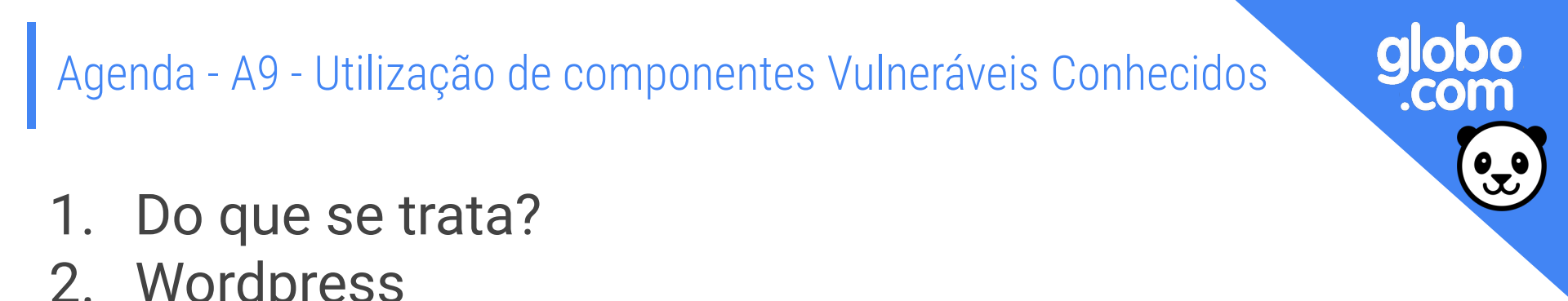
A9 - Using Components with Known Vulnerabilities

globo.com

GTS 33 | PA 05/2019

Agenda - A9 - Utilização de componentes Vulneráveis Conhecidos



1. Do que se trata?
2. Wordpress
3. Google Hacking
4. Safety
5. RetireJS
6. huskyCI
7. Como se proteger?
8. Cimentech

Do que se trata?

globo.com

As aplicações que utilizam componentes com vulnerabilidades conhecidas podem minar as suas defesas e permitir uma gama de possíveis ataques e impactos. Atacantes podem explorar uma única falha de segurança já conhecida podendo causar sérias perdas de dados ou comprometimento do servidor.

Versão 4.9

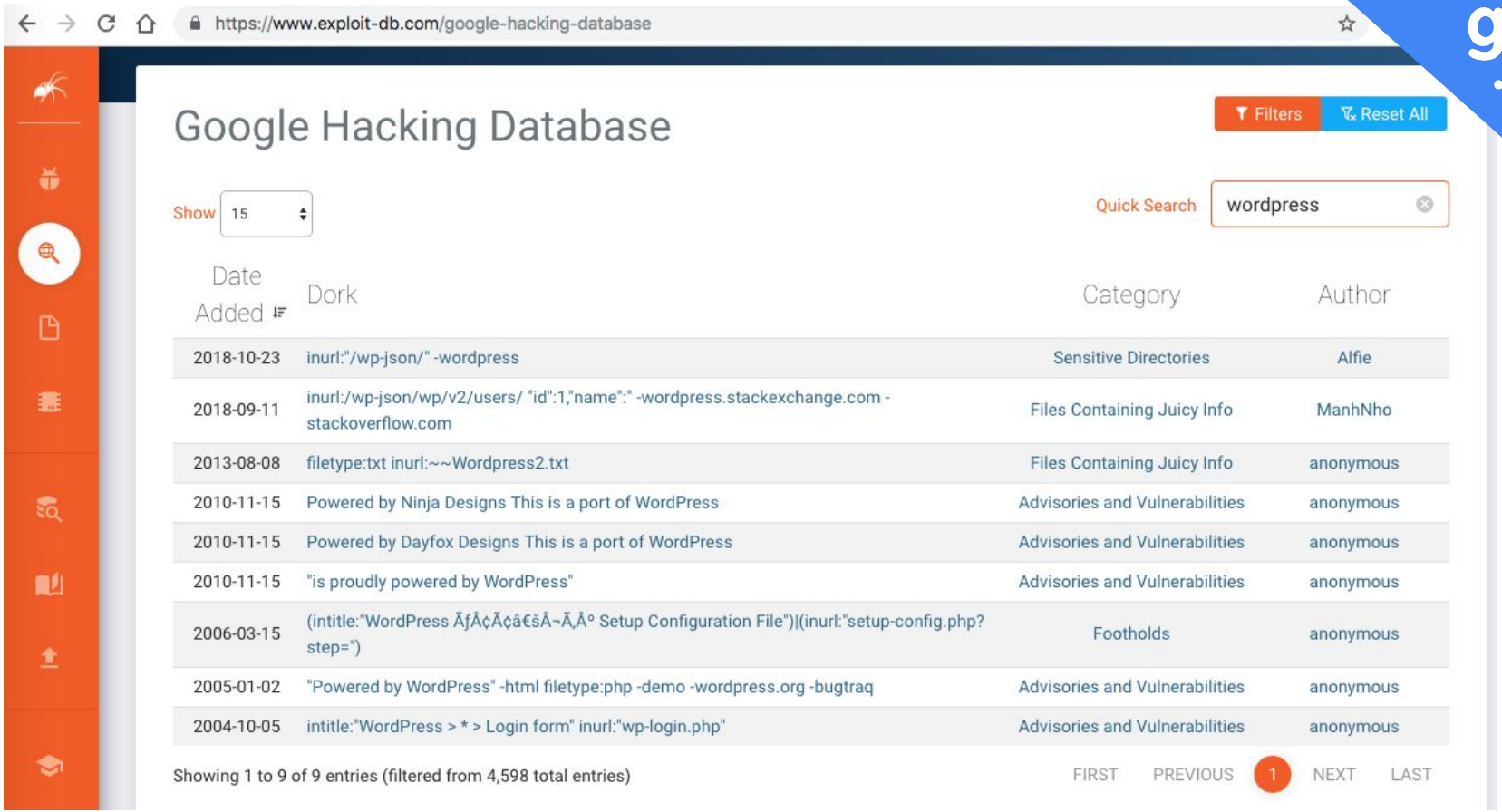
Plataforma de publicação semântica pessoal

Saudações

O WordPress é um projeto muito especial para mim. Todo desenvolvedor e colaborador acrescenta algo único nessa mistura, e juntos nós criamos algo bonito do qual me orgulho de fazer parte. Milhares de horas foram investidas no WordPress, e nós nos dedicamos a melhorá-lo todos os dias. Obrigado por torná-lo parte de seu mundo.

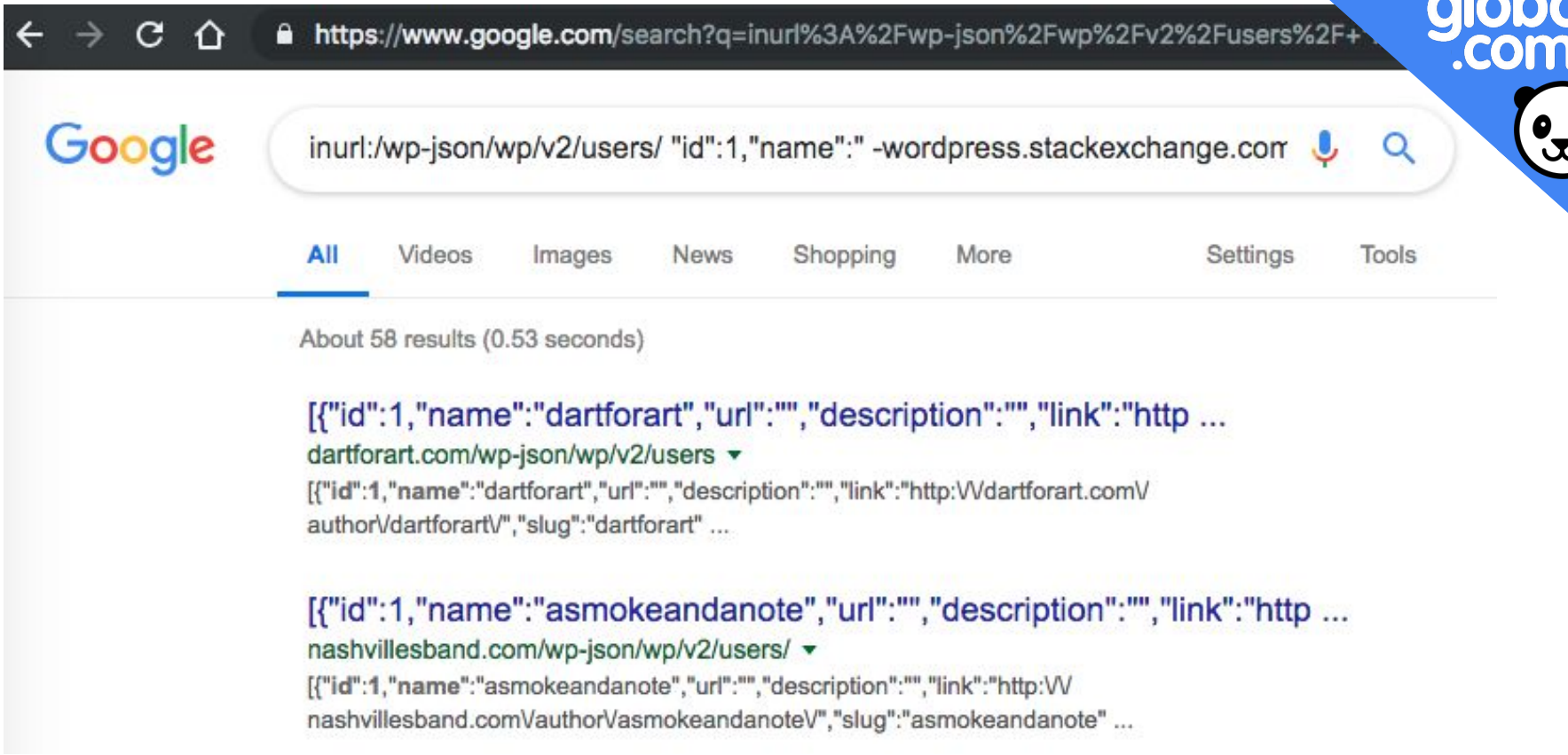
— Matt Mullenweg

Wordpress



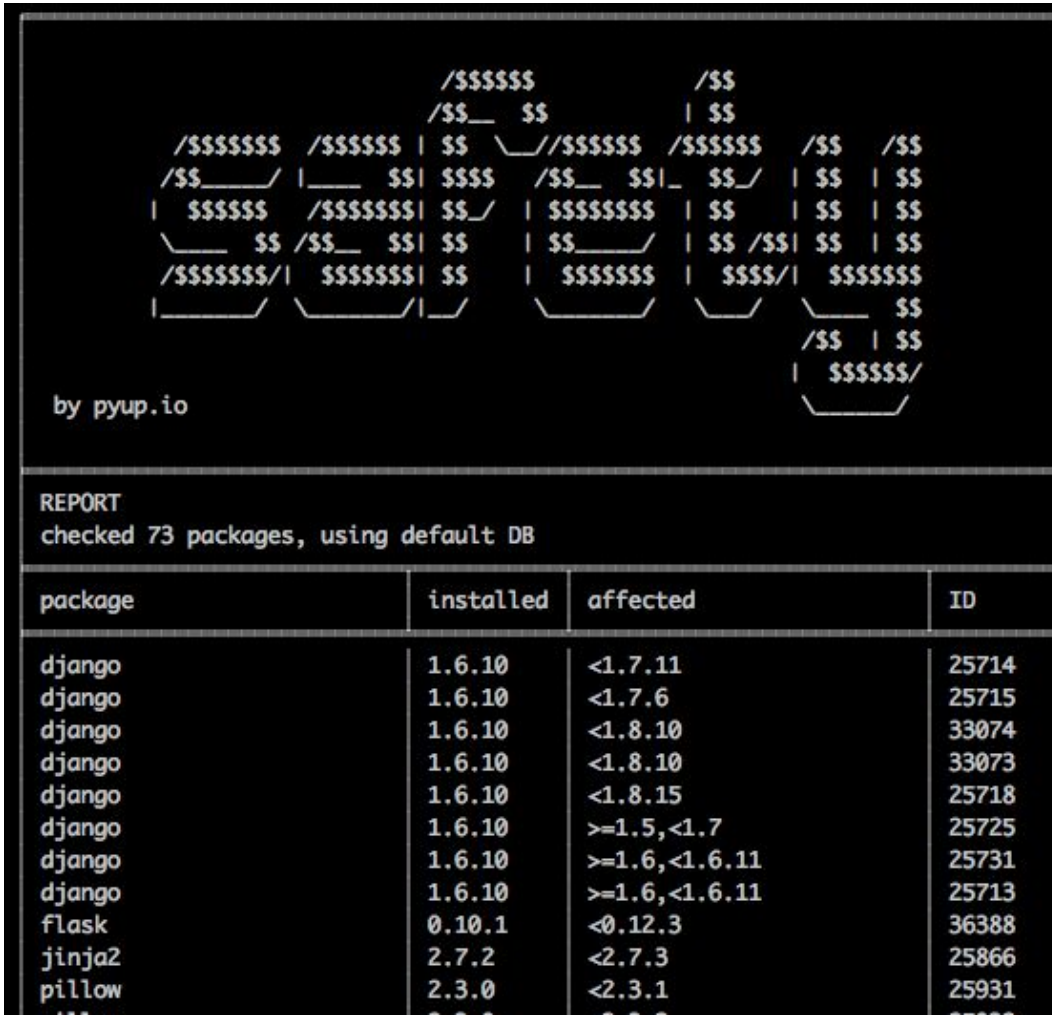
globo.com

Google Hacking



globo.com

Google Hacking


by pyup.io
REPORT
checked 73 packages, using default DB
package | installed | affected | ID
django | 1.6.10 | <1.7.11 | 25714
django | 1.6.10 | <1.7.6 | 25715
django | 1.6.10 | <1.8.10 | 33074
django | 1.6.10 | <1.8.10 | 33073
django | 1.6.10 | <1.8.15 | 25718
django | 1.6.10 | >=1.5,<1.7 | 25725
django | 1.6.10 | >=1.6,<1.6.11 | 25731
django | 1.6.10 | >=1.6,<1.6.11 | 25713
flask | 0.10.1 | <0.12.3 | 36388
jinja2 | 2.7.2 | <2.7.3 | 25866
pillow | 2.3.0 | <2.3.1 | 25931

Safety

```
$ retire
retire.js v2.0.2
Loading from cache: https://raw.githubusercontent.com/RetireJS/retire.js/master/repository/jsrepository.json
Loading from cache: https://raw.githubusercontent.com/RetireJS/retire.js/master/repository/npmrepository.json
node_modules/react-dom/package.json
 ↳react-dom 16.1.1
react-dom 16.1.1 has known vulnerabilities: severity: high; CVE: CVE-2018-6341, summary: RCE affecting some ser
6-4-2.html
node_modules/globule/node_modules/lodash/package.json
 ↳lodash 1.0.2
lodash 1.0.2 has known vulnerabilities: severity: low; summary: Prototype pollution attack; https://hackerone.c
https://hackerone.com/reports/380873
```

RetireJS

globo.com

huskyCI - Performing security tests inside your CI

PASSED

huskyCI is an open source tool that performs security tests inside CI pipelines of multiple projects and centralizes all results into a database for further analysis and metrics.

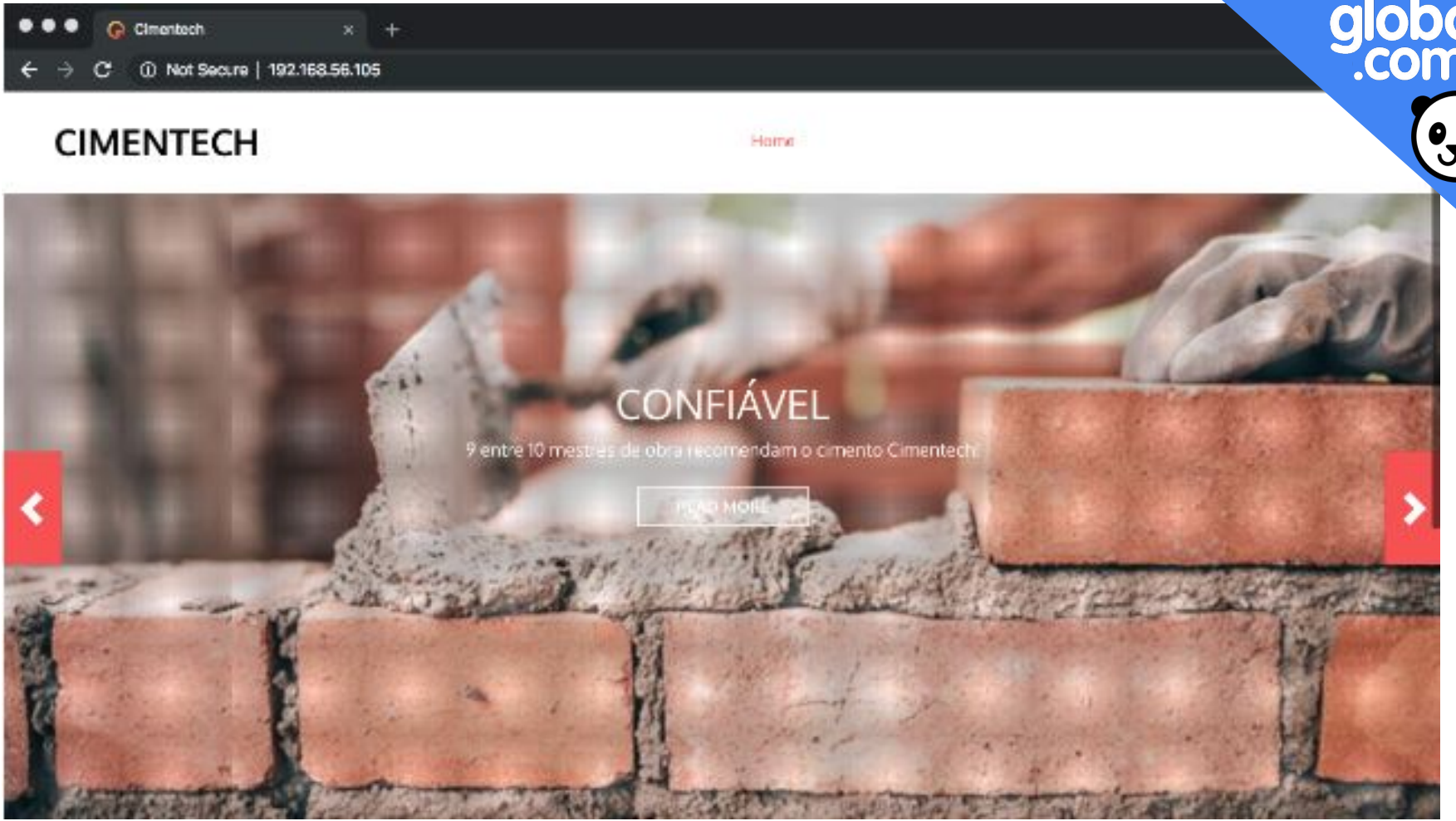
The main goal of this project is to help development teams improve the quality of their code by finding vulnerabilities as soon as possible.

How does it work?

Imagine that an organization has projects like `awesome-golang-project`, `awesome-python-project` and `awesome-ruby-project`. In each project's CI configuration file, the following example code may be included:

Como se prevenir?

1. **Identificar** todos os componentes e as versões utilizadas, incluindo todas as dependências. (ex., versões dos plugins). 📚
2. **Monitorar** componentes que não recebem mais manutenção ou que não recebem mais atualizações de segurança. 🔓
3. Manter os componentes sempre **atualizados** na versão estável mais recente. 👶


Cimentech
Not Secure | 192.168.56.105
CIMENTECH
Home
CONFIÁVEL
9 entre 10 mestres de obra recomendam o cimento Cimentech
READ MORE

Narrativa do ataque

Hands on!

1. Entrar na pasta da app

```
$ cd owasp-top10-2017-apps/a9/cimentech
```

2. Inicializar o container

```
$ make install
```

3. Acessar a página

```
localhost:80
```

globo.com

A9 - Using Components with Known Vulnerabilities