

Acc  s a l  administraci   de WordPress

Description

Descripci   i objectiu del treball

L  objectiu d  aquest treball   s configurar i documentar de manera segura i professional l  acc  s a l  administraci   d  un lloc web basat en WordPress. Per aconseguir un entorn de treball protegit i eficient, s  implementa un model de permisos personalitzat ajustat al principi de m  nim privilegi, aix   com un sistema d  autenticaci   de doble factor (2FA) per bl blindar l  acc  s administratiu davant d  amenaces externes. A m  s, es realitzen les verificacions corresponents per assegurar el correcte funcionament de totes les configuracions aplicades.

Desenvolupament pas a pas

1. Justificaci   del model de permisos i de la doble autenticaci   (2FA)

- Model de permisos triat:** Per garantir una gesti   segura i organitzada, s  aplica el *principi de m  nim privilegi*. Cada usuari rep   nicament el rol i els permisos estrictament necessaris per dur a terme les seves tasques (per exemple, Administrador, Editor, Autor o rols personalitzats). D  aquesta manera, es redueix considerablement el risc d  accions no autoritzades, modificacions accidentals en la configuraci   del lloc o alteracions cr  tiques del sistema.
- Necessitat de la doble autenticaci   (2FA):** En un entorn publicat a Internet, els panells d  administraci   de WordPress (/wp-admin o /wp-login.php) s  n cont  nuament objecte d  atacs automatitzats (com els atacs de for  sa bruta, fusteria de credencials o navegaci   de diccionari). La implementaci   d  un sistema de doble factor afegeix una capes addicional de seguretat vital: tot i que un atacant aconseguixi obtenir o desxifrar la contrasenya d  un usuari, no podr   accedir-hi sense el codi temporal (TOTP) generat en dispositius autoritzats.

2. Configuraci   del model de permisos personalitzats

- Creaci   i assignaci   de rols:** S  han definit els diferents perfils d  usuari a la plataforma d  administraci   de WordPress, ajustant la visibilitat i la capacitat d  edici   del panell segons el rol corresponent.
- Personalitzaci   de capacitats:** Mitjan  sant l    s de funcionalitats native de WordPress o de connectors de gesti   de rols, s  han restringit o ampliat permisos espec  fics (com la gesti   de plugins, edici   de temes, publicaci   de continguts o gesti   d  altres usuaris) per assegurar que cap usuari no administratiu tingui acc  s a opcions cr  tiques.

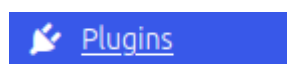
3. Implementaci   i configuraci   de la doble autenticaci   (2FA)

- **Instal·lació del mòdul de seguretat:** S'ha integrat i activat una solució de doble autenticació compatible amb WordPress (com ara Two Factor, Wordfence o Twenty20 2FA).
- **Vinculació de dispositius:** Des del perfil d'administrador i usuaris amb accés especial, s'ha completat la configuració escanejant el codi QR mitjançant una aplicació d'autenticació (com Google Authenticator, Authy o Microsoft Authenticator).
- **Obtenció de codis de recuperació:** S'han generat i emmagatzemat de forma segura els codis de seguretat de recanvi per evitar el bloqueig involuntari del compte en cas de pèrdua del dispositiu principal.

4. Proves i comprovació del funcionament

- **Validació d'accés amb permisos personalitzats:** S'ha iniciat sessió amb usuaris de diferents rols per comprovar que el menü d'administració i les opcions disponibles s'adapten adequadament als permisos establerts.
- **Validació del flux de doble autenticació:** S'ha comprovat el procés d'inici de sessió tancant la sessió activa i tornant-hi a accedir. El sistema sol·licita correctament el codi temporal de 6 dígits després d'introduir l'usuari i la contrasenya.

Evidències



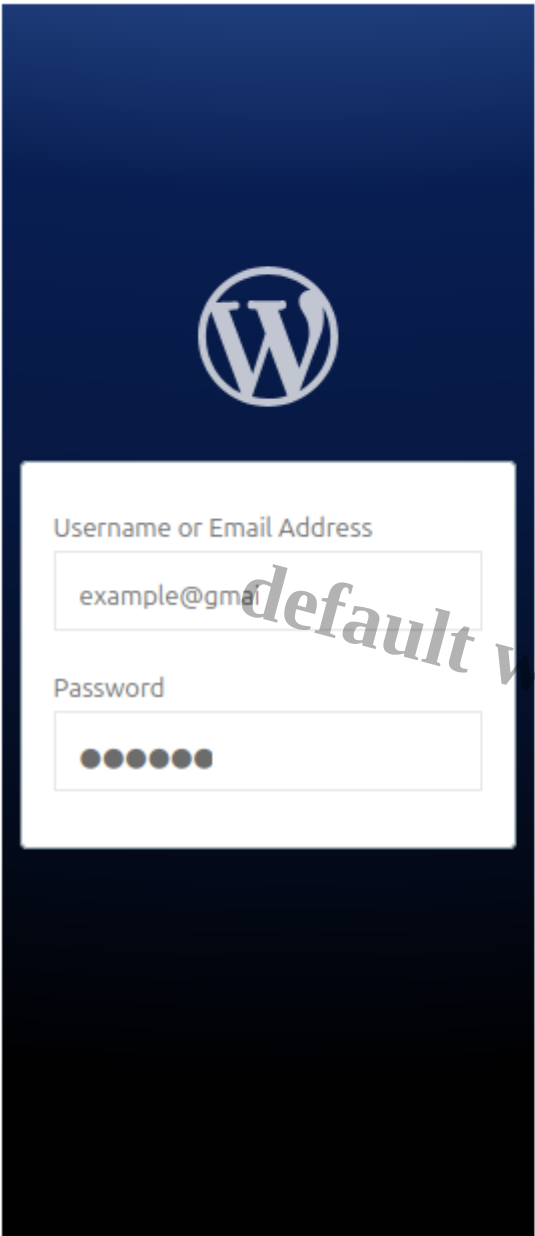
Kadence Security – Password, Two Factor Authentication, and Brute Force Protection

[Install Now](#)

[More Details](#)

Harden your site security with Login Security, Two-Factor Authentication (2FA), Vulnerability Scanner, Firewall, and more. Formerly iThemes Security.

By [Nexcess](#)



Attackers can make thousands of login attempts before you even notice.

Why is this important?

Brute Force protection slows down attackers who try to guess login credentials for your site.

 Brute Force protection is the first brick in your firewall

☒ Local Brute Force Recommended

☐ Network Brute Force  Recommended

The built-in Kadence Security firewall stops automated password-guessing attacks by temporarily blocking them when you enable Local Brute Force. Layer in additional protection by enabling Network Brute Force. Join with other Kadence-protected sites, combining intelligence to combat sophisticated attackers.

Continue →

Category

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

Date Created

October 2, 2026

Author

sachcharifi

default watermark