

WORDCAMP SANTANDER  
Noviembre 2016

# Seguridad en WordPress

## Recogiendo Información





# Técnicas de los “malos”

- Scripts personalizados (avanzado)

# Técnicas de los “malos”

## Explotación de vulnerabilidades (avanzado)

WPScan Vulnerability Database:

[wpvulndb.com](http://wpvulndb.com)

Exploit Database:

[www.exploitalert.com](http://www.exploitalert.com)

[www.exploitalert.com/search-results.html?search=wordpress](http://www.exploitalert.com/search-results.html?search=wordpress)

Google Dorks: Utilizando Google para encontrar webs vulnerables.

["index of" inurl:wp-content](https://www.google.com/search?q=\)

[www.exploit-db.com/google-hacking-database/](http://www.exploit-db.com/google-hacking-database/)

# Técnicas de los “malos”

- Acceso al panel de control de nuestro WordPress



Nombre de usuario o correo electrónico

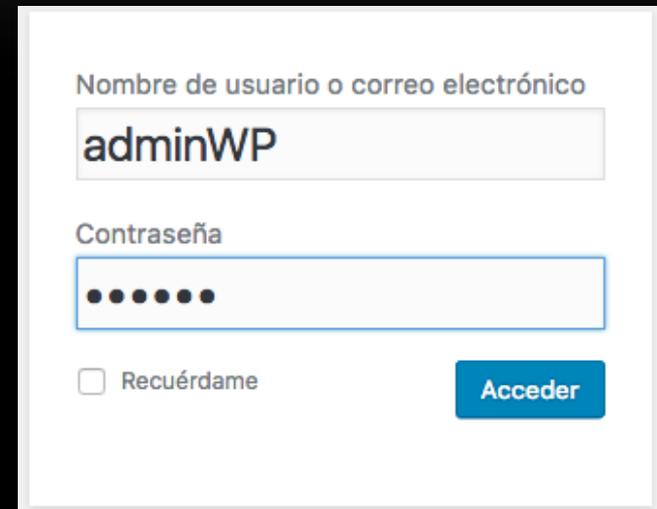
Contraseña

Recuérdame

# Acceso al Panel

¿Qué necesitamos?

- Usuario
- Contraseña



A screenshot of a WordPress login form. The form is white with a light gray border. It contains the following elements:

- A label "Nombre de usuario o correo electrónico" above a text input field containing "adminWP".
- A label "Contraseña" above a password input field containing six black dots.
- A checkbox labeled "Recuérdame" to the left of a blue "Acceder" button.

- ◉ ¿Cómo conseguir el usuario?
  - Autor del post: *miweb.com/author/admin*
  - WPScan

# WPScan

- ◉ Vamos a conseguir los usuarios de una instalación.
- ◉ Demo

**escanear todo (no intrusivo)**

```
wpscan --url http://dymweb.es
```

**escanear usuarios**

```
wpscan --url http://dymweb.es --enumerate u
```

**escanear plugins**

```
wpscan --url http://dymweb.es --enumerate p
```

# Consejos para evitar esto

- ◉ Utiliza un WAF
- ◉ Esconde la ruta a tu panel de control: itthemes security, All in One Wp Security, etc
- ◉ Contraseña de más de 12 caracteres alfanuméricos
- ◉ Modificar el nombre del usuario (~~admin~~)
- ◉ No publiques desde el usuario administrador

# Ya tenemos el usuario

## ¿Y ahora qué?

- ◉ Pues a por la contraseña ;)
- ◉ ¿Cómo la consigo?
  - Conociéndola
  - Técnicas de ingeniería Social
  - Teniendo acceso al email de administrador y usando “he olvidado mi contraseña”.
  - Utilizando la información que hay en internet para intentar “adivinarla”

# Recogida de datos

1. Directamente del sistema para aprender más sobre su configuración y comportamiento.
2. Recabando pistas y datos que se encuentran en internet (OSINT)

# Recogida de datos en WordPress

Tema activo y Plugins

[whatwpthemeisthat.com](http://whatwpthemeisthat.com)

[wpthemedetector.com](http://wpthemedetector.com)

[scanwp.net](http://scanwp.net)

# Recogida de datos en WordPress

- ◉ WPScan
- ◉ WPDoctor ([www.wpdoctor.es](http://www.wpdoctor.es))
- ◉ FOCA
- ◉ Wappalizer (complemento Firefox)
- ◉ [Built width](#)

# HERRAMIENTAS OSINT

Recogida de datos a través de la información existente en internet

[osintframework.com](http://osintframework.com)

[netbootcamp.org/osinttools/](http://netbootcamp.org/osinttools/)

[inteltechniques.com](http://inteltechniques.com)

[rr.reuser.biz](http://rr.reuser.biz)

[www.toddington.com/resources/](http://www.toddington.com/resources/)

# Nuestro ataque

- Crear el diccionario con “Crunch”

```
crunch 8 8 -t ,@@web%% > /root/Desktop/palabros1.lst
```

- Utilizar el archivo de diccionario en WPScan

```
ruby ./wpscan.rb --url www.dymweb.es --wordlist diccionario.lst --username admin
```

# Contraseñas

Generadores de contraseñas:

[www.clavesegura.org](http://www.clavesegura.org)

[randomkeygen.com](http://randomkeygen.com)



Auditar cómo de fuerte es una contraseña:

[www.passwordmeter.com](http://www.passwordmeter.com)

# Muchas gracias

Tomás Sierra Campos  
@Tomycant

