GTS 33 | PA 05/2019

globo.com

secDevLabs:

Tutorial de Desenvolvimento Seguro

Daniel Carlier
daniel.carlier@corp.globo.com

Silvia Pimpão
silvia.vasquez@corp.globo.com

Agenda - secDevLabs

1. Motivações
2. Planejamento do treinamento
3. Como funciona a dinâmica?
4. Resultados dentro da Globo.com
5. Abordagem GTS 33

1. Motivações

2013

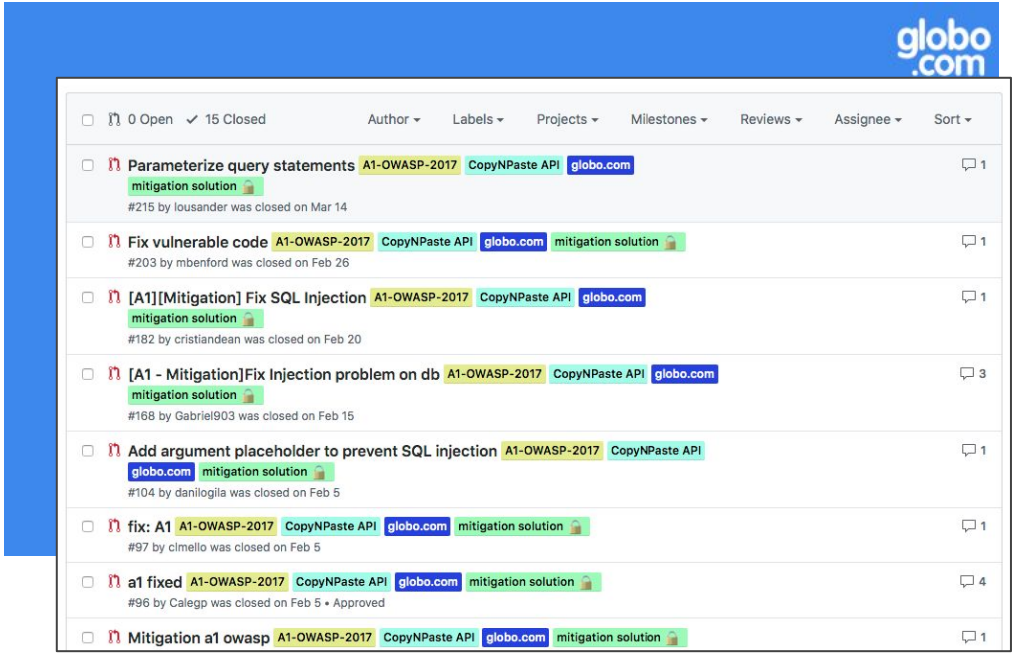
XSS

- Qualquer dado refletido pela aplicação é um possível local vulnerável a XSS
- `<input type="text" name="address" value="myxsstest">`
  - `"><script>alert(1)</script>`
- `<script>var a='myxsstest';var b=123;</script>`
  - `';alert(1); var=foo'`

- Focado em treinar desenvolvedores a encontrar falhas de segurança.
- Focado na parte teórica das vulnerabilidades.
- Realizado fisicamente ao longo de uma semana com 20~30 desenvolvedores por vez.

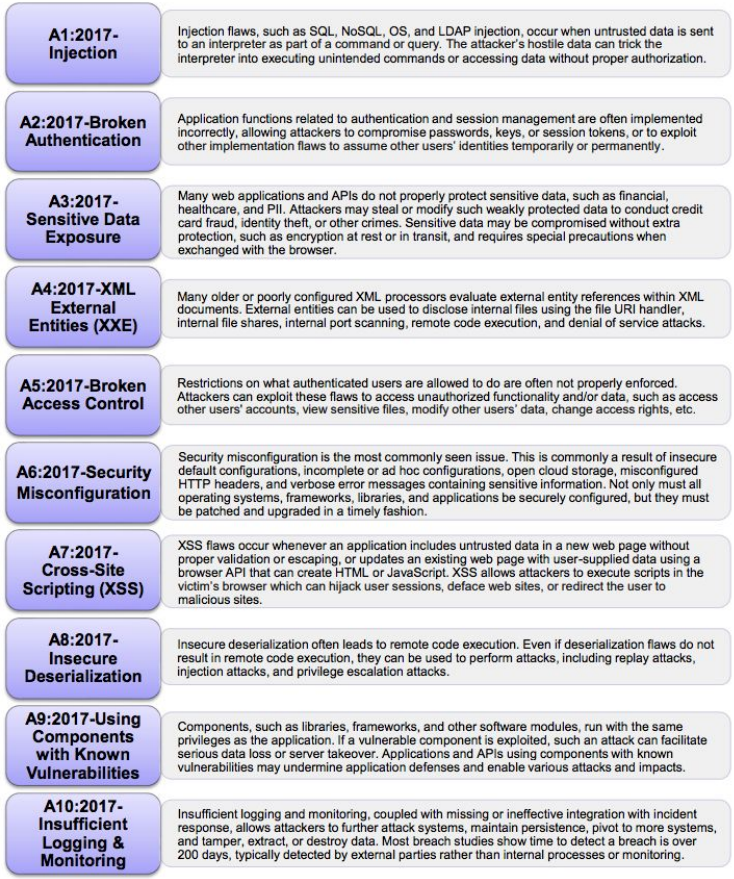
1. Motivações

2019



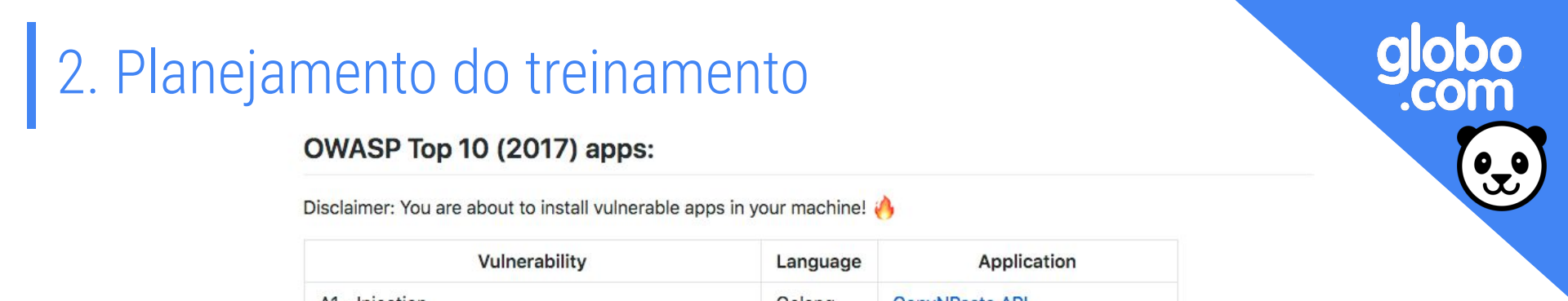
- Focado em treinar desenvolvedores a corrigir falhas de segurança.
- Focado na parte prática das vulnerabilidades.
- Realizado on-line e com a velocidade disponível pelos desenvolvedores.

2. Planejamento do treinamento



O curso apresenta aplicações intencionalmente vulneráveis criadas pelo Time de Segurança da Globo.com baseadas no OWASP Top 10 2017.

2. Planejamento do treinamento



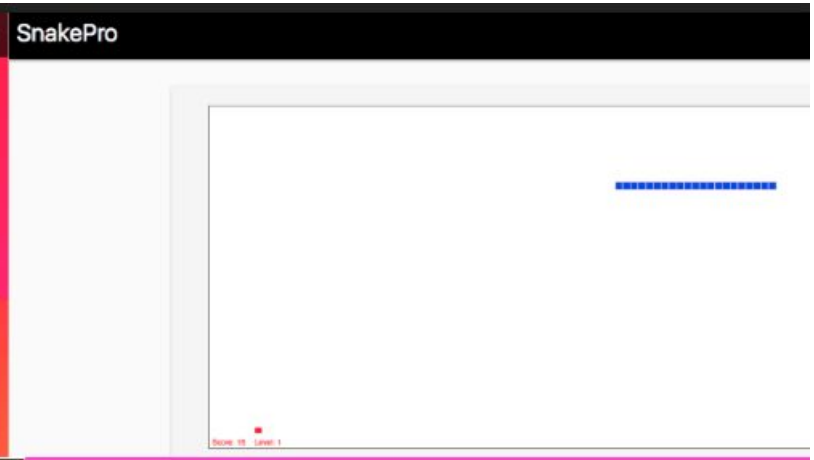
OWASP Top 10 (2017) apps:

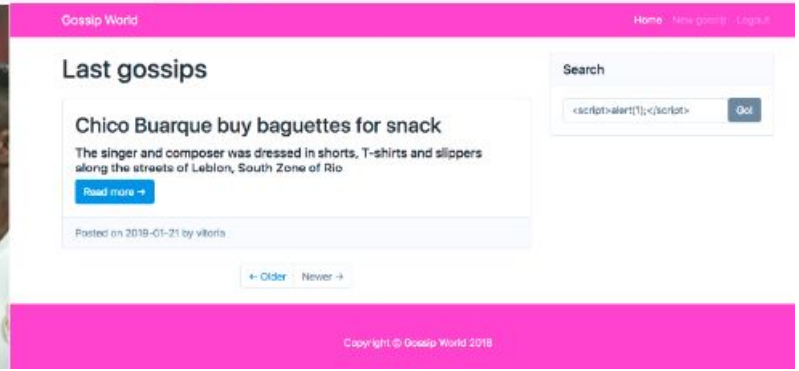
Disclaimer: You are about to install vulnerable apps in your machine! 🔥

Vulnerability	Language	Application
A1 - Injection	Golang	CopyNPaste API
A2 - Broken Authentication	Python	Saidajaula Monster Fit
A2 - Broken Authentication	Golang	Insecure go project
A3 - Sensitive Data Exposure	Golang	SnakePro
A4 - XML External Entities (XXE)	PHP	ViniJr Blog
A5 - Broken Access Control	Golang	Vulnerable Ecommerce API
A6 - Security Misconfiguration	PHP	Vulnerable Wordpress Misconfig
A6 - Security Misconfiguration	NodeJS	Stegonography
A7 - Cross-Site Scripting (XSS)	Python	Gossip World
A8 - Insecure Deserialization	Python	Amarelo Designs
A9 - Using Components With Known Vulnerabilities	PHP	Cimentech
A10 - Insufficient Logging & Monitoring	Python	GamesIrados.com

https://github.com/globocom/secDevLabs

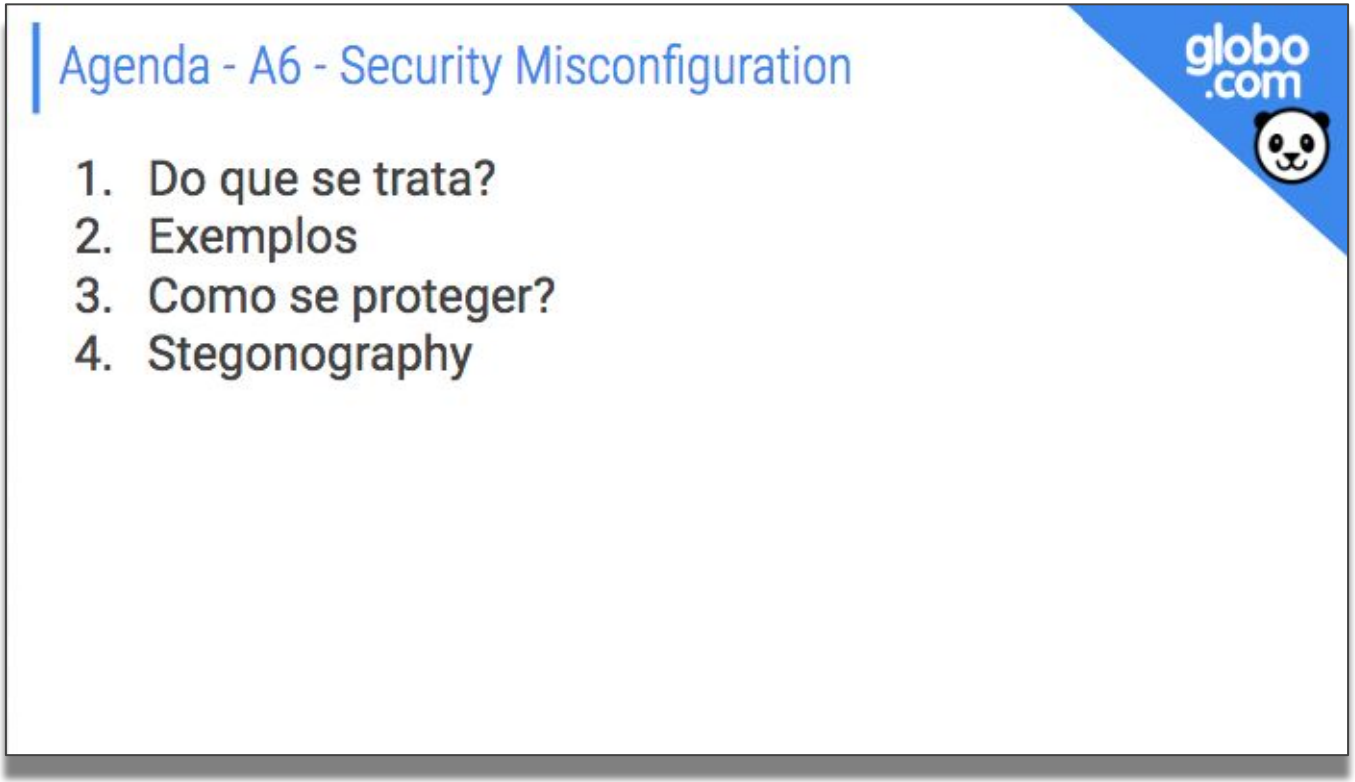
2. Planejamento do treinamento





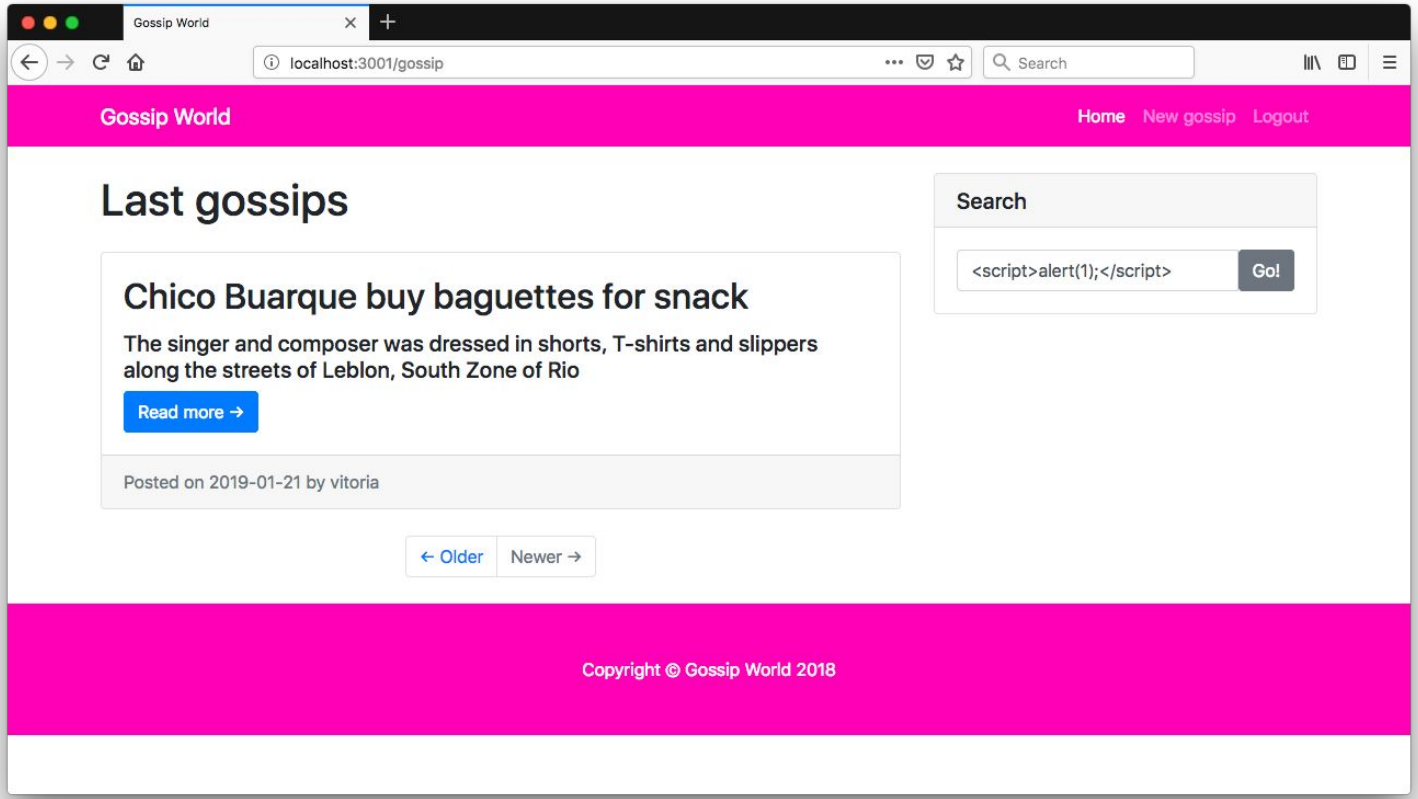
3. Como funciona a dinâmica?

Apresentação do tópico



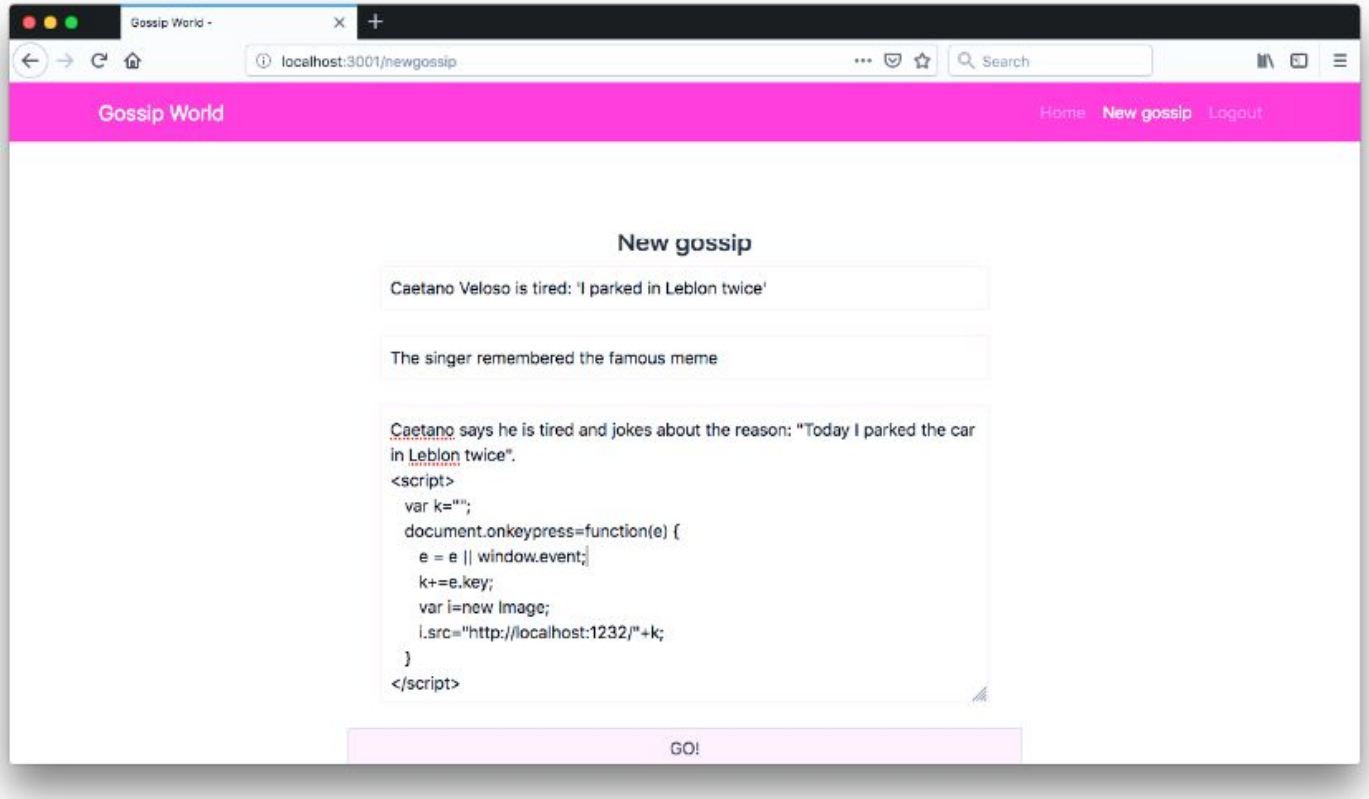
3. Como funciona a dinâmica?

Acesso à aplicação vulnerável



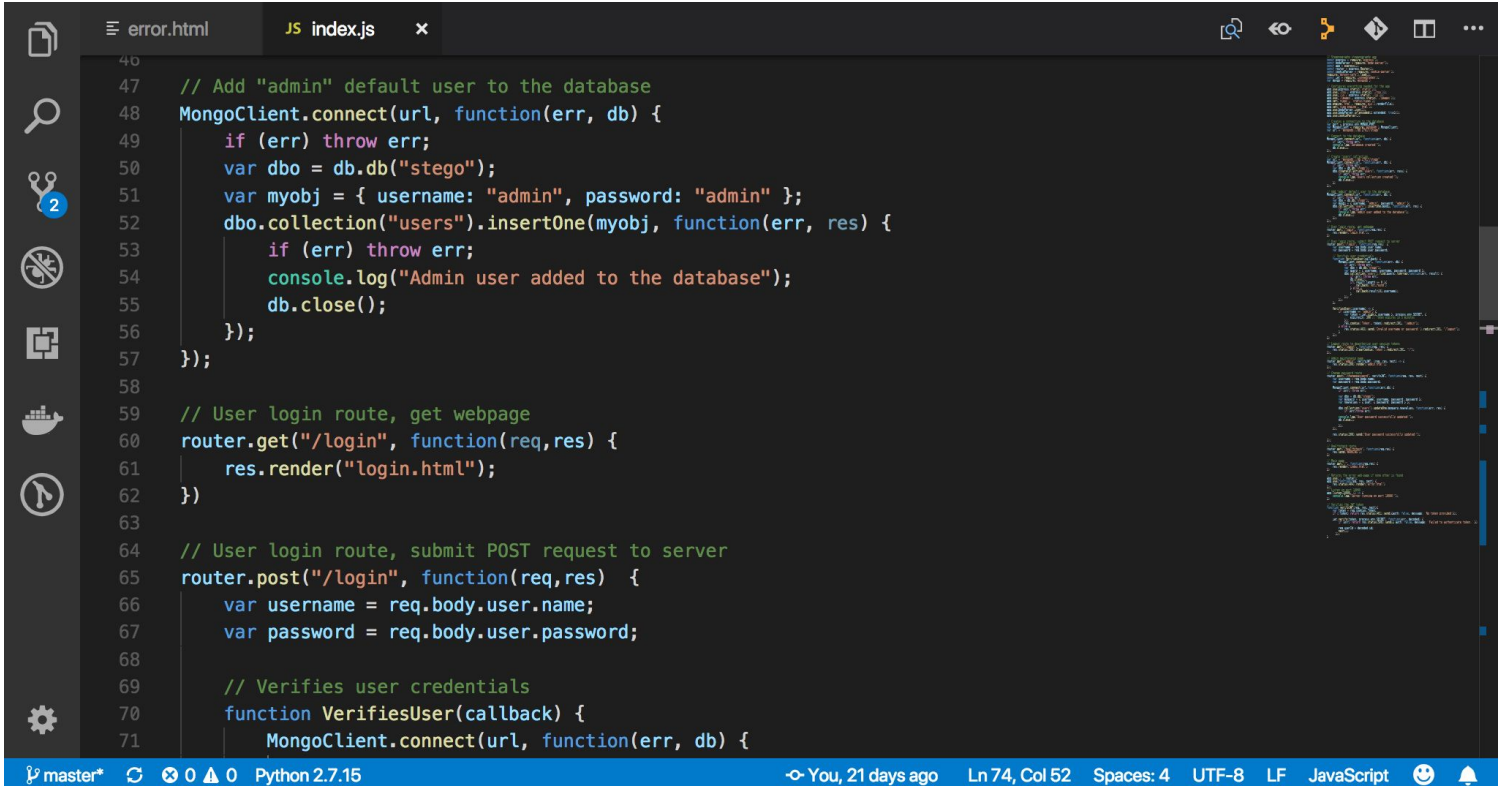
3. Como funciona a dinâmica?

Narrativa de ataque



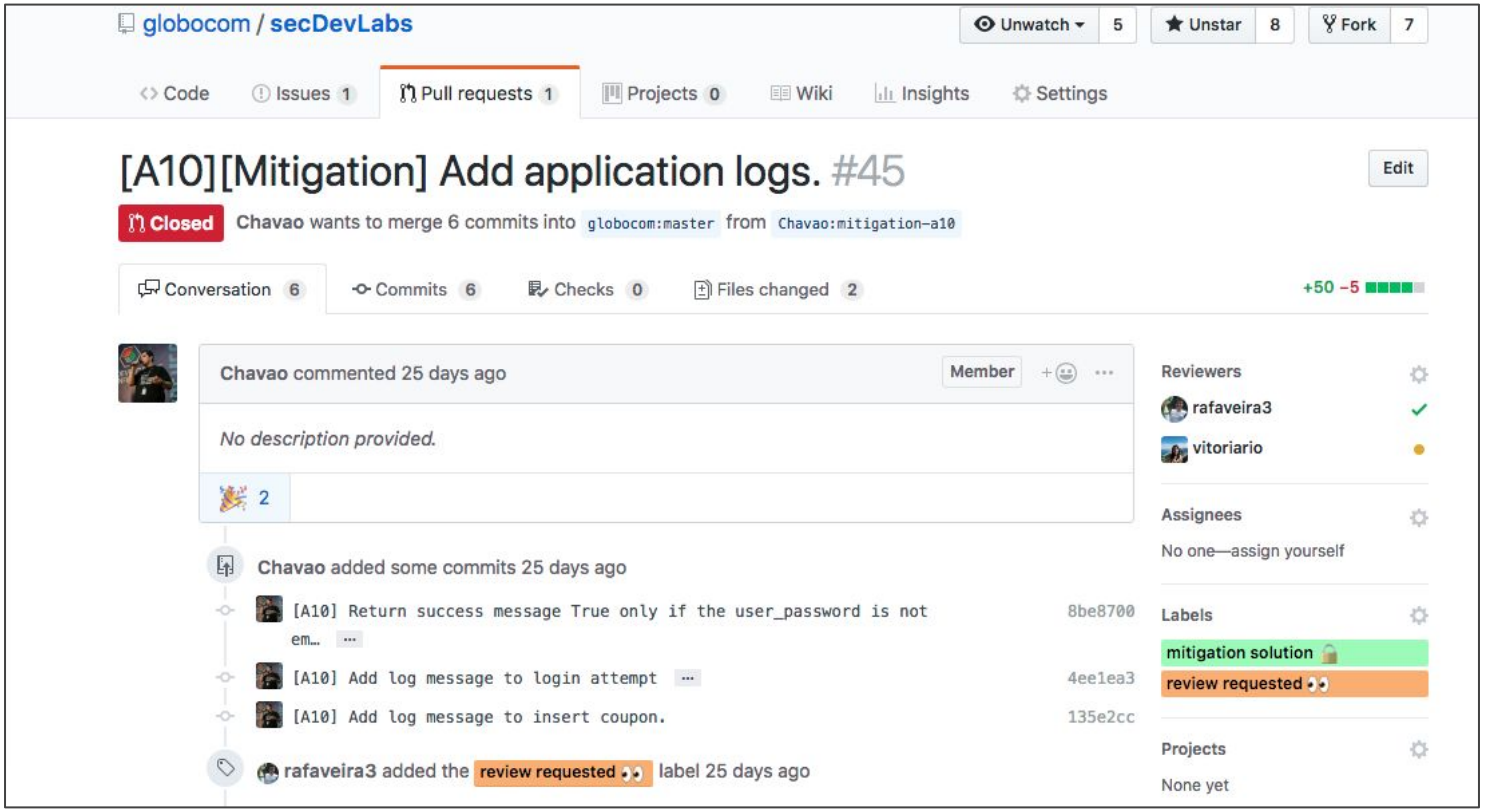
3. Como funciona a dinâmica?

Como você corrigiria as vulnerabilidades?

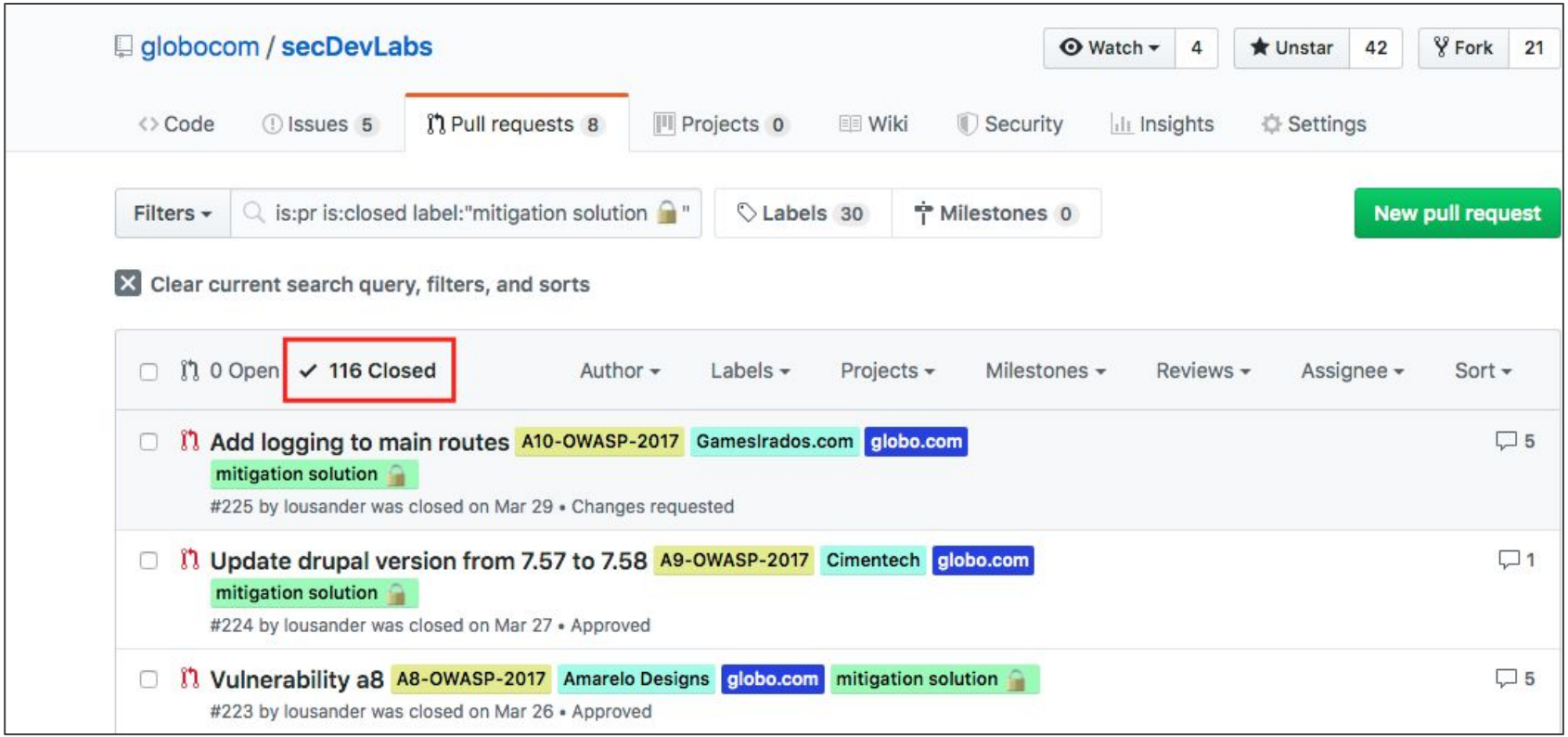


3. Como funciona a dinâmica?

Pull Request com sua mitigação!



4. Resultados dentro da Globo.com



4. Resultados dentro da Globo.com

5. Abordagem GTS 33

5. Abordagem GTS 33

globo.com

8:30 - 10:30 hrs

- A3 - Sensitive Data Exposure
- A4 - External Entities (XXE)

10:30 - 12:30 hrs

- A5 - Broken Access Control
- A6 - Security Misconfiguration
- A7 - Cross Site Scripting (XSS)

14:00 - 15:30 hrs

- A9 - Using Components with Known Vulnerabilities
- A10 - Insufficient Logging & Monitoring

16:00 - 18:00 hrs

- A2 - Broken Authentication
- A1 - Injection
- A8 - Insecure Deserialization

5. Abordagem GTS 33