

Segurització de WordPress

Description

1. Introducció i Objectius

L'objectiu principal d'aquesta pràctica és implementar un conjunt de mesures de seguretat fonamentals en una instal·lació de WordPress per tal de protegir el lloc web contra vulnerabilitats comunes, atacs de força bruta, intrusions no autoritzades i pèrdua de dades.

2. Mesures de Seguretat Recomanades Aplicades

A continuació es detallen els passos realitzats per garantir una configuració segura de l'entorn:

2.1. Actualitzacions del Sistema i Plugins

- Actualització del Nucli (Core):** S'ha verificat que la versió de WordPress estigui actualitzada a la darrera versió estable per corregir vulnerabilitats conegudes.
- Gestió de Plugins i Temes:** S'han eliminat tots els plugins i temes inactius o en desús per reduir la superfície d'atac. Els plugins actius s'han actualitzat a la seva última versió.

2.2. Enfortiment de l'Autenticació i Gestió d'Usuaris

- Canvi d'Usuari Administrador:** S'ha evitat l'ús del nom d'usuari per defecte (admin), creant un usuari administrador amb un nom personalitzat i eliminant el perfil inicial.
- Contrasenyes Segures:** S'ha establert una política de contrasenyes complexes (mínim 12 caràcters, combinant lletres majúscules, minúscules, números i símbols).
- Autenticació de Dos Factors (2FA):** S'ha configurat la verificació en dos passos per a tots els usuaris amb rols d'administració i edició.

2.3. Protecció del Fitxer de Configuració i Permisos

- Modificació de wp-config.php:** S'han afegit regles per deshabilitar l'edició de fitxers des del panell d'administració:
- PHP

```
define('DISALLOW_FILE_EDIT', true);
```

- Permisos de Fitxers i Directoris:** S'han ajustat els permisos en el servidor per seguir les bones pràctiques:
 - Directoris: 755 o 750
 - Fitxers: 644 o 640

- Fitxer wp-config.php: 600 o 400

2.4. Instal·laci3 i Configuraci3 de Plugin de Seguretat

- Sâ??ha implementat i configurat un plugin especialitzat en seguretat (com Wordfence, iThemes Security o All in One WP Security) per incloure:
 - Protecci3 contra atacs de forsa bruta (limitaci3 dâ??intents dâ??inici de sessi3).
 - Canvi de la URL dâ??acc3s per defecte (wp-admin / wp-login.php).
 - Escaneig peri2dic de malware i fitxers alterats.

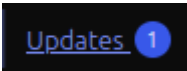
2.5. C2pies de Seguretat (Backups)

- Sâ??ha programat un sistema de c2pies de seguretat autom2tiques (base de dades i fitxers) amb emmagatzematge extern segur.

3. Estructura del Portafolis i Directori Equip

- Sâ??ha integrat aquesta documentaci3 en la p2gina directori del portafolis.
- Es garanteix la vinculaci3 correcta i funcional dels enllaços entre els diferents integrants de lâ??equip de treball.

Evid2ncies



Category

1. 7i,â?£ - 3??• - Portfoli digital
2. Repte 1.1

Date Created

October 2, 2026

Author

sachcharifi