

DevSecOps para Devs

Integrando a Segurança ao DNA do seu código

QUEM SOU EU?



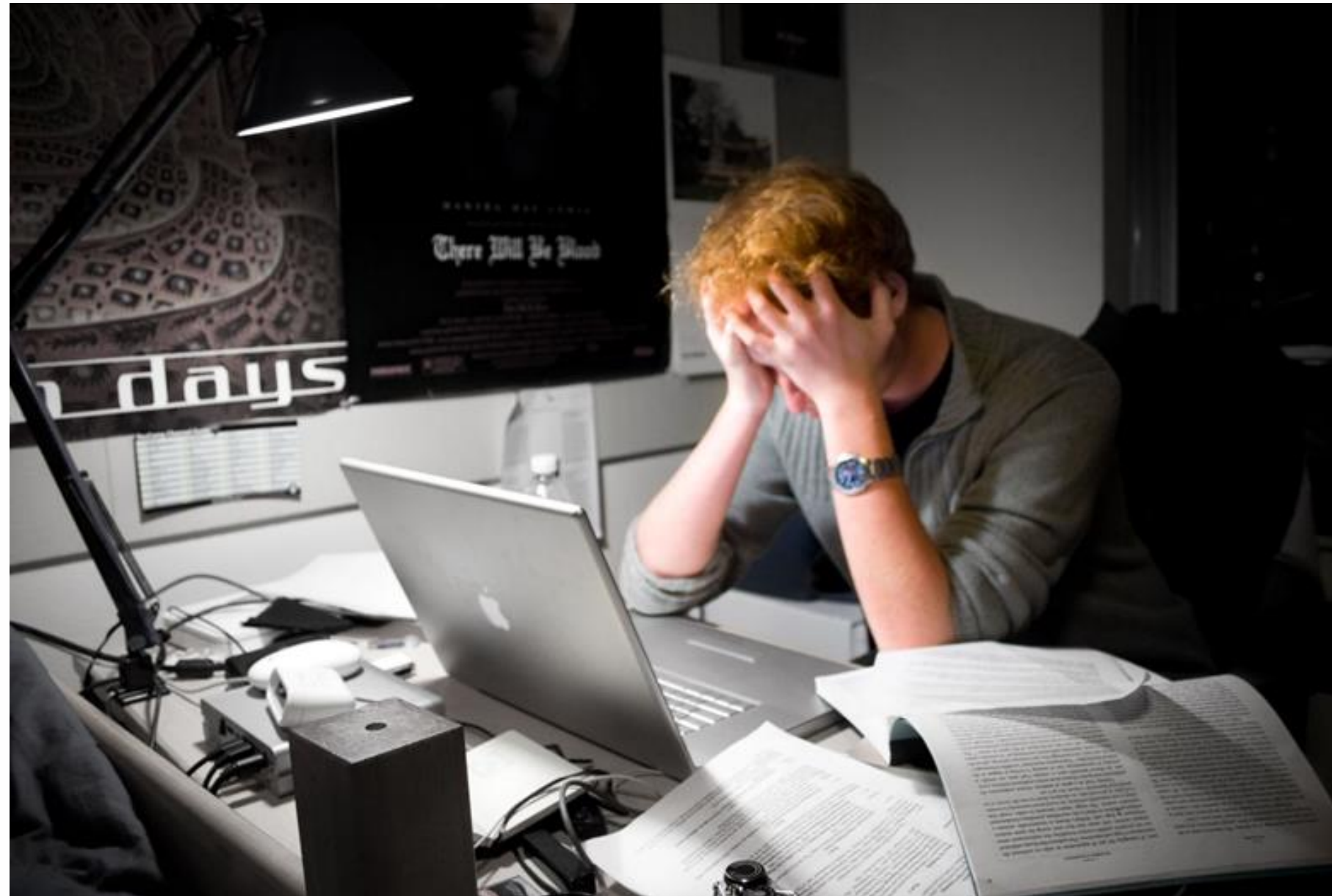
 /denispetri

Denis Petri

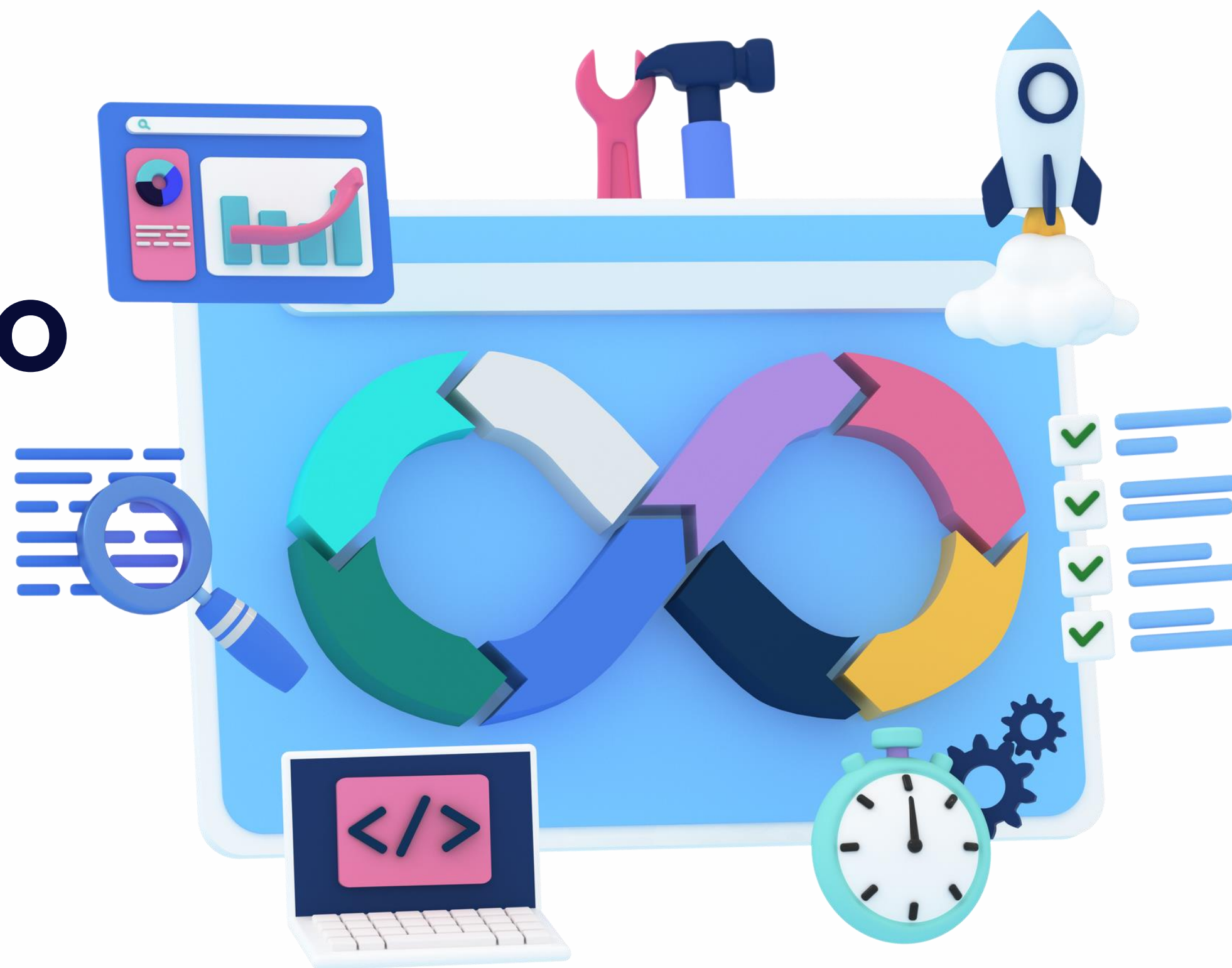
Co-Founder & CEO na **CodeFortress**
Head de Tecnologia na **goFlux**

Arquiteto Corporativo, de Solução e de Software, com mais de 30 anos de experiência na área de TI e principalmente com empresas de Desenvolvimento de Software.

QUEBRANDO O SILÊNCIO



DEVSECOPS: SEGURANÇA INTEGRADA DESDE O INÍCIO



COLABORAÇÃO, AUTOMAÇÃO E MONITORAMENTO CONTÍNUO



SHIFT-LEFT: SEGURANÇA ANTECIPADA



SAST: ENCONTRANDO VULNERABILIDADES NO CÓDIGO-FONTE



SAST NA PRÁTICA (SEMGREP)

Fix vulnerabilities today and prevent tomorrow's with secure guardrails [Learn more](#) →

Supply Chain Vulnerabilities Advisories Dependencies License configuration Group by Rule Opened all time

Projects and branches local_sc... X

Tags All project tags

Status Open (9)

Severity Critical High Medium Low

Transitivity Direct Transitive Undetermined

EPSS probability High Medium Low None

9 Matching Findings Sort by highest severity Triage (0)

- golang.org/x/net: Uncontrolled Resource Consumption** EPSS: 0.4% (Low) CVE 2023-39325
Affected versions of golang.org/x/net are vulnerable to Uncontrolled Resource Consumption. The HTTP/2 vulnerability occurs when a malicious client rapidly creates and resets requests, causing excessive server
[Show more](#)
- 4mo go.mod:6** Direct Always Reachable P main Details
- golang.org/x/net: Uncontrolled Resource Consumption** EPSS: 4.2% (Low) CVE 2022-41723
golang.org/x/net versions before 0.7.0 are vulnerable to Uncontrolled Resource Consumption caused by the HPACK decoder. A malformed HTTP/2 Stream could be sufficient to cause a denial of service from a
[Show more](#)
- 4mo go.mod:6** Direct Conditionally Reachable P main Details
- golang.org/x/net: Infinite Loop** EPSS: 0.1% (Low) CVE 2021-33194
Affected versions of golang.org/x/net are vulnerable to Loop with Unreachable Exit Condition ('Infinite Loop').



SAST NA PRÁTICA (SEMGREP)

The screenshot displays the Snyk web interface. On the left is a dark sidebar with navigation links: Dashboard, Projects, Code (66), Secrets, Supply Chain (53), Rules, Get Started (41%), Feedback, Settings, Docs, and Help. The main content area has a blue header with the text "Fix vulnerabilities today and prevent tomorrow's with secure guardrails" and a "Learn more" link. Below the header, the page shows the path "Supply Chain > #77265511" and the file "go.mod:6". A redacted area is visible next to the file name. The vulnerability details for "golang.org/x/net: Uncontrolled Resource Consumption" are shown, including an EPSS of 4.2% (Low) and a high severity rating. The description states that versions before 0.7.0 are vulnerable to a denial of service. The "Reachability Details" section explains that the vulnerability is reachable if a user-facing application uses the HPACK decoder. The "Remediation" section advises patching to version 0.7.0. A table compares the "YOUR VERSION" (0.0.0-20210226172049-e18ecbb05110) with the "RECOMMENDED PATCH" (0.7.0). The "Activity" section on the right shows a "New note" button and a "Seen on" entry for the "main" branch on "Wed, 24 Jul 2024 18:53:13", noting it was seen "4 months ago via Azure DevOps". At the bottom, there are "REFERENCES" to GitHub and NVD advisories.

Supply Chain > #77265511

go.mod:6

4mo Conditionally Reachable Direct [redacted] main caec2bc

golang.org/x/net: Uncontrolled Resource Consumption

EPSS: 4.2% (Low) **H** High severity

golang.org/x/net versions before 0.7.0 are vulnerable to Uncontrolled Resource Consumption caused by the HPACK decoder. A malformed HTTP/2 Stream could be sufficient to cause a denial of service from a small number of small requests.

Reachability Details

This vulnerability is reachable if you host a user-facing application utilizing net with the HPACK decoder

Remediation

Validate whether this meets the reachable condition. If it does, patch to version 0.7.0.

0.0.0-20210226172049-e18ecbb05110	0.7.0
YOUR VERSION	RECOMMENDED PATCH

REFERENCES

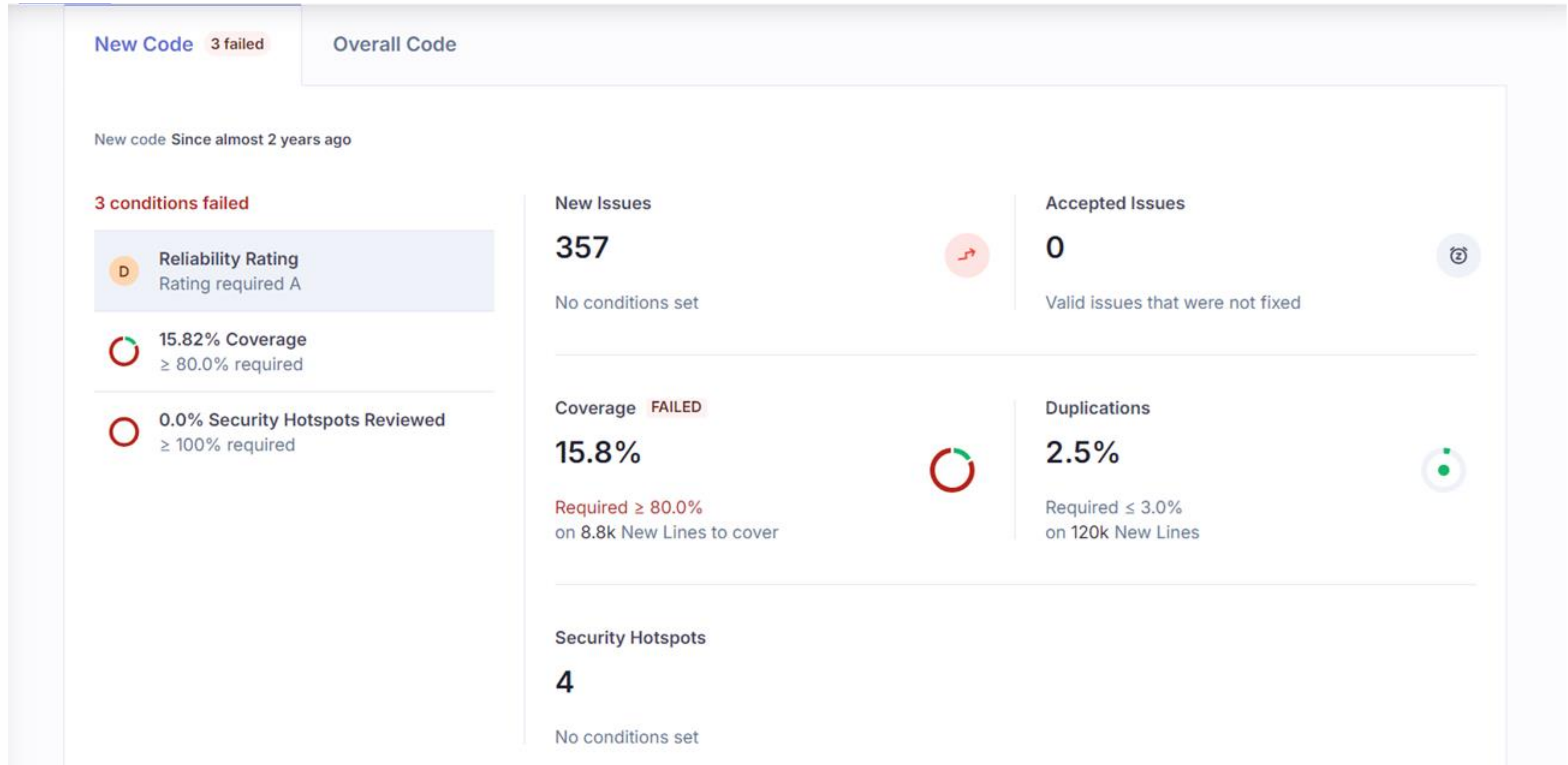
- <https://github.com/advisories/GHSA-...>
- <https://nvd.nist.gov/vuln/detail/CVE-...>

On 1 branch

Activity

- New note
- Seen on
main
Wed, 24 Jul 2024 18:53:13
4 months ago via Azure DevOps

ANALISE DE QUALIDADE DE CÓDIGO NA PRÁTICA (SONARQUBE)



ANALISE DE QUALIDADE DE CÓDIGO NA PRÁTICA (SONARQUBE)

The screenshot displays the SonarQube web interface. On the left is a dark sidebar with navigation links: Overview, Main Branch, Pull Requests (1), Branches (1), Information, and Administration. The main area shows the 'Issues' tab for a project named 'develop'. A red bar obscures the project name. The top navigation bar includes 'My Projects', 'My Issues', 'Explore', and a search icon. Below the project name, there are tabs for 'Summary', 'Issues', 'Security Hotspots', 'Measures', 'Code', and 'Activity'. The 'Issues' tab is active, showing a list of issues. On the left side of the main area, there are filters for 'Clean Code Attribute' (Consistency: 0, Intentionality: 16, Adaptability: 0, Responsibility: 0) and 'Software Quality' (Security: 0, Reliability: 16, Maintainability: 372). The 'Reliability' filter is selected. On the right side, there are three issue cards, each titled 'Intentionality' and containing the text 'Consider using 'await' for the promise inside this 'try' or replace it with 'Promise.prototype.catch(...)' usage.' The issues are categorized as 'Reliability' (orange icon), 'Bug' (star icon), and 'Major' (blue icon). Each issue has a '5min effort' and '1 year ago' timestamp. The top right of the main area shows '16 issues' and '1h 22min effort'.

SonarQube cloud

My Projects My Issues Explore

develop

Summary Issues Security Hotspots Measures Code Activity

Filters Clear All Filters

Clean Code Attribute

Consistency	0
Intentionality	16
Adaptability	0
Responsibility	0

Software Quality 1 x

Security	0
Reliability	16
Maintainability	372

Add to selection Ctrl + click

Severity ?

Blocker	0
High	1
Medium	15
Low	0
Info	0

Intentionality

Consider using 'await' for the promise inside this 'try' or replace it with 'Promise.prototype.catch(...)' usage.

Open Not assigned Reliability Bug Major

5min effort 1 year ago

Intentionality

Consider using 'await' for the promise inside this 'try' or replace it with 'Promise.prototype.catch(...)' usage.

Open Not assigned Reliability Bug Major

5min effort 1 year ago

Intentionality

Consider using 'await' for the promise inside this 'try' or replace it with 'Promise.prototype.catch(...)' usage.



Open Not assigned Reliability Bug Major



5min effort 1 year ago


16 issues 1h 22min effort

ANALISE DE QUALIDADE DE CÓDIGO NA PRÁTICA (SONARQUBE)

☐ Bulk Change

Select issues  


Navigate to issue  






 16 issues 1h 22min effort

app/Services/BillingStayParametersService.ts

☐ Intentionality

Consider using 'await' for the promise inside this 'try' or replace it with 'Promise.prototype.catch(...)' usage.

No tags 


☐ Open  ☐ Not assigned  Reliability   Bug  Major






5min effort • 1 year ago

app/Services/DefaultService.ts

☐ Intentionality

Consider using 'await' for the promise inside this 'try' or replace it with 'Promise.prototype.catch(...)' usage.

No tags 

☐ Open  ☐ Not assigned  Reliability   Bug  Major

5min effort • 1 year ago

CONTAINER SEGURO NA PRÁTICA



```
2. bash
bash-3.2$ trivy knqyf263/test-image:1.2.3
2019-05-13T15:19:03.912+0900 INFO Updating vulnerability database...
2019-05-13T15:19:05.983+0900 INFO Detecting Alpine vulnerabilities...
2019-05-13T15:19:05.987+0900 INFO Updating npm Security DB...
2019-05-13T15:19:07.048+0900 INFO Detecting npm vulnerabilities...
2019-05-13T15:19:07.048+0900 INFO Updating pipenv Security DB...
2019-05-13T15:19:08.507+0900 INFO Detecting pipenv vulnerabilities...
2019-05-13T15:19:08.508+0900 INFO Updating bundler Security DB...
2019-05-13T15:19:09.574+0900 INFO Detecting bundler vulnerabilities...
2019-05-13T15:19:09.575+0900 INFO Updating cargo Security DB...
2019-05-13T15:19:10.441+0900 INFO Detecting cargo vulnerabilities...
2019-05-13T15:19:10.441+0900 INFO Updating composer Security DB...
2019-05-13T15:19:11.649+0900 INFO Detecting composer vulnerabilities...

knqyf263/test-image:1.2.3 (alpine 3.7.1)
=====
Total: 26 (UNKNOWN: 0, LOW: 3, MEDIUM: 16, HIGH: 5, CRITICAL: 2)

+-----+-----+-----+-----+-----+-----+
| LIBRARY | VULNERABILITY ID | SEVERITY | INSTALLED VERSION | FIXED VERSION | TITLE |
+-----+-----+-----+-----+-----+-----+
| curl | CVE-2018-14618 | CRITICAL | 7.61.0-r0 | 7.61.1-r0 | curl: NTLM password overflow via integer overflow |
+-----+-----+-----+-----+-----+-----+
| | CVE-2018-16839 | HIGH | | 7.61.1-r1 | curl: Integer overflow leading to heap-based buffer overflow in Curl_sasl_create_plain_message() |
+-----+-----+-----+-----+-----+-----+
| | CVE-2019-3822 | | | 7.61.1-r2 | curl: NTLMv2 type-3 header stack buffer overflow |
+-----+-----+-----+-----+-----+-----+
| | CVE-2018-16840 | | | 7.61.1-r1 | curl: Use-after-free when closing "easy" handle in Curl_close() |
+-----+-----+-----+-----+-----+-----+
| | CVE-2018-16890 | MEDIUM | | 7.61.1-r2 | curl: NTLM type-2 heap out-of-bounds buffer read |
+-----+-----+-----+-----+-----+-----+
| | CVE-2019-3823 | | | | curl: SMTP end-of-response out-of-bounds read |
+-----+-----+-----+-----+-----+-----+
| | CVE-2018-16842 | | | 7.61.1-r1 | curl: Heap-based buffer over-read in the curl tool warning formatting |
+-----+-----+-----+-----+-----+-----+
| git | CVE-2018-19486 | HIGH | 2.15.2-r0 | 2.15.3-r0 | git: Improper handling of PATH allows for commands to be executed from... |
+-----+-----+-----+-----+-----+-----+
```


DAST: TESTANDO O APLICATIVO EM EXECUÇÃO



OWASP
Zed Attack Proxy

Screenshot of the OWASP Zed Attack Proxy (ZAP) interface showing a successful HTTP request and a detected Cross Site Scripting (Reflected) alert.

Request Details:

- Header: Text
- Body: Text
- HTTP/1.1 200 OK
- Date: Sun, 09 Jul 2023 16:55:22 GMT
- Server: Apache/2.4.54 (Unix)
- X-Powered-By: PHP/8.1.14
- Expires: Thu, 19 Nov 1981 08:52:00 GMT
- Cache-Control: no-store, no-cache, must-revalidate
- Pragma: no-cache
- Content-Length: 2046

Response Body (HTML):

```
<input type="text" name="user" class="form-control" placeholder="Username">
<input type="password" name="pass" class="form-control" placeholder="Password">
</div>
<button type="submit" class="btn btn-primary w-100">Login</button>
</form><script>alert(1);</script><form>
```

Alerts (13):

- Cross Site Scripting (Reflected)
- Absence of Anti-CSRF Tokens (2)
- Content Security Policy (CSP) Header Not Set
- Directory Browsing (2)
- Missing Anti-clickjacking Header (4)
- Cookie No HttpOnly Flag
- Cookie without SameSite Attribute
- Server Leaks Information via "X-Powered-By" t

Cross Site Scripting (Reflected) Details:

- URL: http://10.10.239.217:8082/login.php?err=%3C%2Fform%3E%3Cscript%3Ealert%281%29%3B%3C%2Fscript%3E%3Cform%3E
- Risk: High
- Confidence: Medium
- Parameter: err
- Attack: </form> <script>alert(1);</script> <form>
- Evidence: </form> <script>alert(1);</script> <form>
- CWE ID: 79
- WASC ID: 8

SEGREDOS PROTEGIDOS: GUARDANDO SUAS CHAVES



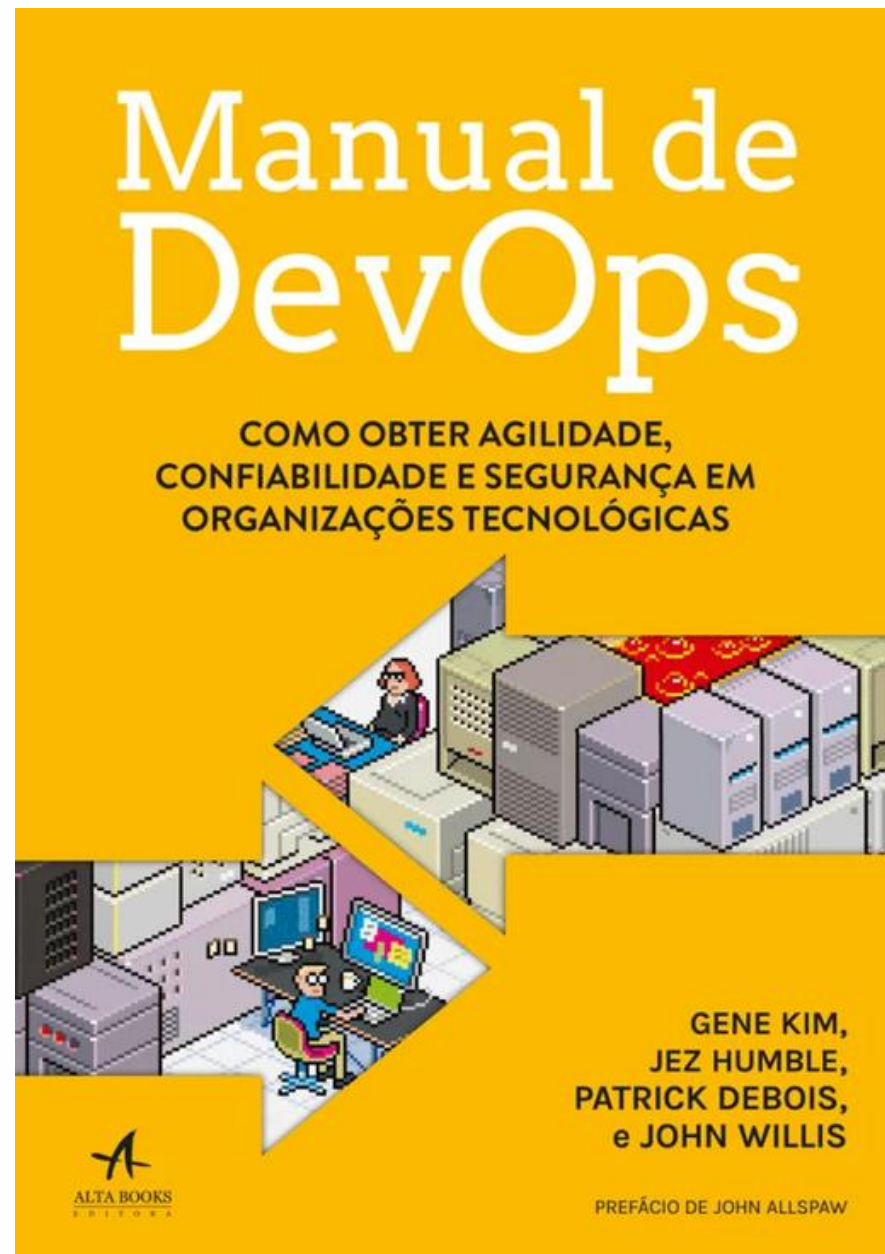


CULTURA DE SEGURANÇA: RESPONSABILIDADE DE TODOS

DEVSECOPS: CONSTRUINDO UM FUTURO SEGURO



APROFUNDE SEU CONHECIMENTO



Segurança

Em aplicações web

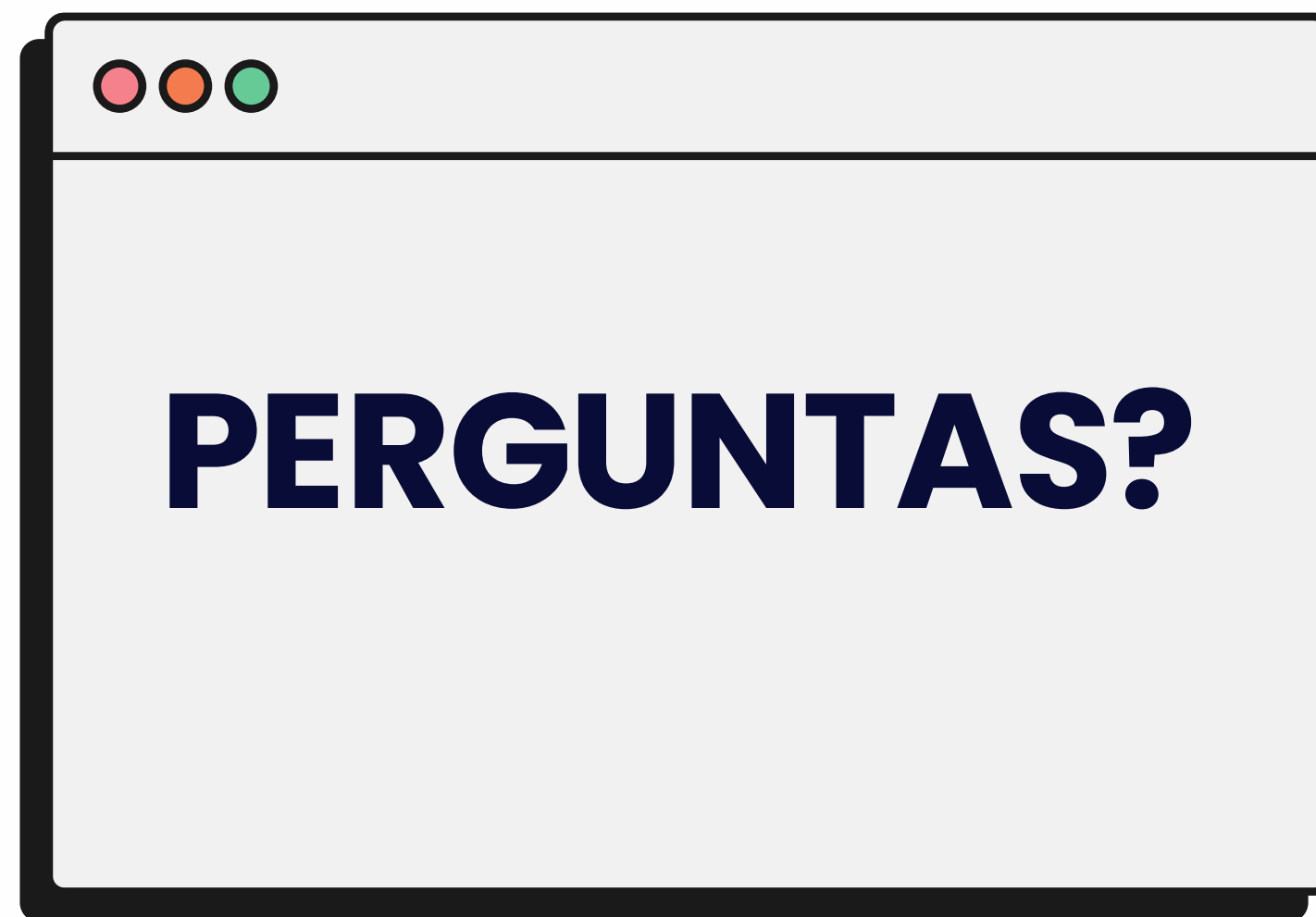


Casa do Código

RODRIGO FERREIRA



owasp.org
owasp.org/www-project-devsecops-guideline
devops.com





OBRIGADO PELA PRESENÇA!

Denis Petri

Co-Founder & CEO

✉ denis.petri@codefortress.com.br

🌐 codefortress.com.br

🌐 [/denispetri](https://www.linkedin.com/in/denispetri)

🌐 [/company/codefortress](https://www.linkedin.com/company/codefortress)

