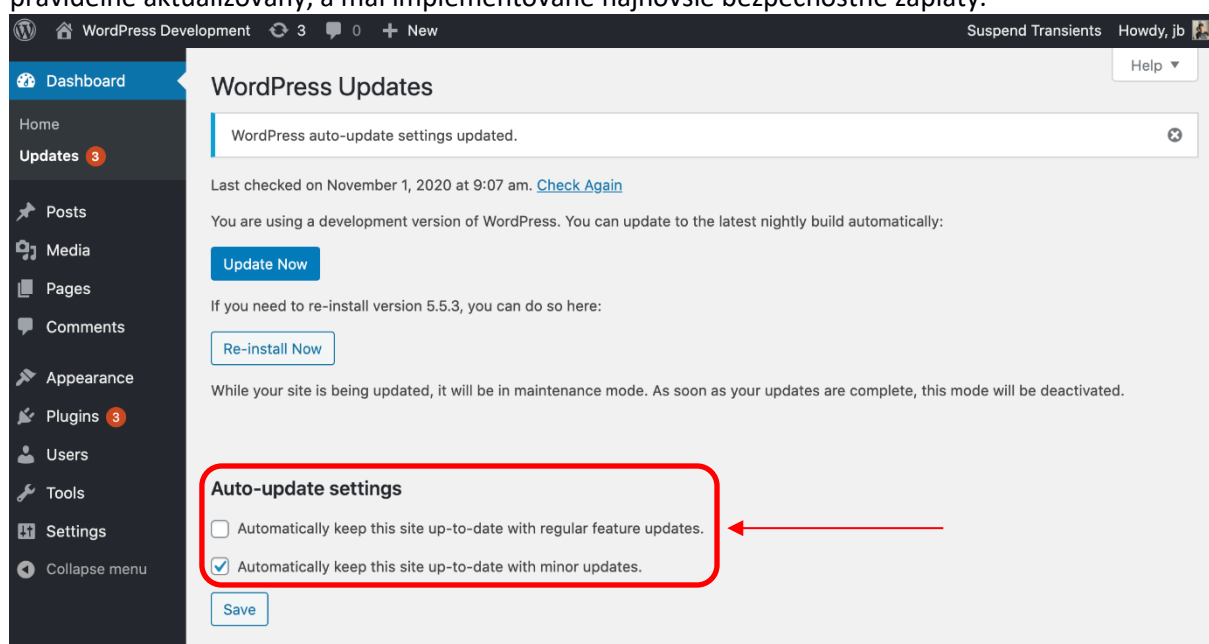


Wordpress hardening manuál

Tento dokument opisuje základné kroky potrebné pre zvýšenie bezpečnosti vlastnej inštancie redakčného systému Wordpress.

1. Pravidelná aktualizácia

Aktualizácie plnia veľmi dôležitú úlohu. Opravujú chyby v operačných systémoch, softvéroch a aplikáciách, ktoré by mohli byť zneužitú. Z tohto dôvodu je potrebné dbať na to, aby bol softvér pravidelne aktualizovaný, a mal implementované najnovšie bezpečnostné záplaty.



Obr. 1: Od verzie 3.7 je možné zároveň zapnúť možnosť automatickej aktualizácie.

WordPress však nemusí byť schopný aktualizovať plugíny a témy automaticky. V takomto prípade je potrebné aktualizovať tieto doplnky manuálne pomocou SFTP.

2. Používanie silných hesiel

Tvorba prístupového hesla k WP by mala podliehať rovnakým pravidlám ako tvorba hesiel k iným citlivým systémom. Mali by sme sa teda vyhýbať:

- Krátkym heslám
- Permutáciám osobných údajov
- Používaniu slovníkových slov
- Použitíu výhradne numerických alebo alfabetických hesiel

Vhodné je taktiež spojiť silné heslo s použitím viacfaktorovej autentifikácie.

Návod na vytvorenie bezpečného hesla môžete nájsť na našej FB stránke:

https://m.facebook.com/story.php?story_fbid=pfbid0X5hzSrCet6seVRb9Sevms5p565SywDmRfGMWPPABUB1fN5P5ATH9WnzH53qYamoDI&id=370362056427576&sfnsn=mo

3. Konfigurácia používateľských práv

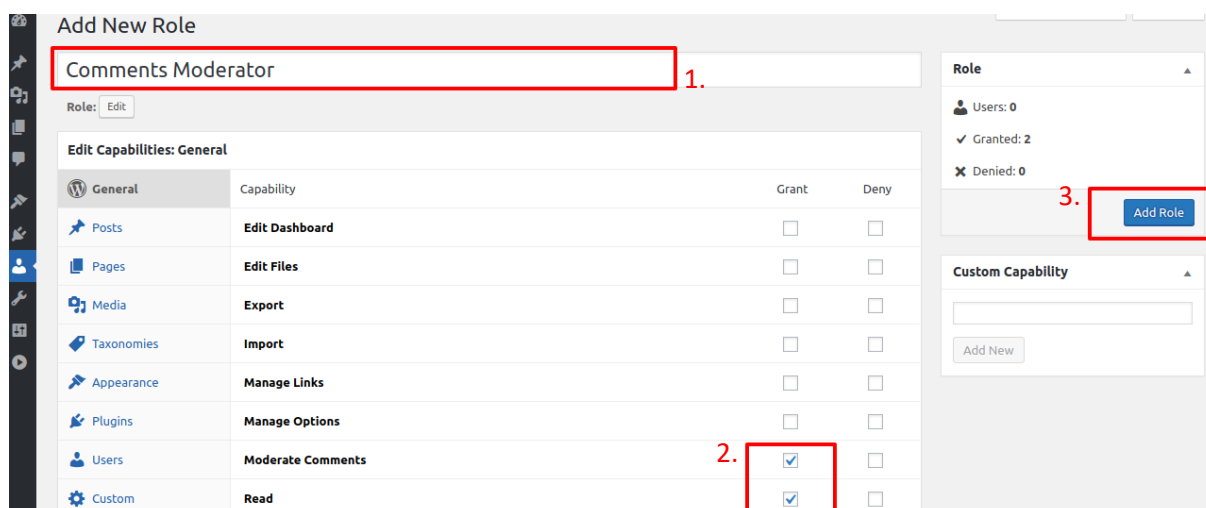
Vhodná konfigurácia používateľských rolí umožňuje jednoznačne definovať, čo môže, resp. nemôže daná skupina používateľov vykonávať. To môže v prípade incidentu výrazne zmenšiť škody, nakoľko útočník nedisponuje prístupom k citlivým súborom a údajom, resp. právam k ich úprave.

Medzi existujúce role patria:

- **Super admin:** rola s úplnými administrátorskými právami v rámci siete stránok.
- **Administrátor:** rola s úplnými administrátorskými právami v rámci 1 stránky.
- **Editor:** rola s právami uverejňovať a upravovať články ostatných používateľov.
- **Autor:** rola s právami uverejňovať a upravovať vlastné články.
- **Prispievateľ:** rola s právami upravovať vlastné články, avšak bez možnosti ich uverejnenia.
- **Odberateľ:** rola s právami na úpravy vlastného profilu.

Wordpress taktiež poskytuje možnosť vytvorenia vlastných rolí, ako je to vidieť na nasledujúcom obrázku:

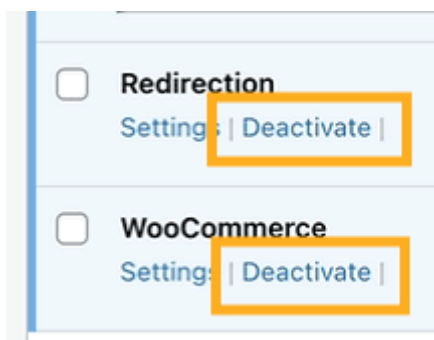
1. Názov role
2. Oprávnenia role
3. Tlačidlo na vytvorenie role



4. Deaktivácia nepoužívaných pluginov s prípadnou re-aktíváciou (len po dobu potreby používania pluginu)

Ak sa v našej inštancii WordPress nachádzajú doplnky (pluginy), ktorých využitie je zriedkavé, odporúčame ich deaktivovať a držať sa pravidla - povoliť len nutné.

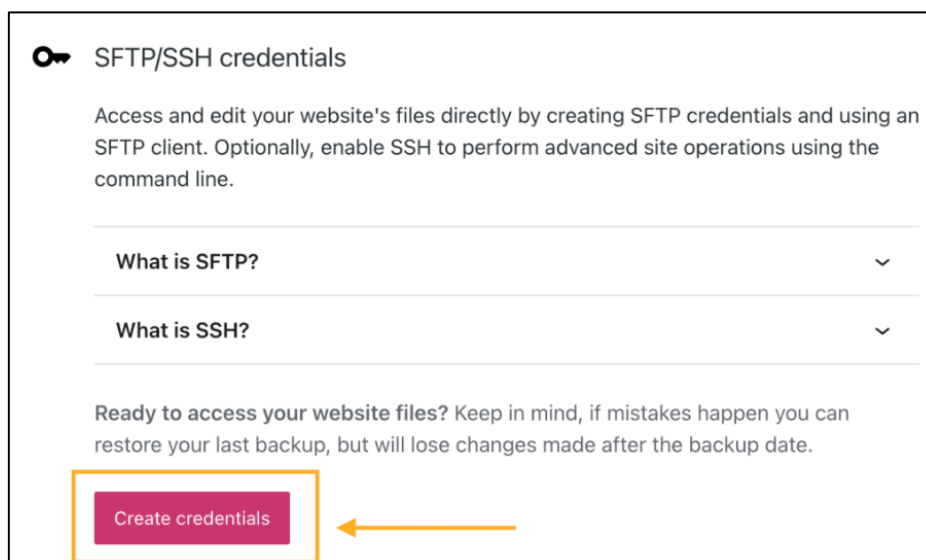
Plugins -> Installed plugins



5. Pripojenie pomocou SFTP/SSH

Pripojenie pomocou SFTP/SSH namiesto FTP zaručuje šifrovanie prenášaných dát.

Dashboard -> Settings -> Hosting Configuration -> SFTP/SSH credentials



SFTP/SSH credentials

Access and edit your website's files directly by creating SFTP credentials and using an SFTP client. Optionally, enable SSH to perform advanced site operations using the command line.

What is SFTP? ▼

What is SSH? ▼

Ready to access your website files? Keep in mind, if mistakes happen you can restore your last backup, but will lose changes made after the backup date.

Create credentials

SFTP/SSH credentials

Use the credentials below to access and edit your website files using an SFTP client.

[Learn more about SFTP on WordPress.com](#)

URL

 Copy

Port

 Copy

Username

 Copy

Password

For security reasons, you must reset your password to view it.

SSH Access

Enable SSH access for this site. [Learn more](#)

Po úspešnom vygenerovaní príkazu pre vytvorenie SSH spojenia, skopírujeme príkaz do príkazového riadku, čím vytvoríme aktívne spojenie.

SSH Access

Enable SSH access for this site.

ssh [redacted] wp.com Copy

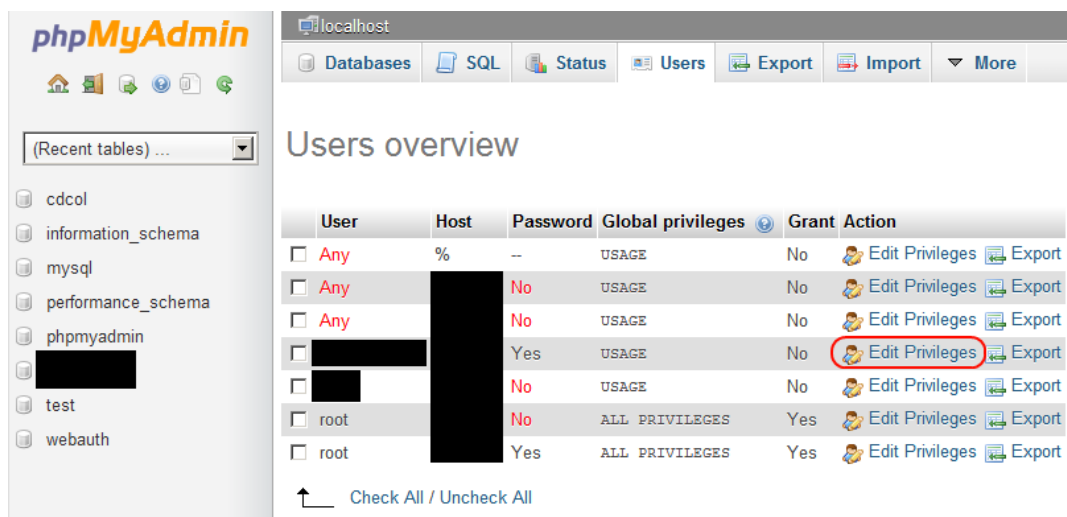
6. Implementácia súborových práv

V rámci používania WP je vhodné čo najviac obmedziť súborové práva, teda práva na čítanie, zápis a spustenie. Následne je ich možné uvoľniť výhradne pre nevyhnutné potreby a na čas nevyhnutný na ich vykonanie, napr. `find /path/to/your/wordpress/install/ -type d -exec chmod 755 {} \;`

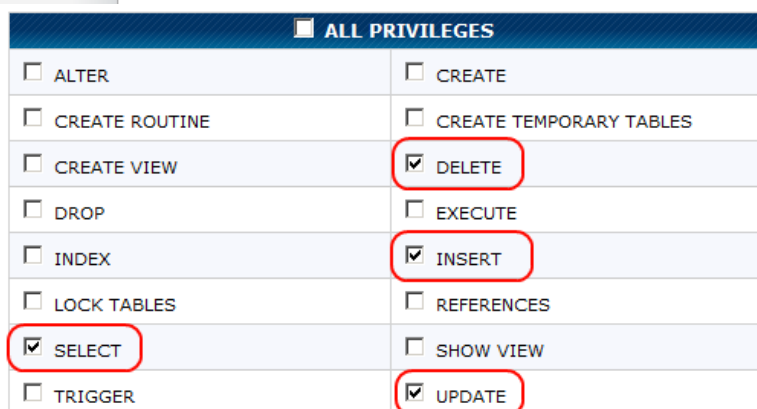
Viac o prístupových právach v Linuxe na <https://www.geeksforgeeks.org/permissions-in-linux/>.

7. Obmedzenie práv databázy

Pre bežné používanie a správu WP sú pre používateľa postačujúce práva na operácie SELECT, INSERT, UPDATE a DELETE. Všetky ostatné operácie tak môžu byť zakázané. Vhodným nástrojom je PhpMyAdmin (viď. Obrázok nižšie), XAMPP, DataGrip a pod.



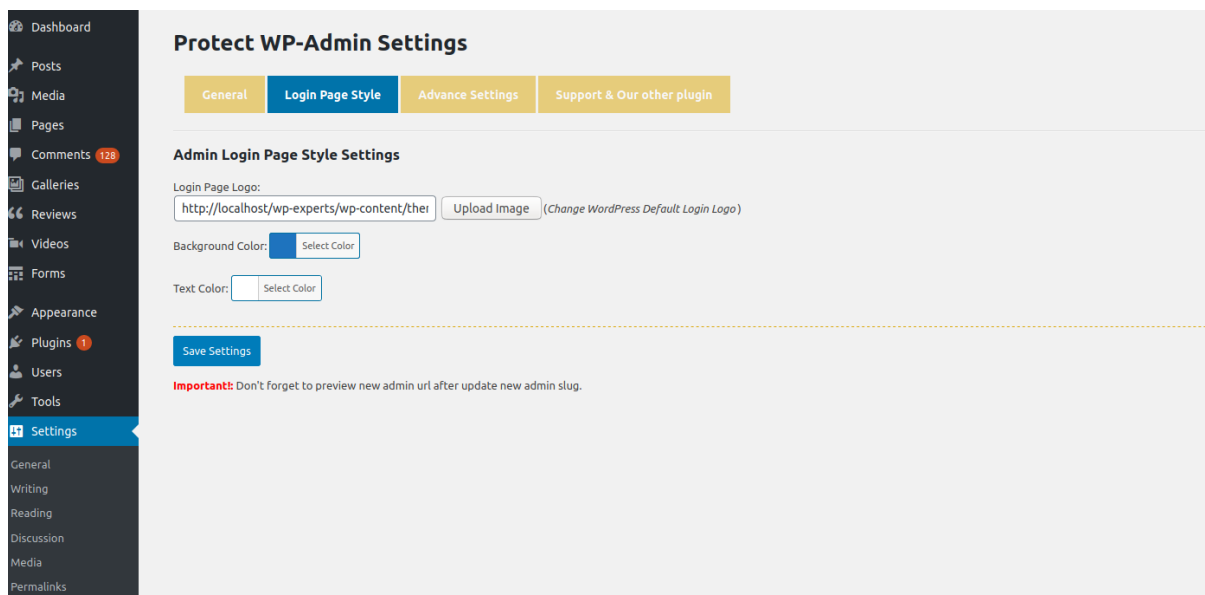
User	Host	Password	Global privileges	Grant	Action
<input type="checkbox"/> Any	%	--	USAGE	No	Edit Privileges Export
<input type="checkbox"/> Any		No	USAGE	No	Edit Privileges Export
<input type="checkbox"/> Any		No	USAGE	No	Edit Privileges Export
<input type="checkbox"/> [redacted]		Yes	USAGE	No	Edit Privileges Export
<input type="checkbox"/> [redacted]		No	USAGE	No	Edit Privileges Export
<input type="checkbox"/> root		No	ALL PRIVILEGES	Yes	Edit Privileges Export
<input type="checkbox"/> root		Yes	ALL PRIVILEGES	Yes	Edit Privileges Export



ALL PRIVILEGES	
<input type="checkbox"/> ALTER	<input type="checkbox"/> CREATE
<input type="checkbox"/> CREATE ROUTINE	<input type="checkbox"/> CREATE TEMPORARY TABLES
<input type="checkbox"/> CREATE VIEW	<input checked="" type="checkbox"/> DELETE
<input type="checkbox"/> DROP	<input type="checkbox"/> EXECUTE
<input type="checkbox"/> INDEX	<input checked="" type="checkbox"/> INSERT
<input type="checkbox"/> LOCK TABLES	<input type="checkbox"/> REFERENCES
<input checked="" type="checkbox"/> SELECT	<input type="checkbox"/> SHOW VIEW
<input type="checkbox"/> TRIGGER	<input checked="" type="checkbox"/> UPDATE

Viac o nástroji PhpMyAdmin na <https://docs.phpmyadmin.net/en/latest/privileges.html>.

8. Zabezpečenie URL wp-admin a súborovej štruktúry



Pomocou tohto nastavenia si vynútime aj druhé prihlásenie (viacstupňová verifikácia) pri prístupe k súborom, kde sú potrebné administrátorské práva. Zároveň je vhodné aktivovať administráciu prostredníctvom HTTPS.

9. Zabezpečenie súboru wp-includes

Vložením tohto kódu do súboru `.htaccess` mimo blok kódu ohraničený reťazcami `# BEGIN WordPress`, `# END WordPress` zablokujeme skripty pre používateľov, ktorí nemajú oprávnenia k ich použitiu.

```

# Block the include-only files.
<IfModule mod_rewrite.c>
RewriteEngine On
RewriteBase /
RewriteRule ^wp-admin/includes/ - [F,L]
RewriteRule !^wp-includes/ - [S=3]
RewriteRule ^wp-includes/[^\.]+\.\php$ - [F,L]
RewriteRule ^wp-includes/js/tinymce/langs/.+\.\php - [F,L]
RewriteRule ^wp-includes/theme-compat/ - [F,L]
</IfModule>

```

Nesprávnou manipuláciou s `.htaccess` môžeme spôsobiť znefunkčnenie našej Wordpress-ovej inštancie. Z tohto dôvodu je vhodné vykonávať zmeny prostredníctvom okna administrácie, prípadne s využitím modulov.

10. Zabezpečenie súboru wp-json

Zabezpečenie `wp-json` umožňuje zabezpečenie systému voči zneužitiu REST API, zároveň so zachovaním všetkých jej funkcií.

Pre zabezpečenie súboru `wp-json` môžete použiť modul Disable WP REST API:

- Stiahnite plugin-u Disable WP REST API (<https://wordpress.org/plugins/disable-wp-rest-api/>)
- Plugin zabezpečí, že REST API bude dostupné iba pre autentifikovaného používateľa

11. Zabezpečenie súboru wp-config.php

Súbor wp-config.php sa predvolene nachádza v koreňovom adresári inštancie WordPress. Obsahuje informácie o databáze vrátane hostiteľa, používateľského mena a hesla. Umožňuje napr. komunikovať s databázou pri ukladaní a načítavaní údajov.

Odporúčame nastaviť oprávnenia na tento súbor tak, aby ste jeho obsah mohli čítať vy (a webový server) - spravidla sa jedná o oprávnenia 400 alebo 440. V prípade potreby úprav tohto súboru, odporúčame zmenu oprávnení na čas nevyhnutný pre ich vykonanie.

Tak isto je všeobecne odporúčané presunutie súboru wp-config.php, napr. o jednu úroveň nad koreňový adresár s inštaláciou WordPress.

12. Aktivácia logovania a limitu počtu prihlásení

Vhodným zabezpečením WP je taktiež aktivácia logovania pomocou zvoleného WP pluginu (napr. <https://wordpress.org/plugins/wp-security-audit-log/>). Pomocou logovania tak získame prehľad o dianí na stránke.

Rovnako pomocou WP pluginu vieme aktivovať reštrikcie na počet neúspešných prihlásení (napr. <https://wordpress.org/plugins/limit-login-attempts-reloaded/>).

13. Použitie nástroja Web Application Firewall (WAF)

Implementácia WAF umožňuje zablokovanie útočníka ešte pred navštívením našej stránky. WAF kontroluje IP adresy návštevníkov stránky. V prípade, že je daná IP adresa priradená k podozrivej aktivite, je automaticky zablokovaná. WP WAF je možné implementovať napr. pomocou <https://www.malcare.com/firewall-plugin/>. Malcare zároveň slúži ako všeobecný bezpečnostný plugin pre WP, ktorý umožňuje nie len implementáciu WAF, ale aj logovanie, scanovanie aktivity, implementáciu MFA autentifikácie, ako aj notifikácie v reálnom čase.

Pri implementácii WAF však treba dbať, či ho chceme implementovať na úrovni Apache alebo až na WP úrovni.

Viac o WAF na <https://www.cloudflare.com/learning/ddos/glossary/web-application-firewall-waf/>.

14. Deaktivácia funkcie xmlrpc.php

XML-RPC je funkcia, ktorá umožňuje prenos údajov, pričom protokol HTTP funguje ako prenosový mechanizmus a XML ako kódovací mechanizmus. Táto funkcia je však zastaralá, a prináša so sebou hneď niekoľko bezpečnostných rizík.

Plne ju nahradilo rozhranie REST API, avšak táto funkcia ostáva vo WordPress predvolene zapnutá a je potrebná jej dodatočná deaktivácia.

Vypnutie funkcie XML-RPC priamo vo WordPress inštancii:

Umiestnenie nasledovného príkazu do súboru .htaccess v koreňovom priečinku

```
<files xmlrpc.php>  
order deny,allow  
deny from all  
</files>
```

Vypnutie funkcie XML-RPC pre NGINX:

Umiestnenie nasledovného príkazu do súboru .htaccess (napr. v zložke /etc/nginx/sites-available)

```
Location = /xmlrpc.php {  
    deny all;  
}
```

15. Pravidelná zmena bezpečnostných kľúčov

Bezpečnostné kľúče (tzv. security keys & salts) sa nachádzajú v súbore wp-config.php a z času na čas sa odporúča ich výmena za nové. Ak chcete získať novú sadu bezpečnostných kľúčov, je možné ich vygenerovať na webovom sídle WordPress - <https://api.wordpress.org/secret-key/1.1/salt/>.

16. Používanie bezpečnostných modulov

Bezpečnostné moduly dostupné pre stránky na platforme Wordpress poskytujú možnosti dodatočného zabezpečenia. Napríklad modul Sucuri (<https://wordpress.com/plugins/sucuri-scanner>) poskytuje bezpečnostný audit, kontrolu integrity súborov, skenovanie škodlivého kódu, hardening stránky, bezpečnostné notifikácie či zabezpečenie webu po napadnutí.