

Taller de Seguridad básica en WordPress



+



WORDPRESS

OWASP

#WHOAMI



Juan José Domenech

@juanjodomenech



Ramón Salado

@ramon_salado

#OWASP



Organización sin ánimo de lucro a nivel mundial, dedicada a mejorar la seguridad de las aplicaciones web

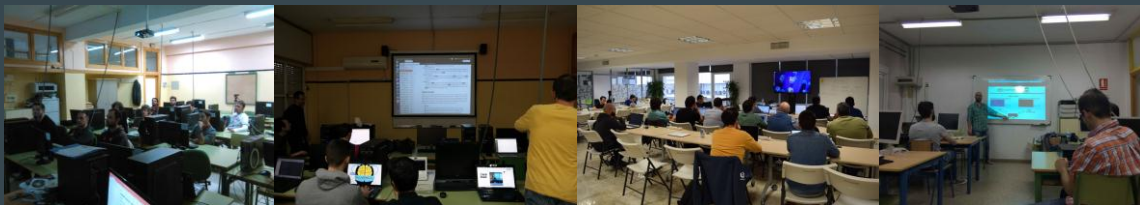
Cualquiera puede participar en OWASP, todos sus proyectos y documentación están disponibles gratuitamente

OWASP SEVILLA



Organizamos un evento mensual abierto a todo el que quiera participar

Proyectos: Divulgación sobre Seguridad y Traducción GUÍA DE TESTING 4



WORDCAMP
SEVILLA16
#WCSevilla16

@OWASP_Sevilla

OWASP, PRINCIPALES PROYECTOS

A1 – Injection

A2 – Broken Authentication and Session Management

A3 – Cross-Site Scripting (XSS)

A4 – Insecure Direct Object References

A5 – Security Misconfiguration

A6 – Sensitive Data Exposure

A7 – Missing Function Level Access Control

A8 – Cross-Site Request Forgery (CSRF)

A9 – Using Known Vulnerable Components

A10 – Unvalidated Redirects and Forwards



SEGURIDAD

Equipos seguros

Comunicaciones Seguras (wifi, vpn, ...)

Contraseñas robustas (doble factor, cambios periódicos, ...)

Precauciones BYOD y teletrabajo

¿Es WordPress inseguro?

¿Qué lo hace inseguro?

SEGURIDAD WordPress

INFRAESTRUCTURA
DE RED



CONFIGURACIÓN
SERVIDOR



INSTALACIÓN
WORDPRESS



HARDENING
WORDPRESS



SEGURIDAD WordPress

Infraestructura de red

¿Compartido? ¿VPS? ¿Dedicado? ¿Con o sin soporte?

Cifrado de discos

¡SSH y SFTP siempre!

Backups

¡Últimas versiones! (Apache/NGINX, PHP, MySQL, ...)

Logs y analizadores de tráfico



SEGURIDAD WordPress

Configuración del Servidor

Utilizar directivas *Allow* y *Deny* para restringir accesos al servidor

Deshabilitar listado de directorios y módulos innecesarios

Permisos de los directorios “mínimos”

WAF: Mod_Security

Fortificar PHP y MySQL

HTTP 1.1 / 2.0 y HTTPS

```
$ sudo apt-get install libapache2-mod-security  
$ sudo a2enmod mod-security  
$ sudo /etc/init.d/apache2 force-reload
```

SEGURIDAD WordPress

Instalación de WordPress

No utilizar usuario “admin”

Fortificar contraseña

No utilizar prefijos de tablas “wp_”

Cuidado con robots.txt, readme.html

¡Personaliza todo!

Permisos

No abusar de plugins



The screenshot shows the WordPress installation database configuration screen. At the top is the WordPress logo. Below it, a note says: "Below you should enter your database connection details. If you're not sure about these, contact your host." The form contains five rows of input fields with labels and descriptions:

Field Label	Value	Description
Database Name	wordpress	The name of the database you want to run WP in.
User Name	root	Your MySQL username
Password	admin	...and MySQL password.
Database Host	localhost	99% chance you won't need to change this value.
Table Prefix	wp_	If you want to run multiple WordPress installations in a single database, change this.

At the bottom of the form is a "Submit" button.

SEGURIDAD WordPress

Hardening WordPress

Core, themes y plugins actualizados

Roles adecuados para cada uso








Cambiar id del usuario 1

Alias distinto del nombre de usuario

Ocultar wp-admin, wp-login, ...

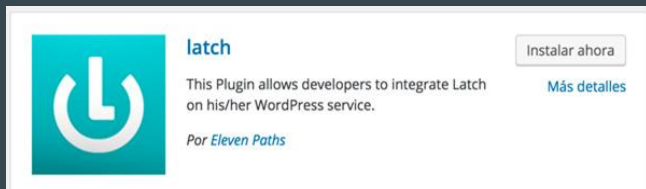
Control de comentarios

No utilizar plugins de “dudosa procedencia”

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

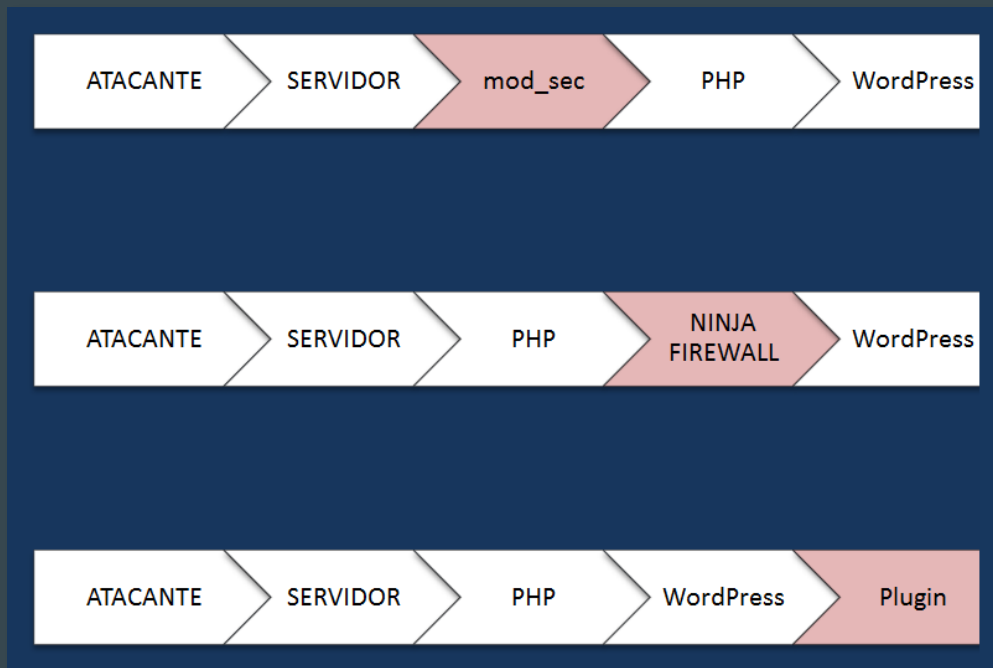
SEGURIDAD WordPress

Hardening WordPress, con Plugins



SEGURIDAD WordPress

Hardening WordPress, con Plugins



SEGURIDAD WordPress

Hardening WordPress

Configuración 'default' muy completa

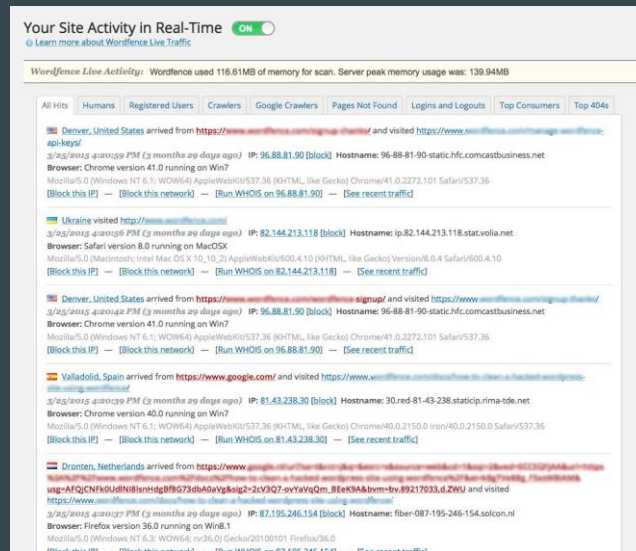
Incluye varios niveles preconfigurados

Verifica core, themes y plugins con WordPress

Cortafuegos para bloquear amenazas

Limita intentos de login y uso de blacklist

Visión en tiempo real de todo el tráfico



SEGURIDAD WordPress

Hardening WordPress

WAF por plugin

Gran motor de filtrado

Protección XSS, SQLi, ...

Protege API XML-RPC

A screenshot of the "Login Protection" settings page in the Ninja Firewall plugin. The page has a light gray background and a blue header bar with the "Ninja Firewall" logo and a "Help" link. The settings are organized into sections with radio buttons and checkboxes. The "Enable brute force attack protection" section has three options: "Yes, if under attack" (selected), "Always ON", and "No (default)". The "Protect the login page against" section has three options: "GET request attacks", "POST request attacks (default)" (selected), and "GET and POST requests attacks". The "Password-protect it" section has input fields for "For 5 minutes, if more than 8 POST requests within 15 seconds." and a checkbox for "Apply the protection to the xmlrpc.php script as well." The "HTTP authentication" section has fields for "User: ninjatech" and "Password: *****" with a note "User and Password must be from 6 to 32 characters." and a "Message (max. 150 ASCII characters): Access restricted" field. The "AUTH log" section has a checkbox for "Write incident to the server AUTH log." and a note "See contextual help before enabling this option." At the bottom, there is a blue "Save Login Protection" button and a link to "See our benchmark and stress-test: WordPress brute-force attack detection plugins comparison, WordPress brute-force attack protection in a production environment."

SEGURIDAD WordPress

Hardening WordPress

Security Check

Cambiar la ruta de /wp-admin

Verifica los permisos de las carpetas

WordPress Tweaks



Security Status

All High Medium Low Completed

High Priority

These are items that should be secured immediately.

- Your site is not performing any scheduled database backups. [Fix it](#)
- Malware scanning is not enabled. [Fix it](#)

Medium Priority

These are items that should be secured if possible however they are not critical to the overall security of your site.

- Your website is not protected against bots looking for known vulnerabilities. Consider turning on 404 protection. [Fix it](#)
- Your WordPress Dashboard is available 24/7. Do you really update 24 hours a day? Consider using Away Mode. [Fix it](#)
- Your login area is partially protected from brute force attacks. We recommend you use both network and local blocking for full security. [Fix it](#)
- Your website is not looking for changed files. Consider turning on file change detections. [Fix it](#)
- Your WordPress Dashboard is using the default addresses. This can make a brute force attack much easier. [Fix it](#)

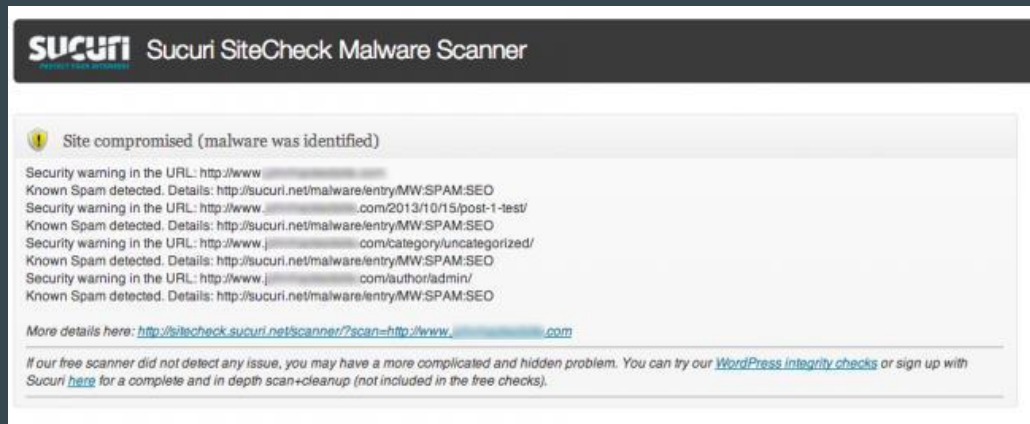
SEGURIDAD WordPress

Hardening WordPress

Escaneo en busca de malware en nuestra web

Reforzar la seguridad de tu sitio Web

CloudProxy (\$)



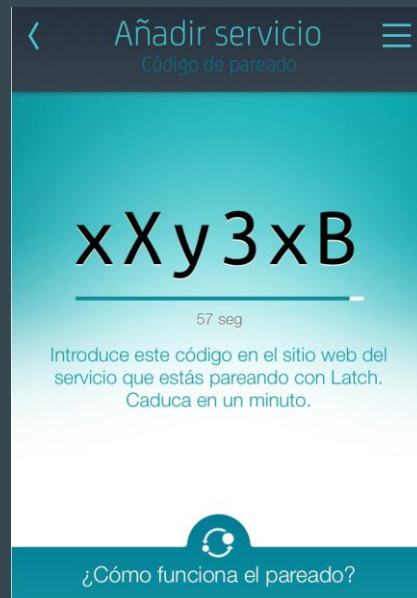
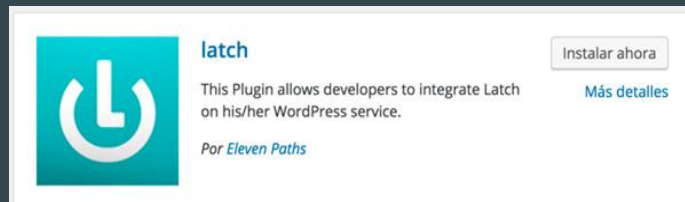
SEGURIDAD WordPress

Hardening WordPress

Doble factor de autenticación

Bloquear acceso para inactividad

Alertas de intentos de acceso



SEGURIDAD WordPress

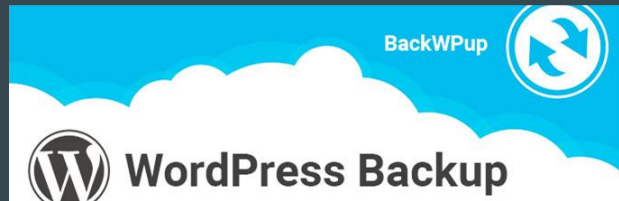
Hardening WordPress

Posibilidad de automatizar backups

Archivos + Base de Datos

Aloja en servicios externos (drive, dropbox, ...)

Archivos zip con password



BackWPup > Job: lokal

General Schedule DB Backup Files XML export Plugins DB Check To: Folder

Job Name

Please name this job.

Job Tasks

This job is a ...

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

Backup File Creation

Archive name

Preview: backwpup_d2d010_2016-05-12_16-43-37.zip

SEGURIDAD WordPress

Hardening WordPress, Otros



AUDITANDO WordPress

Wpscan. Instalación

Listar vulnerabilidades y enumeración de usuarios

Ataque fuerza bruta

Algunos ejemplos de la Guia Testing (ghdb, robots, xss, ...)

eval, base64, ...

Taller de Seguridad básica en WordPress



GRACIAS