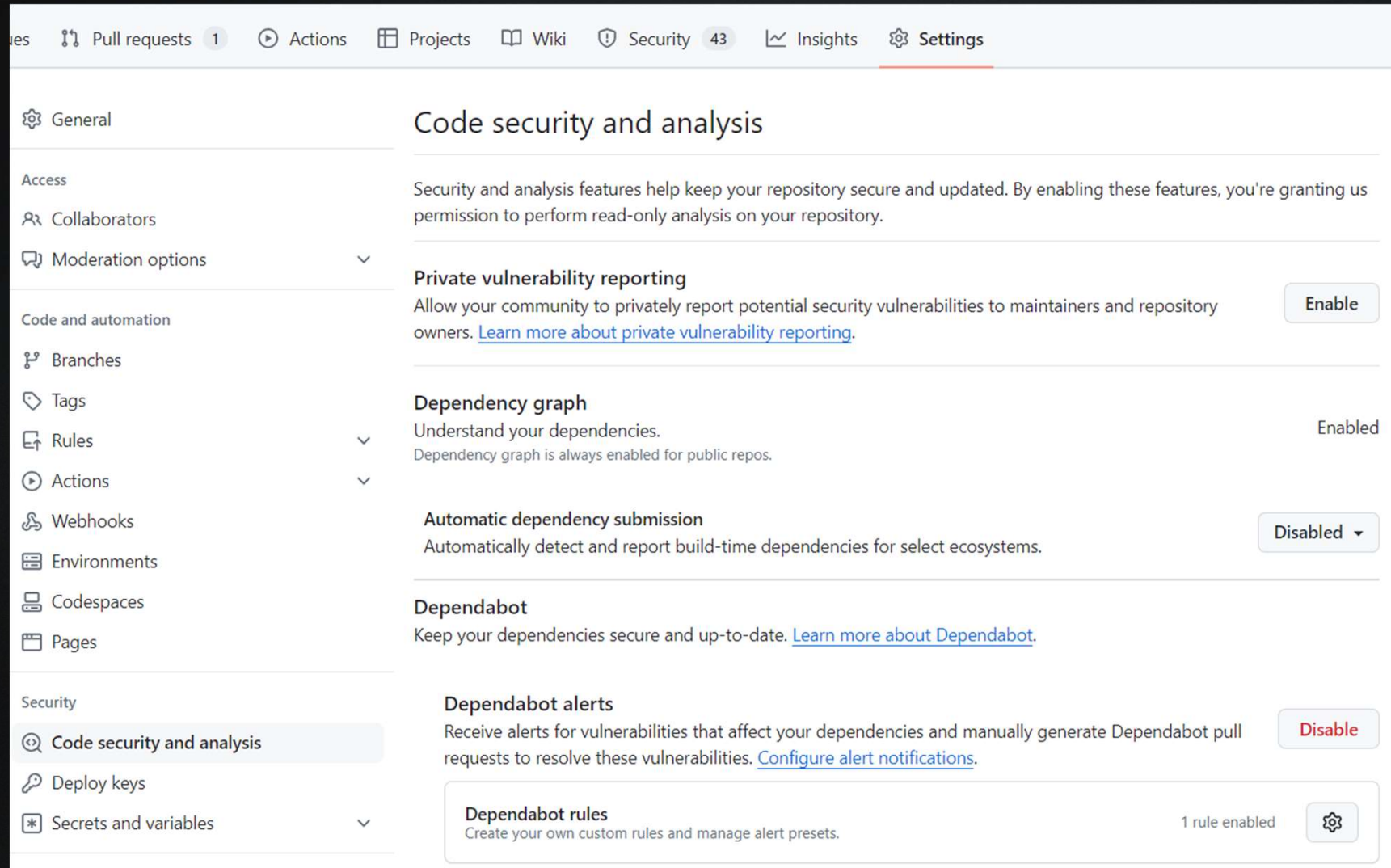
Dependabot

- Pode ser configurado nas configurações segurança do seu repositório
- Irá detectar arquivos de dependência para fazer verificar se tem dependências com vulnerabilidades
- Irá criar alertas para essas dependências e pode criar PRs para fazer atualizações de dependências
- Capaz de trabalhar com várias linguagens.

Análise Estática

Dependabot

FIAP



The screenshot shows the GitHub repository settings page for a repository named 'es'. The 'Settings' tab is selected in the top navigation bar. The left sidebar contains a list of settings categories: General, Access, Code and automation, and Security. The 'Security' category is expanded, and 'Code security and analysis' is selected. The main content area is titled 'Code security and analysis' and contains several sections: 'Private vulnerability reporting' (with an 'Enable' button), 'Dependency graph' (marked as 'Enabled'), 'Automatic dependency submission' (with a 'Disabled' button), 'Dependabot' (with a link to learn more), 'Dependabot alerts' (with a 'Disable' button), and 'Dependabot rules' (showing '1 rule enabled' with a settings icon).

es Pull requests 1 Actions Projects Wiki Security 43 Insights Settings

General

Access

Collaborators

Moderation options

Code and automation

Branches

Tags

Rules

Actions

Webhooks

Environments

Codespaces

Pages

Security

Code security and analysis

Deploy keys

Secrets and variables

Code security and analysis

Security and analysis features help keep your repository secure and updated. By enabling these features, you're granting us permission to perform read-only analysis on your repository.

Private vulnerability reporting

Allow your community to privately report potential security vulnerabilities to maintainers and repository owners. [Learn more about private vulnerability reporting.](#) **Enable**

Dependency graph

Understand your dependencies. **Enabled**
Dependency graph is always enabled for public repos.

Automatic dependency submission

Automatically detect and report build-time dependencies for select ecosystems. **Disabled**

Dependabot

Keep your dependencies secure and up-to-date. [Learn more about Dependabot.](#)

Dependabot alerts

Receive alerts for vulnerabilities that affect your dependencies and manually generate Dependabot pull requests to resolve these vulnerabilities. [Configure alert notifications.](#) **Disable**

Dependabot rules

Create your own custom rules and manage alert presets. **1 rule enabled**

Análise Estática

Dependabot

FIAP

main.py


requirements.txt

test.py

Code

Blame

2 lines (2 loc) · 23 Bytes

 Code 55% faster with GitHub Copilot

```
1 Flask==0.1
2 Django==1.4
```

Análise Estática

Dependabot

FIAP

Alertas

The screenshot displays the GitHub interface for Dependabot alerts. The top navigation bar includes links for Pull requests (1), Actions, Projects, Wiki, Security (43), Insights, and Settings. The left sidebar shows the 'Security' section with sub-items: Overview, Reporting, Policy, Advisories, Vulnerability alerts, Dependabot (43), Code scanning, and Secret scanning. The main content area is titled 'Dependabot alerts' and includes a 'Give feedback' link and a 'Configure' dropdown. A section titled 'Auto-triage your alerts' explains how to control how Dependabot opens pull requests and provides a link to 'Learn more about auto-triage'. Below this is a search bar with the text 'is:open'. A summary bar shows '43 Open' alerts and '0 Closed'. The table of alerts lists four critical and high severity issues for Django, each with a checkbox, a severity label, and a link to the pull request.

| Package | Ecosystem | Manifest | Severity | Sort | | | | | |
|--------------------------|-----------|---|----------|--|------|--|--|--|--|
| <input type="checkbox"/> | ! | 43 Open | ✓ | 0 Closed | | | | | |
| <input type="checkbox"/> | ! | SQL injection in Django | Critical | #6 opened 2 hours ago • Detected in django (pip) • requirements.txt | 🔗 #1 | | | | |
| <input type="checkbox"/> | ! | Django Potential account hijack via password reset form | Critical | #5 opened 2 hours ago • Detected in django (pip) • requirements.txt | 🔗 #1 | | | | |
| <input type="checkbox"/> | ! | Django Directory Traversal via ssi template tag | High | #34 opened 2 hours ago • Detected in django (pip) • requirements.txt | 🔗 #1 | | | | |
| <input type="checkbox"/> | ! | Django Vulnerable to MySQL Injection | High | #29 opened 2 hours ago • Detected in django (pip) • requirements.txt | 🔗 #1 | | | | |

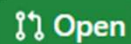
Análise Estática

Dependabot

FIAP

- PR

Bump django from 1.4 to 3.2.25 #1



dependabot wants to merge 1 commit into `main` from `dependabot/pip/django-3.2.25`

Merging this pull request will resolve [40 Dependabot alerts](#) on django including a **critical** severity alert.



Conversation 0



Commits 1



Checks 0



Files changed 1



dependabot bot commented on behalf of github 2 hours ago

Bumps [django](#) from 1.4 to 3.2.25.

► Commits

compatibility unknown

Dependabot will resolve any conflicts with this PR as long as you don't alter it yourself. You can also trigger a rebase manually by commenting `@dependabot rebase`.

- Análise de boas práticas de Código Python

```
pip install pylint
```

Pylint

Exemplo

```
python test.py
```

```
Olá mundo  
1
```

Pylint

Exemplo

```
1      a = 0
2
3      def __x(a):
4          return a
5
6      if __name__ == "__main__":
7          if True:
8              print("Olá mundo")
9              pass
10         print(__x(1))
11         pass
```


Pylint

Exemplo

FIAP

```
pylint test.py
```

```
***** Module test
test.py:4:0: W0311: Bad indentation. Found 1 spaces, expected 4 (bad-indentation)
test.py:7:0: C0325: Unnecessary parens after 'if' keyword (superfluous-parens)
test.py:11:0: C0304: Final newline missing (missing-final-newline)
test.py:1:0: C0114: Missing module docstring (missing-module-docstring)
test.py:1:0: C0103: Constant name "a" doesn't conform to UPPER_CASE naming style (invalid-name)
test.py:3:8: W0621: Redefining name 'a' from outer scope (line 1) (redefined-outer-name)
test.py:7:7: W0125: Using a conditional statement with a constant value (using-constant-test)
test.py:9:8: W0107: Unnecessary pass statement (unnecessary-pass)
test.py:11:4: W0107: Unnecessary pass statement (unnecessary-pass)

-----
Your code has been rated at 0.00/10 (previous run: 0.00/10, +0.00)
```

Pylint

Exemplo

FIAP

```
pylint test.py
```

Your code has been rated at 10.00/10 (previous run: 8.00/10, +2.00)

Java checkstyle

FIAP

https://checkstyle.sourceforge.io/cmdline.html#Download_and_Run

Java

checkstyle

https://checkstyle.sourceforge.io/cmdline.html#Download_and_Run

```
java -jar checkstyle-10.17.0-all.jar -c /sun_checks.xml MyClass.java  
java -jar checkstyle-10.17.0-all.jar -c /google_checks.xml MyClass.java
```


Checkstyle

Exemplo

```
1  public.class.TestMain.{ CR LF
2  CR LF
3  → public.static.void.main(String[] .args) CR LF
4  → { CR LF
5  → if("AA" .==. "AA") { CR LF
6  → System.out.println("olá") ; CR LF
7  → .....} CR LF
8  → } CR LF
9  → ..... CR LF
10 }
```

Checkstyle

Exemplo

```
-c /sun_checks.xml TestMain.java
Iniciando a auditoria...
[ERROR] C:\Users\desig\Downloads\check\Itens\TestMain.java:1: O arquivo não termina com uma linha em branco. [NewlineAtEndOfFile]
[ERROR] C:\Users\desig\Downloads\check\Itens\TestMain.java:1: O arquivo package-info.java está faltando. [JavadocPackage]
[ERROR] C:\Users\desig\Downloads\check\Itens\TestMain.java:1:1: Classes utilitárias não deveriam ter construtores públicos ou com visibilidade de pacote. [HideUtilityClassConstructor]
[ERROR] C:\Users\desig\Downloads\check\Itens\TestMain.java:3:1: O arquivo contém caracteres de tabulação (esta é a primeira ocorrência). [FileTabCharacter]
[ERROR] C:\Users\desig\Downloads\check\Itens\TestMain.java:3:9: Falta o comentário Javadoc. [MissingJavadocMethod]
[ERROR] C:\Users\desig\Downloads\check\Itens\TestMain.java:3:33: O parâmetro args deve ser final. [FinalParameters]
[ERROR] C:\Users\desig\Downloads\check\Itens\TestMain.java:4:9: O '{' na coluna 2 deveria estar na linha anterior. [LeftCurly]
[ERROR] C:\Users\desig\Downloads\check\Itens\TestMain.java:5:9: 'if' não está seguido de espaço em branco. [WhitespaceAfter]
[ERROR] C:\Users\desig\Downloads\check\Itens\TestMain.java:5:9: 'if' não está seguido de espaço em branco. [WhitespaceAround]
[ERROR] C:\Users\desig\Downloads\check\Itens\TestMain.java:5:25: '{' não está precedido por espaço em branco. [WhitespaceAround]
[ERROR] C:\Users\desig\Downloads\check\Itens\TestMain.java:9: Line has trailing spaces. [RegexpSingleline]
Auditoria completa.
O Checkstyle terminou com 11 erros.
```

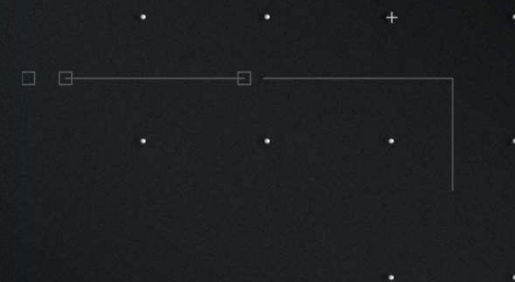
Exercício Opcional

FIAP

Tente passar código que você já desenvolveu por um ou mais ferramentas,
aparece algum alerta ?

Você consegue corrigir todos os alertas ?

Obrigado!



FIAP