Průvodce nastavením bezpečnostního pluginu iThemes Security

Poslední aktualizace 23 srpna, 2024

iThemes Security je vedle WordFence, o kterém v naší nápovědě píšeme také, jeden z nejlepších bezpečnostních pluginů pro WordPress, které můžete pro zabezpečení svých webových stránek použít.

V tomto článku si ukážeme, jak se iThemes Security nastavuje. Vzhledem k tomu, že je v angličtině, si zde také postupně vysvětlíme všechny možnosti nastavení.

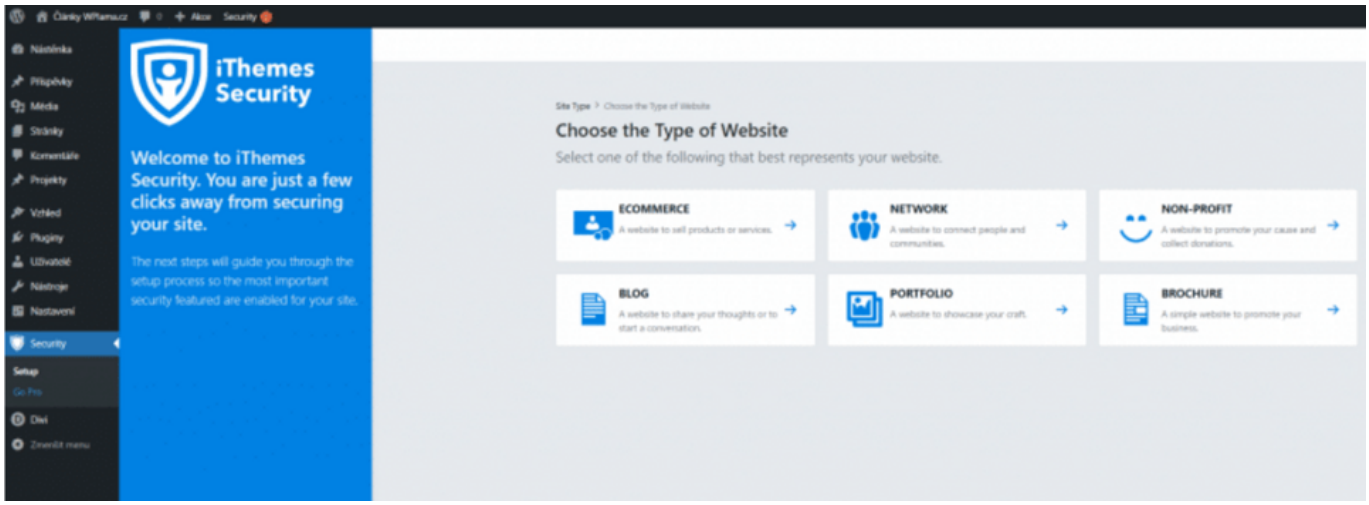
V některých srovnáních vychází WordFence jako vítěz, v jiných naopak vyhrává iThemes. My na náš WordPress hosting automaticky instalujeme plugin WordFence, a to především z toho důvodu, že podporuje češtinu.

Nastavení pluginu iThemes Security pro WordPress

iThemes Security obsahuje průvodce, který vás nastavením v několika krocích provede:

1. Výběr typu stránky

Po instalaci si můžete všimnout výzvy k základnímu nastavení zabezpečení. Přejděte proto do nastavení pluginu kliknutím na novou podstránku administrace **Security → Setup**



Dostanete se na **nástěnku** iThemes Security, kde si musíte vybrat typ stránky, který provozujete. Na výběr máte z možností:

- Ecommerce (E-shop)
- Network (Sociální síť)
- Non-profit (Nezisková organizace)
- Blog
- Portfolio
- Brochure (Firemní stránka)

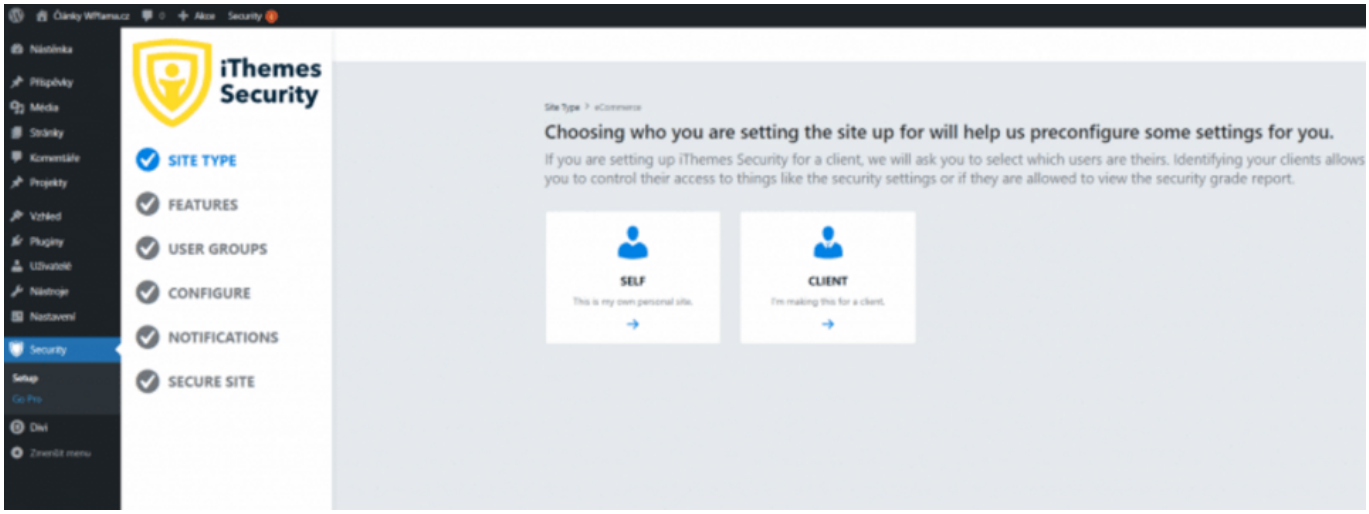
Vyberte požadovaný typ webu. Podle zvoleného typu se bude lišit druhý krok.

Vyberete-li například E-Shop, v druhém kroku budete ještě muset vybrat uživatelskou roli, kterou dostávají zákazníci.

2. Pro koho nastavujete web

Nyní je potřeba vybrat, kdo nastavuje web. Na výběr máte:

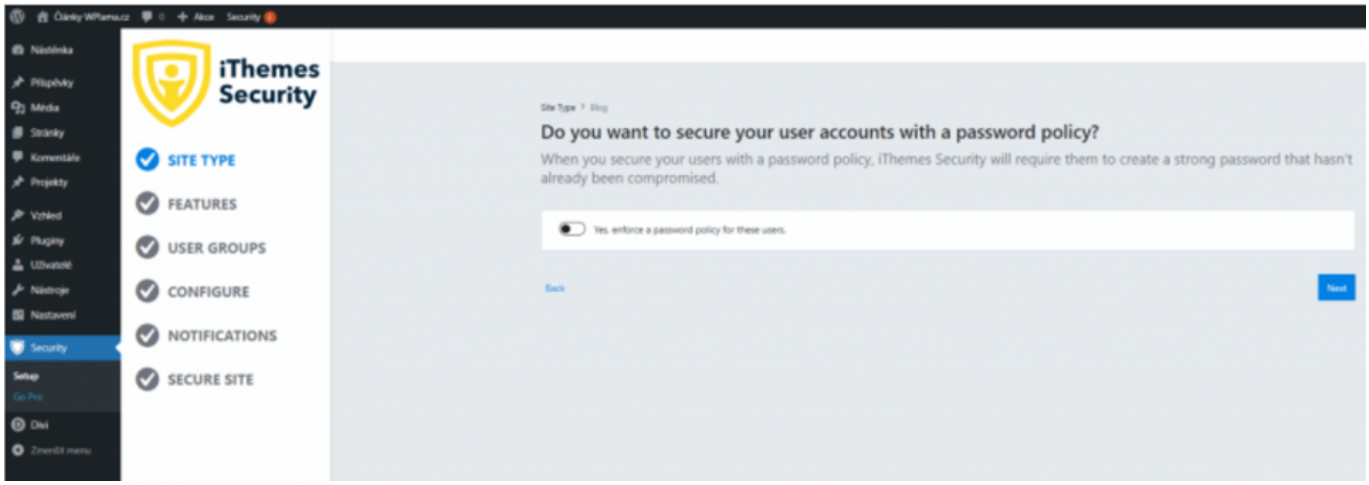
- Self (Pro sebe)
- Client (Pro klienta)



3. Vynucení silného hesla

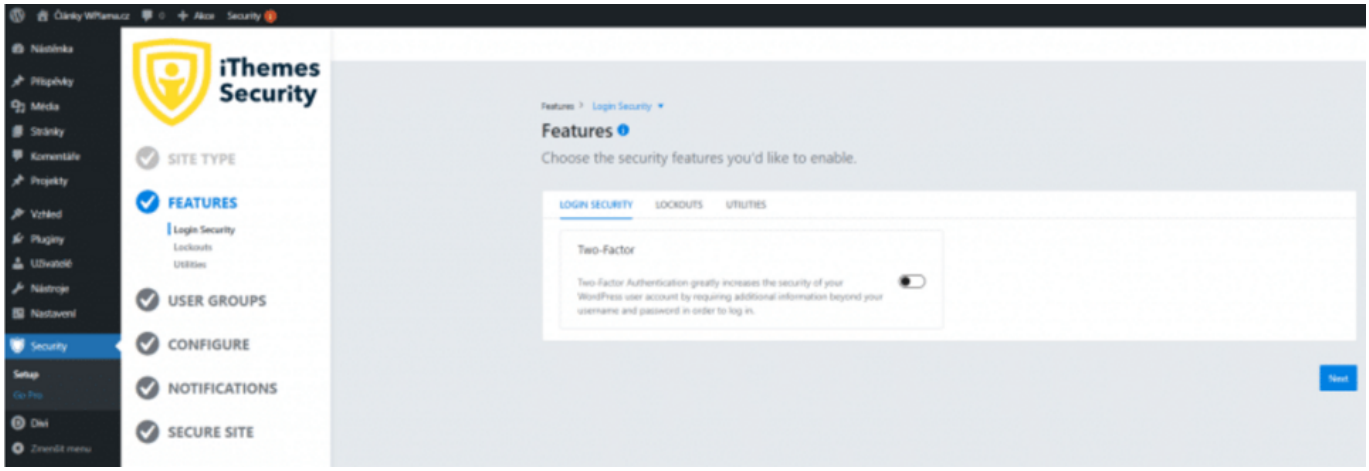
Dále je potřeba nastavit vynucení použití silného hesla. Doporučujeme tuto možnost nastavit.

V případě, že bude mít administrátor slabé heslo, plugin jej donutí si jej při dalším přihlášení změnit na silné.



4. Features

Plugin obsahuje také užitečné funkce k ochraně webu, v tomto kroku si je můžete nastavit.



Login Security

- Two-Factor – dvoufázové ověření pomocí e-mailu, při přihlášení zašle na e-mail uživatele kód, kterým se ověří jeho identita.

Lockouts

- Local Brute Force – ochrana proti prolomení hesla hrubou silou, kde se útočník snaží heslo uhádnout pomocí náhodných kombinací.
- Network Brute Force – přihlášení do systému iThemes, kde se předávají informace i „špatných IP“, poté je uživatel z této IP automaticky zablokován.

Utilities

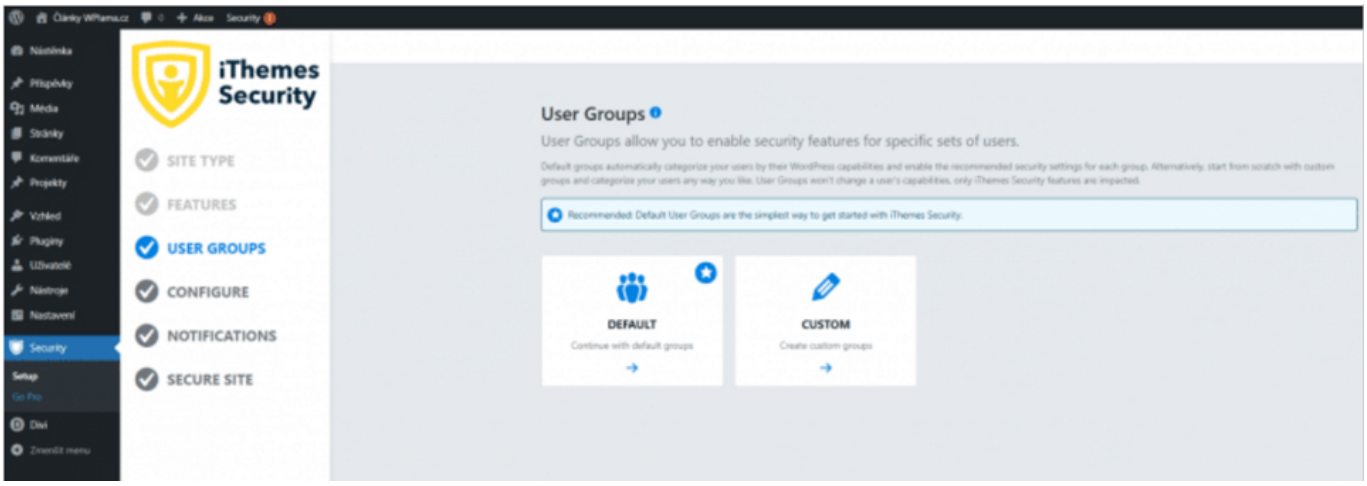
- Security Check Pro – kontrola IP adresy uživatele při přihlášení.

5. User Groups

V tomto kroku si můžete ovlivnit jednotlivé nastavení pro používané uživatelské skupiny.

Na výběr máte z možností:

- Default (Výchozí) – v drtivé většině případů využijte toto
- Custom



V případě, že jste zvolili výchozí uživatelské skupiny, tak si nyní můžete upravit jejich jednotlivé nastavení.

Jedná se o skupiny Administrátor, Editor, Spolupracovník, Autor, Návštěvník a ostatní.

Nastavení pro jednotlivé uživatelské role je:

Global Settings

- Manage iThemes Security – povolit úpravu nastavení iThemes Security

Security Dashboard

- Enable Dashboard Creation – přístup do nástěnky pluginu.

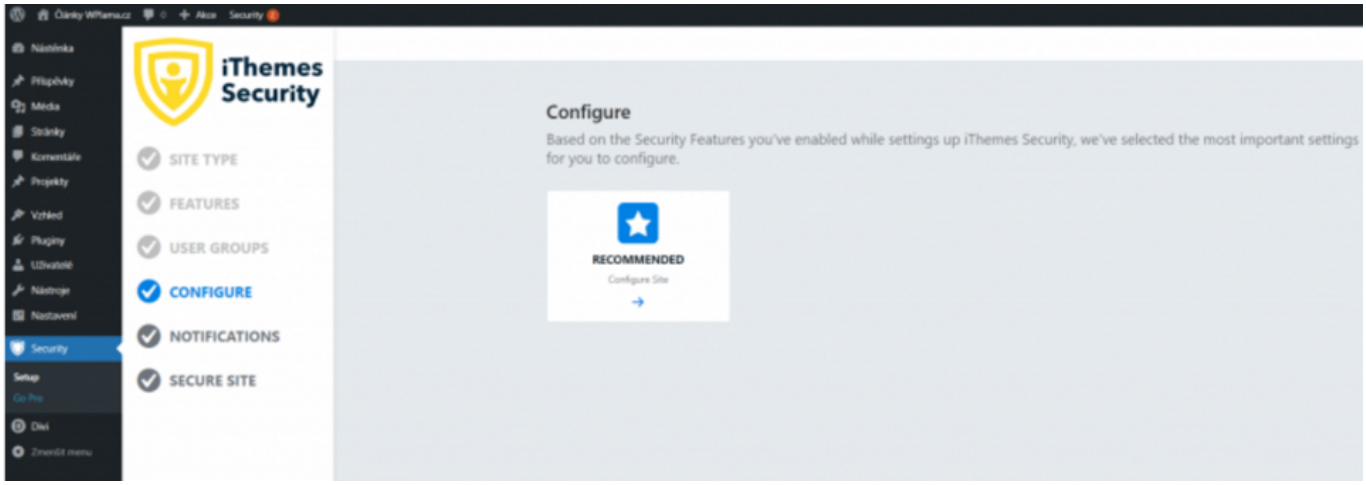
Password Requirements

- Strong Passwords – silná hesla, po aktivaci budou uživatelé při registraci donuceni

zvolit silné heslo (podle WordPress hodnocení).
- Refuse Compromised Passwords – vynucení použití hesla, které se neobjevilo v žádné databázi uniklých hesel.

6. Configure

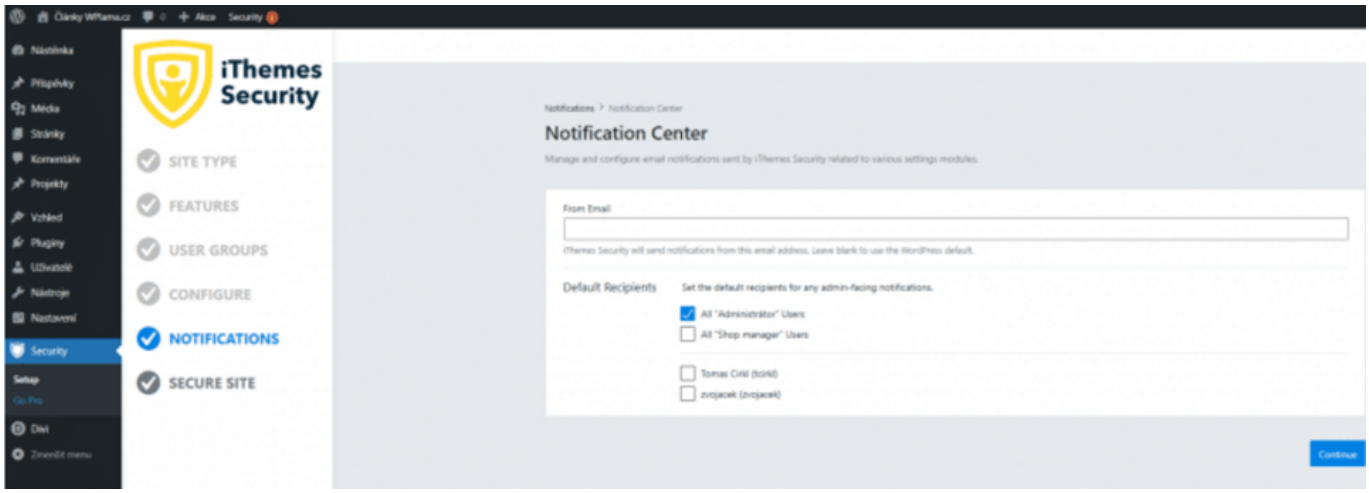
Základní nastavení pluginu a přístupů.



- Authorized Hosts – zde si můžete přidat IP adresy ověřených uživatelů, tyto IP se zařadí do whitelistu a nemůže u nich dojít k banu.
- API Configuration – zadejte e-mail pro aktivaci Network Brute Force.

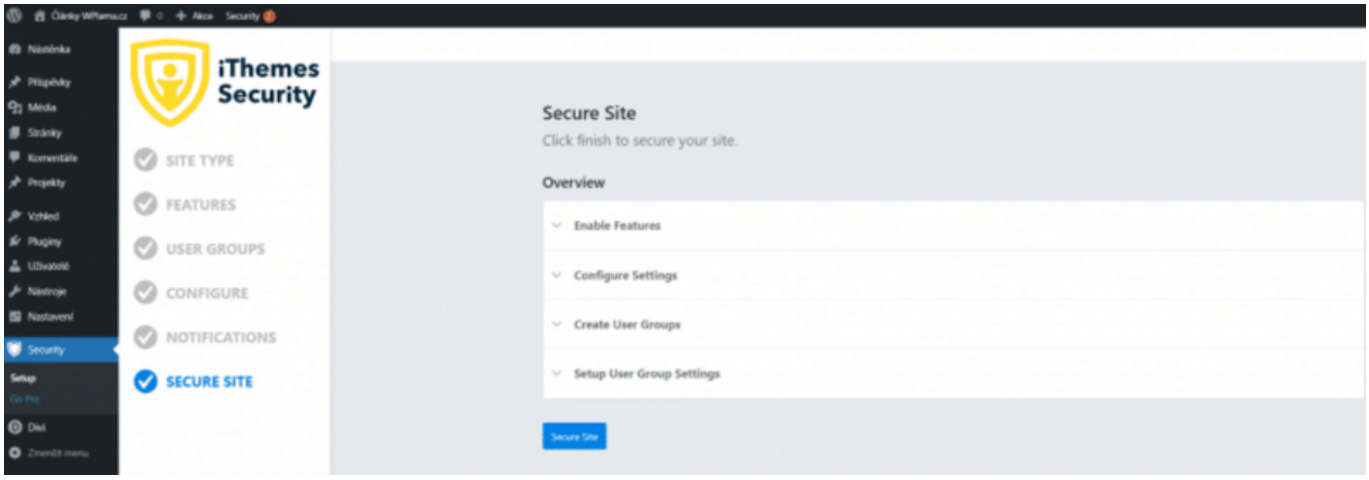
7. Notification Center

V centru notifikací si můžete nastavit pravidla, na jaký e-mail, případně jaké uživatelské roli, přijde upozornění při bezpečnostní události.



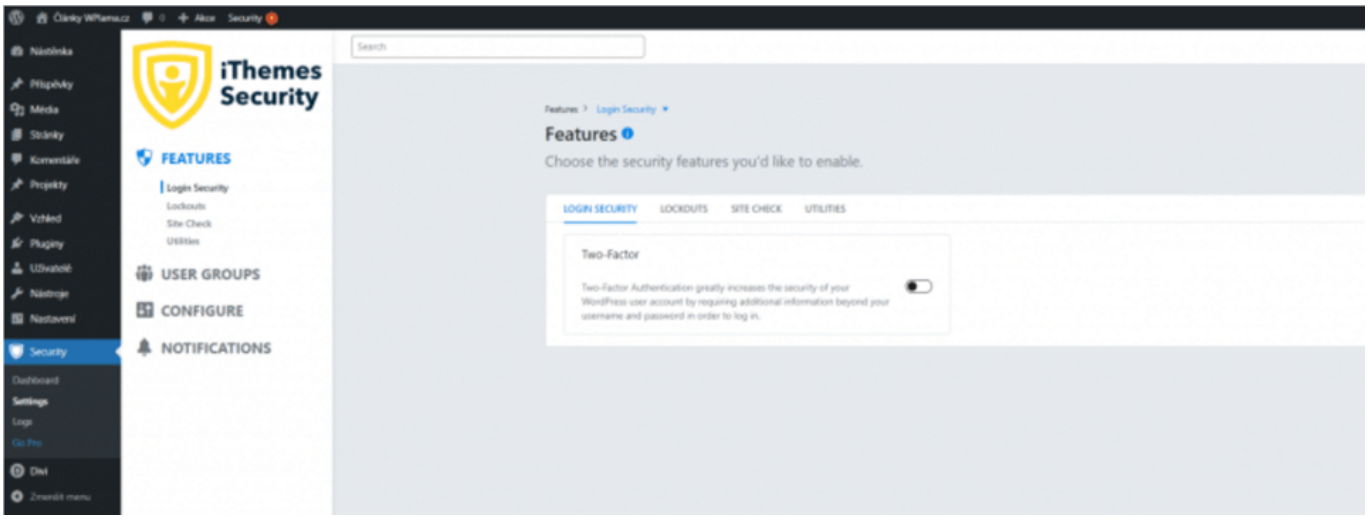
8. Secure Site

Posledním krokem základního nastavení je shrnutí a uložení.



Další volitelná nastavení iThemes Security

Kromě základního nastavení má plugin i další možnosti, které si představíme níže.



Features

Login Security

- **Two-Factor –** dvoufázové ověření pomocí e-mailu, při přihlášení zašle na e-mail uživatele kód, kterým se ověří jeho identita. Lockouts

- **Ban Users –** povolí funkci banování uživatelů.
- **Local Brute Force –** povolí funkci ochrany proti útoku hrubou silou.
- **Network Brute Force –** povolí přihlášení do systému iThemes, kde se předávají informace i „špatných IP“, poté je uživatel z této IP automaticky zablokován.

Site Check

- **File Change –** funkce, která detekuje změny v souborech vaší WordPress instalace. Po její aktivaci se vám může zobrazit upozornění, že při aktuálním nastavení maximální paměti pro PHP skripty může dojít k deaktivaci webu právě kvůli chybě při nedostatku paměti. Na běžném hostingu asi bude s touto funkcí problém. Pokud máte VPS s alespoň 256MB PHP paměti nemělo by dojít k potížím. Musíte si však funkci otestovat na svém nastavení.

Utilities

- **Enforce SSL –** vynucení použití SSL.
- **Database Backups –** protože základem bezpečnosti jakékoliv internetové stránky je právě zálohování, iThemes Security se dokáže postarat o automatické pravidelné zálohování databáze a odesílání záloh na email nebo ukládání na server.
- **Security Check Pro –** kontrola IP adresy uživatele při přihlášení.

User Groups

Global Settings

- **Manage iThemes Security –** povolit úpravu nastavení iThemes Security

Security Dashboard

- **Enable Dashboard Creation –** přístup do nástěnky pluginu.

Password Requirements

- **Strong Passwords –** silná hesla, po aktivaci budou uživatelé při registraci donuceni zvolit silné heslo (podle WordPress hodnocení).
- **Refuse Compromised Passwords –** vynucení použití hesla, které se neobjevilo v žádné databázi uniklých hesel.

Configure

Global Settings

- **Write to Files –** povolí zapisovat pluginu iThemes Security do souborů wp-config.php a .htaccess.
- **Lockouts –** povolí zapisovat pluginu iThemes Security do souborů wp-config.php a .htaccess.
  – Minutes to Lockout – čas, po který bude uživatel zabanován po dosažení limitu počtu přihlášení.
  – Days to Remember Lockouts – časové rozmezí, ve kterém musí uživatel daného počtu banů dosáhnout (např. 3× během týdne atd.).
  – Ban Repeat Offender – pokud tuto možnost zaškrtnete, bude uživatel po určitém množství (nastavíte dále) dočasných banů přidán na černou listinu, to znamená, že bude zabanován navždy. Někteří roboti jsou nepoučitelní a stále se vrací, tímto dojde k jejich úplnému zablokování.
  – Ban Threshold – po kolika blokacích (dočasných banech, lockoutech) dojde k přidání na černou listinu.
- **Lockout Messages**
  – Host Lockout Message – tato zpráva se zobrazí při zablokování serveru (IP adresy), můžete použít některé HTML tagy (jejich seznam je pod formulářem)
  – User Lockout Message – zpráva pro zablokovaného uživatele (obvykle, pokud je zabanovaný kvůli velkému množství neúspěšných pokusů o přihlášení).

– Community Lockout Message – tato zpráva se zobrazí uživateli, který byl zablokován na základě špatné IP adresy.

- **Authorized Hosts**
  – Automatically Temporarily Authorize Hosts – po přihlášení uživatele jej iThemes přidá na 24h do whitelistu.
  – Authorized Hosts – IP adresy autorizovaných uživatelů.
- **Logging**
  – How should event logs be kept – kam by se měli ukládat logy (doporučujeme databáze).
  – Days to Keep Database Logs – po jakou dobu uchovávat logy.
- **IP Detection**
  – Proxy Detection – typ detekce IP adresy
- **UI Tweaks**
  – Hide Security Menu in Admin Bar – skryje iThemes Security položku s horní WordPress lišty.
  – Enable Grade Report – povolí Grade Report zprávy při notifikacích.

Lockouts

- **Default Ban List –** touto možností okamžitě zabanujete všechny IP adresy uvedené v seznamu, který dal dohromady Jim Walker z HackRepair.com, **doporučujeme nezapínat**, Seznam bot je součástí banu.
- **Enable Ban Lists –** povolí funkci banování uživatelů.
- **Automatically ban „admin“ user –** automaticky zabanuje uživatele, který se chce přihlásit s uživatelským jménem admin.
- **Login Attempts**
  – Max Login Attempts Per Host – maximální počet pokusů o přihlášení z IP.
  – Max Login Attempts Per User – maximální počet pokusů o přihlášení pro uživatele.
- – Minutes to Remember Bad Login (check period) – doba, po kterou si plugin pamatuje neúspěšné pokusy.
- **Ban Reported IPs –** banovat špatné IP.

Utilities

- **Scheduling**
  – Schedule Database Backups – zaškrtnutím povolíte pravidelnou zálohu databáze.
- **Configuration**
  – Backup Method – způsob zálohování (e-mailem, na hosting).
- – Compress Backup Files – povolit kompresy zálohy.

- **Backup Tables –** jaké tabulky databáze se budou zálohovat.

Notifications

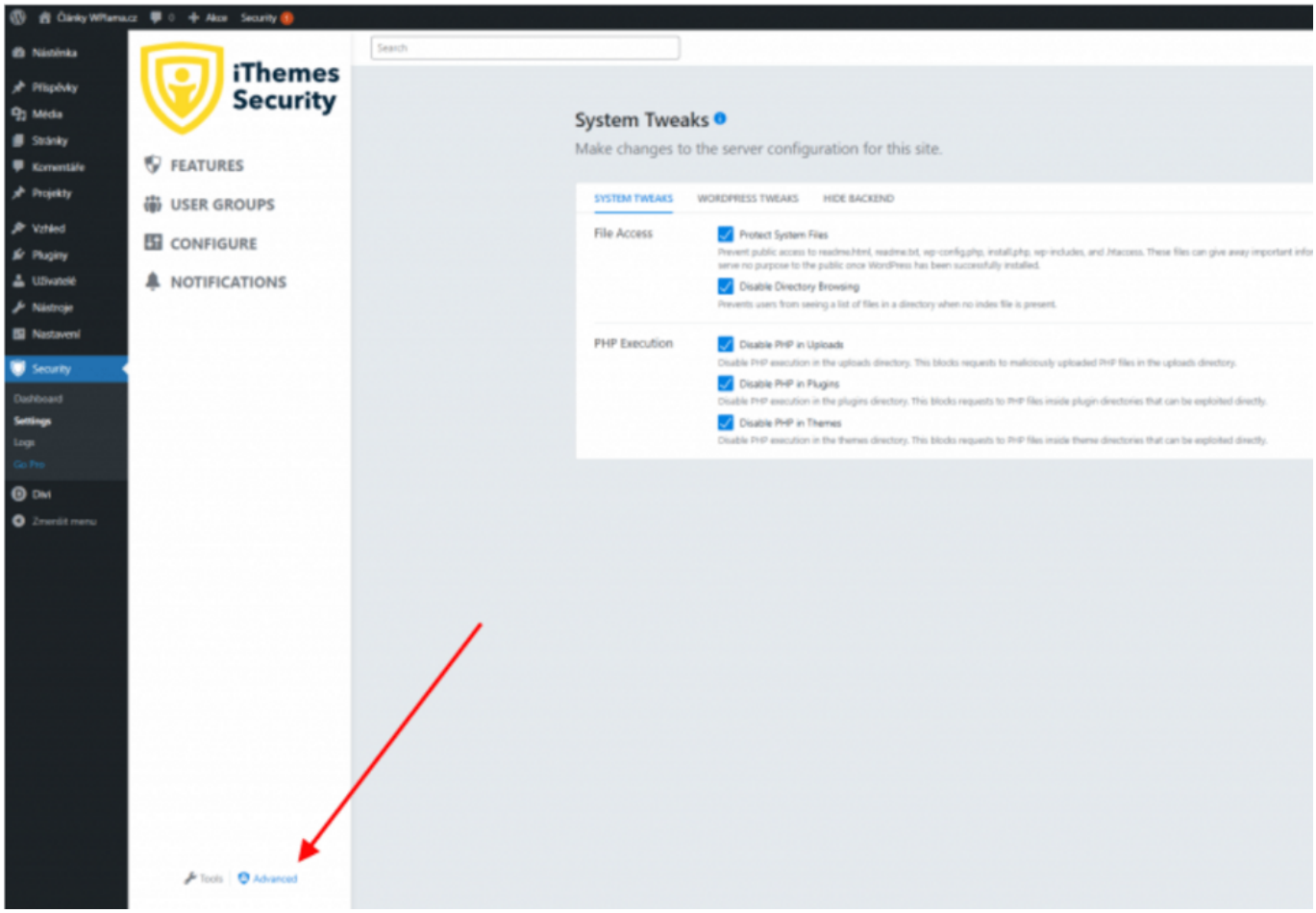
From Email – nastavení e-mailu použitého jako odesílatel.

Default Recipients – výchozí příjemci upozornění. Zaškrtejte vybrané.

- – Enabled – aktivuje toto upozornění.
  – Customize – změna předmětu e-mailu.
  – Schedule – frekvence odesílání upozornění.
  – Recipient – příjemci upozornění.
- **Security Digest –** denní souhrnná zpráva s informacemi o bezpečnostní webu.
  – Enabled – aktivuje toto upozornění.
  – Customize – změna předmětu e-mailu.
  – Recipient – příjemci upozornění.
- **Site Lockouts –** upozornění při zabanování uživatele. Pozor, při větším útoku na web můžete najednou dostat i stovky e-mailů. Zvažte tedy aktivaci.
  – Enabled – aktivuje toto upozornění.
  – Customize – změna předmětu e-mailu.
- – Recipient – příjemci upozornění.
- **Database Backup –** upozornění po vytvoření zálohy databáze.
  – Customize – změna předmětu e-mailu.
  – Recipient – příjemci upozornění.

Pokročilé nastavení v iThemes Security

V levém dolním rohu v nastavení pluginu najdete odkaz na pokročilé nastavení. Pojďme se podívat, na jednotlivé možnosti, které zde máte k dispozici.



System Tweaks – Úpravy v nastavení serveru.

- **File Access**
  – Protect System Files – touto funkcí zamezíte komukoliv zobrazit soubory readme.html, readme.txt, wp-config.php, install.php, wp-includes a .htaccess, které mohou prozradit důležité informace (například verzi WordPressu).
  – Disable Directory Browsing – zamezí uživatelům zobrazovat adresáře, kde není žádný index soubor. Zamezí hackerům poznat adresářovou strukturu vašeho webu. Tuto znalost by mohl zkušený hacker zneužít.
- **PHP Execution**
  – Disable PHP in Uploads – zabrání vykonávání PHP skriptů v adresáři Uploads.
  – Disable PHP in Plugins – zabrání vykonávání PHP skriptů v adresáři Plugins.
  – Disable PHP in Themes – zabrání vykonávání PHP skriptů v adresáři Themes (WordPress šablony).

System Tweaks – Úpravy v chování WordPressu.

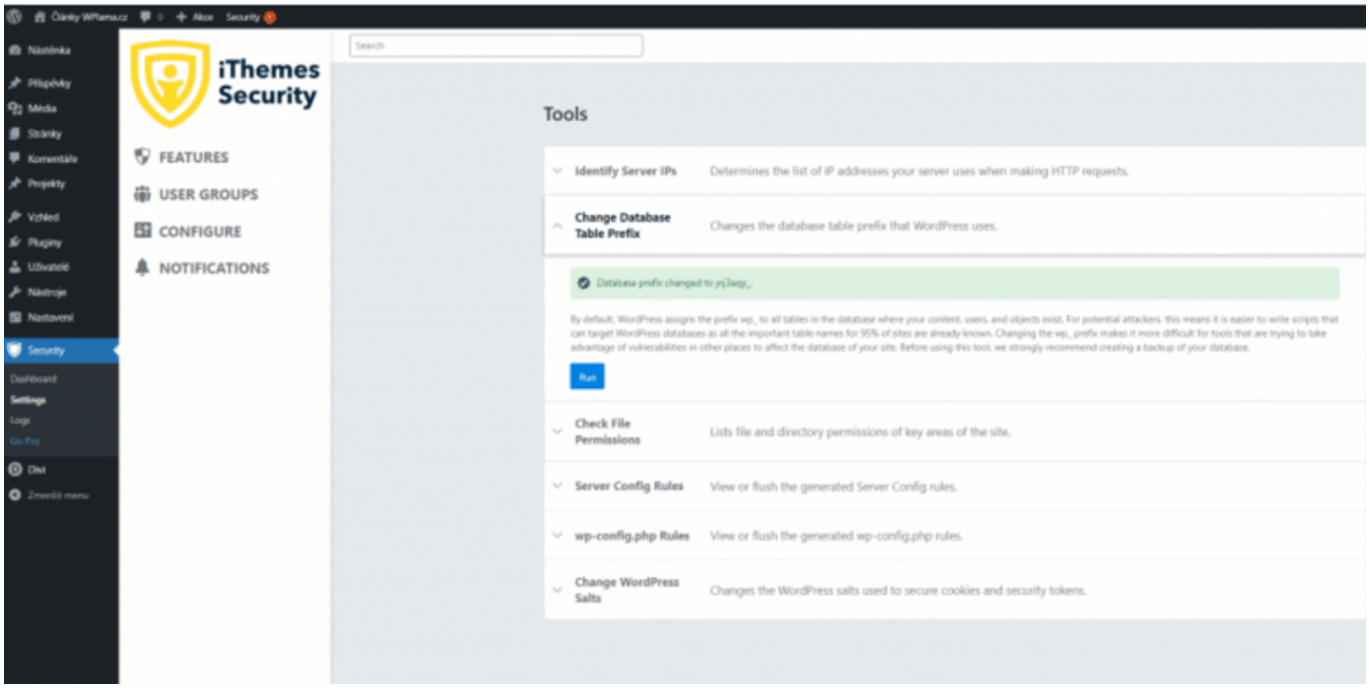
- **Disable File Editor**
  – základní bezpečnostní funkce, která vypne editor kódu v administraci.

- **API Access**
  – XML-RPC – deaktivaci XML-RPC funkce. Doporučuji vypnout, ale pak nebudou fungovat některé pluginy, které XML-PRC vyžadují (např. JetPack).
  – REST API – deaktivace REST API.
- **Users**
  – Login with Email Address or Username – povolí možnost přihlášení pomocí e-mailu nebo uživatelského jména anebo jednoho vybraného.
  – Force Unique Nickname – při registraci a aktualizaci profilu bude WordPress vyžadovat unikátní uživatelské jméno.
  – Disable Extra User Archives – vypne zobrazování profilů uživatelů (Author Page), kteří na vaši stránku nepřispívají, tím se zamezí shromažďování uživatelských jmen různými roboty.

Hide Backend – Přesun přihlašovacího formuláře na jinou adresu než /wp-admin, wp-login.php a další výchozí adresy WordPressu je jedním ze základních prvků obrany proti hackerům a různým botům. WordPress je dnes už notoricky známým redakčním systémem pro všechny, kteří mají co do činění s tvorbou webu, takže každý ví, kde se přihlašovací obrazovka nachází. Abychom hodili další klacek pod nohy všem hackerům, změníme si adresu pro login do administrace.

- **Hide Backend**
  – aktivujte pro „ukrytí“ všech formulářů pro přihlášení.
- **URLs**
  – Login Slug – slovo, které bude použito pro stránku s přihlašovacím formulářem. Výchozí je „wplogin“ – doporučuji nastavit na jiné slovo jako „logintowp“, „wpprihlaseni“ apod. V případě „logintowp“ byste pak přihlášení do administrace našli na adrese www.vasedomena.cz/logintowp.
  – Register Slug – slovo pro registraci.
- **Redirection**
  – Enable Redirection – povolí přesměrování.
  – Redirection Slug – slovo, kam bude přesměrován uživatel při zadání zablokovaného standardního přihlašovacího formuláře.
- **Advanced**
  – Custom Login Action – WordPress používá pro obsluhu přihlašování/odhlašování proměnnou action, která může nabývat nejrůznějších hodnot. iThemes Security zvládá ty základní, ale některé šablony nebo pluginy mohou vyžadovat vlastní akci. Pokud o nějaké takové akci víte, můžete ji přidat (obvykle to nebude potřeba).

Change Database Prefix – změna prefixu databáze



Poznámka: Před touto změnou doporučuji udělat zálohu databáze.

Databáze je asi nejdůležitějším prvkem celé WordPress instalace, a proto se její bezpečnost nedoporučuje podceňovat. Jedním ze základních zabezpečovacích kroků je uvedení jiného než výchozího prefixu tabulek („wp_“). Změna prefixu je s pluginem iThemes Security velmi jednoduchá:

1. V **Settings** vyberte v levém dolním rohu **Tools**.
2. Zde je rozbalovací položka **Change Database Prefix**.
3. Po rozbalení klikněte na **Run** a prefix databáze je změněný.

Sekce Logs

Logy najdete v levém WordPress menu **Security → Logs.**

V logách můžete najít veškeré problémy zjištěné pluginem iThemes Security.

Pokud například někdo provede neúspěšný pokus o přihlášení, uvidíte to zde. Objeví-li se někomu chyba 404, hlášení bude v logu také.

Čas od času je dobré se do logů podívat, i přesto, že o důležitých událostech budete upozorněni emailem (pokud jste si tak nastavili v **Settings → Nastavení**).

Závěrem

Zabezpečení WordPressu by se určitě nemělo podceňovat a iThemes Security je skvělý plugin schopný odstranit široké spektrum bezpečnostních problémů, kterými WordPress trpí.

Doufáme, že článek vám trochu pomůže s nastavením bezpečnosti na vlastním webu.

Ovládněte WordPress

S naším zbrusu novým WordPress hostingem je tvorba webu hračka.

Zjistit více