

A9 - Using Components with Known Vulnerabilities





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?



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



Google Hacking Database

Filters Reset All

Show 15

Quick Search

Date Added	Dork	Category	Author
2018-10-23	<code>inurl:"wp-json/"-wordpress</code>	Sensitive Directories	Alfie
2018-09-11	<code>inurl:/wp-json/wp/v2/users/"id":1,"name:"-wordpress.stackexchange.com-stackoverflow.com</code>	Files Containing Juicy Info	ManhNho
2013-08-08	<code>filetype:txt inurl:~~Wordpress2.txt</code>	Files Containing Juicy Info	anonymous
2010-11-15	<code>Powered by Ninja Designs This is a port of WordPress</code>	Advisories and Vulnerabilities	anonymous
2010-11-15	<code>Powered by Dayfox Designs This is a port of WordPress</code>	Advisories and Vulnerabilities	anonymous
2010-11-15	<code>"is proudly powered by WordPress"</code>	Advisories and Vulnerabilities	anonymous
2006-03-15	<code>(intitle:"WordPress ÃfÃçÃâÃšÃ~Ã,Ã° Setup Configuration File")(inurl:"setup-config.php?step=")</code>	Footholds	anonymous
2005-01-02	<code>"Powered by WordPress" -html filetype:php -demo -wordpress.org -bugtraq</code>	Advisories and Vulnerabilities	anonymous
2004-10-05	<code>intitle:"WordPress > * > Login form" inurl:"wp-login.php"</code>	Advisories and Vulnerabilities	anonymous

Showing 1 to 9 of 9 entries (filtered from 4,598 total entries)

FIRST PREVIOUS **1** NEXT LAST



https://www.google.com/search?q=inurl%3A%2Fwp-json%2Fwp%2Fv2%2Fusers%2F+



inurl:/wp-json/wp/v2/users/ "id":1,"name": " -wordpress.stackexchange.com



All

Videos

Images

News

Shopping

More

Settings

Tools

About 58 results (0.53 seconds)

`{"id":1,"name":"dartforart","url":"","description":"","link":"http ...`
dartforart.com/wp-json/wp/v2/users ▾

`{"id":1,"name":"dartforart","url":"","description":"","link":"http://dartforart.com/v/author/dartforart/","slug":"dartforart" ...`

`{"id":1,"name":"asmokeandanote","url":"","description":"","link":"http ...`
nashvillesband.com/wp-json/wp/v2/users/ ▾

`{"id":1,"name":"asmokeandanote","url":"","description":"","link":"http://nashvillesband.com/v/author/asmokeandanote/","slug":"asmokeandanote" ...`



```

                /$$$$$$
                /$$__ $$
    /$$$$$$$ /$$$$$$ | $$ \ /$$$$$$ /$$$$$$ /$$ /$$
    /$$____/ |__ $$ | $$$ /$$__ $$ | $$ / | $$ | $$
    | $$$$$ /$$$$$$$ | $$ / | $$$$$$ | $$ | $$ | $$
    \__ $$ /$$__ $$ | $$ | $$____/ | $$ /$$ | $$ | $$
    /$$$$$$$/ | $$$$$$ | $$ | $$$$$$ | $$$$/ | $$$$$$
    |_____/ |_____/ | / |_____/ |_____/ |_____/ $$
                                     /$$ | $$
                                     | $$$$$$/
    
```

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
jinj2	2.7.2	<2.7.3	25866
pillow	2.3.0	<2.3.1	25931



```
$ 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 se
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.
https://hackerone.com/reports/380873
```




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

Home



CONFIÁVEL

9 entre 10 mestres de obra recomendam o cimento Cimentech

LEIA MAIS





Narrativa do ataque



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
```



A9 - Using Components with Known Vulnerabilities