Sprievodca nastavením bezpečnostného pluginu iThemes Security

Last updated 19 novembra, 2024

iThemes Security je popri WordFence, o ktorom v našej nápovede píšeme tiež, jedným z najlepších bezpečnostných pluginov pre WordPress, ktoré môžete použiť na zabezpečenie svojich webových stránok.

V tomto článku si ukážeme, ako sa iThemes Security nastavuje. Vzhľadom na to, že je v angličtine, si tu tiež postupne vysvetlíme všetky možnosti nastavenia.

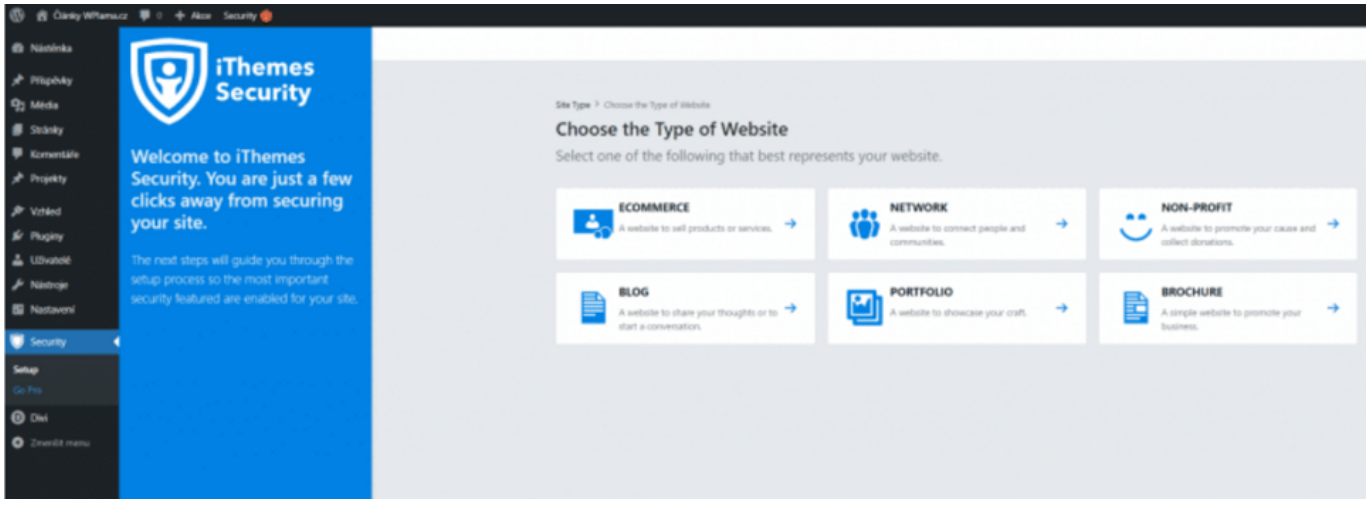
Z niektorých porovnaní vychádza WordFence ako víťaz, v iných, naopak, vyhráva iThemes. My na náš WordPress hosting automaticky inštalujeme plugin WordFence, a to predovšetkým preto, že podporuje češtinu.

Nastavenie pluginu iThemes Security pre WordPress

iThemes Security obsahuje sprievodcu, ktorý vás nastavením v niekoľkých krokoch prevedie:

1. Výber typu stránky

Po inštalácii si môžete všimnúť výzvu na základné nastavenie zabezpečenia. Prejdite preto kliknutím na novú podstránku administrácie do nastaven pluginu **Security → Setup**



Dostanete sa na nástenku iThemes Security, kde si musíte vybrať typ stránky, ktorú

prevádzkujete. Na výber máte z možností:

- Ecommerce (E-shop)
- Network (Sociálna sieť)
- Non-profit (Nezisková organizácia)
- Blog
- Portfólio
- Brochure (Firemná stránka)

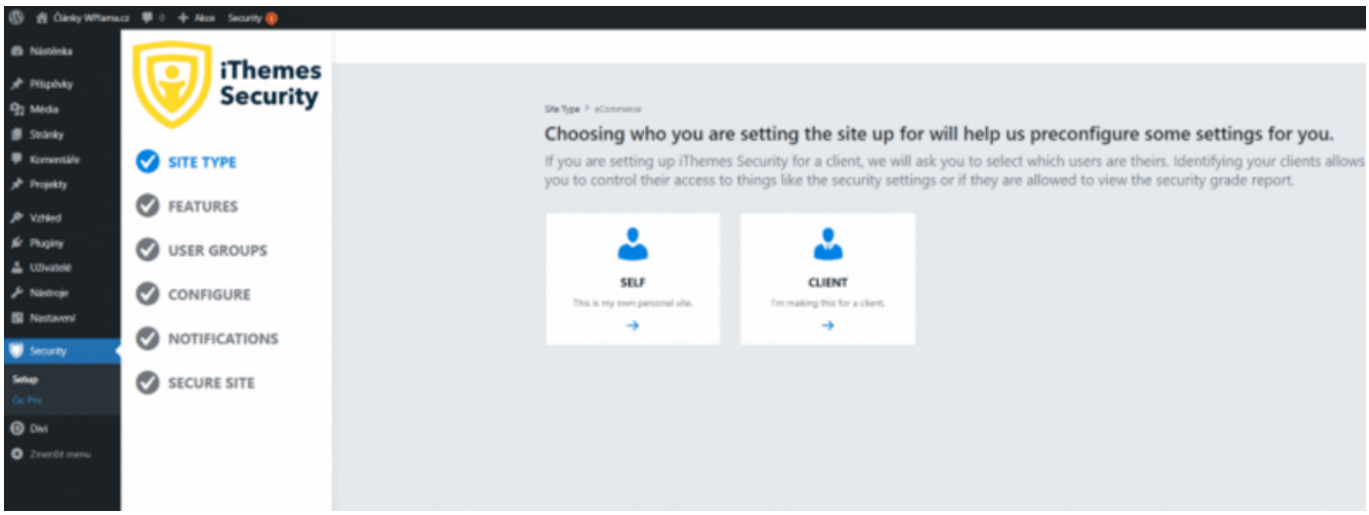
Vyberte požadovaný typ webu. Podľa zvoleného typu sa bude líšiť druhý krok.

Ak si vyberiete napríklad E-Shop, v druhom kroku budete ešte musieť vybrať používateľskú rolu, ktorú dostávajú zákazníci.

2. Pre koho web nastavujete

Teraz je potrebné zvoliť, kto nastavuje web. Na výber máte:

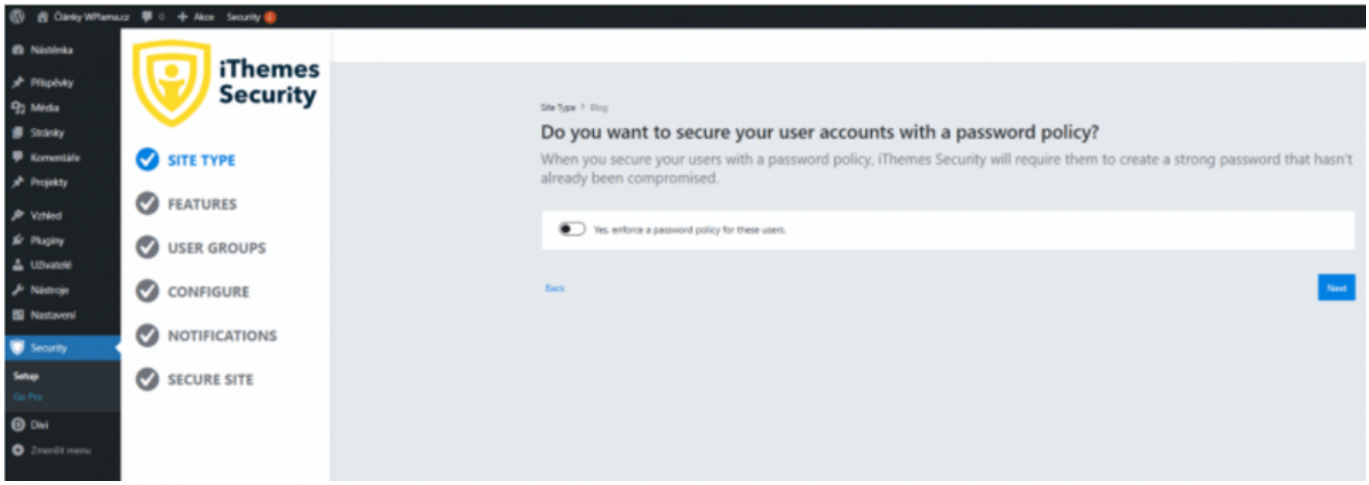
- Self (Pre seba)
- Client (Pre klienta)



3. Vynútenie silného hesla

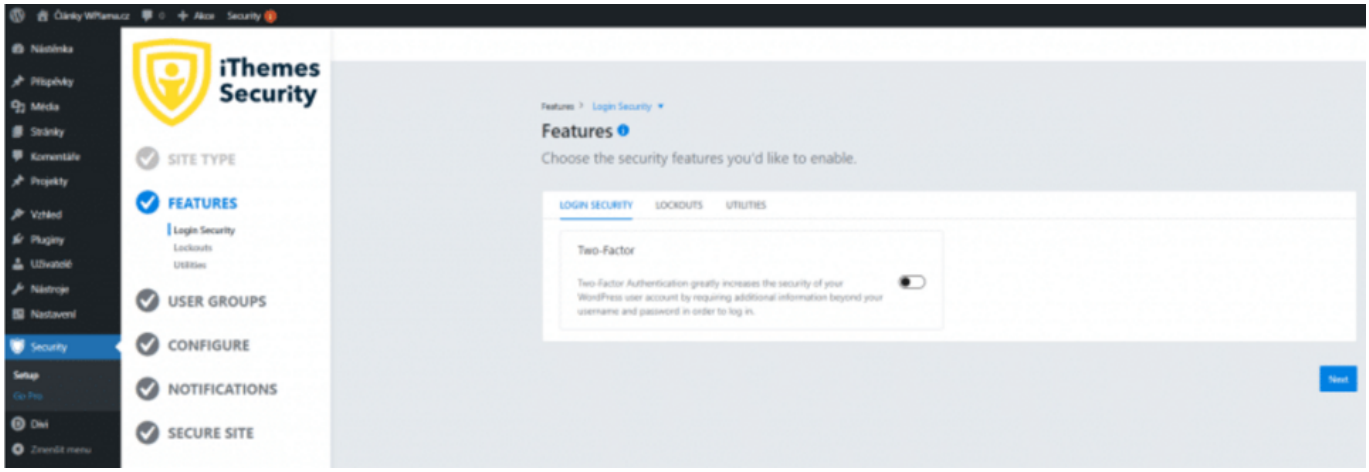
Potom si treba nastaviť vynútenie použitia silného hesla. Odporúčame si túto možnosť aktivovať.

V prípade, že bude mať administrátor slabé heslo, plugin ho donúti si ho pri ďalšom prihlásení zmeniť na silné.



4. Features

Plugin obsahuje aj užitočné funkcie na ochranu webu. V tomto kroku si ich môžete nastaviť.



Login Security

- Two-Factor – dvojfázové overenie pomocou e-mailu pri prihlásení zašle na e-mail používateľa kód, ktorým sa overí jeho identita.

Lockouts

- Local Brute Force – ochrana proti prelomeniu hesla hrubou silou, pri ktorom sa útočník snaží heslo uhádnuť pomocou náhodných kombinácií.
- Network Brute Force – prihlásenie do systému iThemes, kde sa predávajú informácie o „zlých IP“, po ktorom je používateľ z tejto IP automaticky zablokovaný.

Utilities

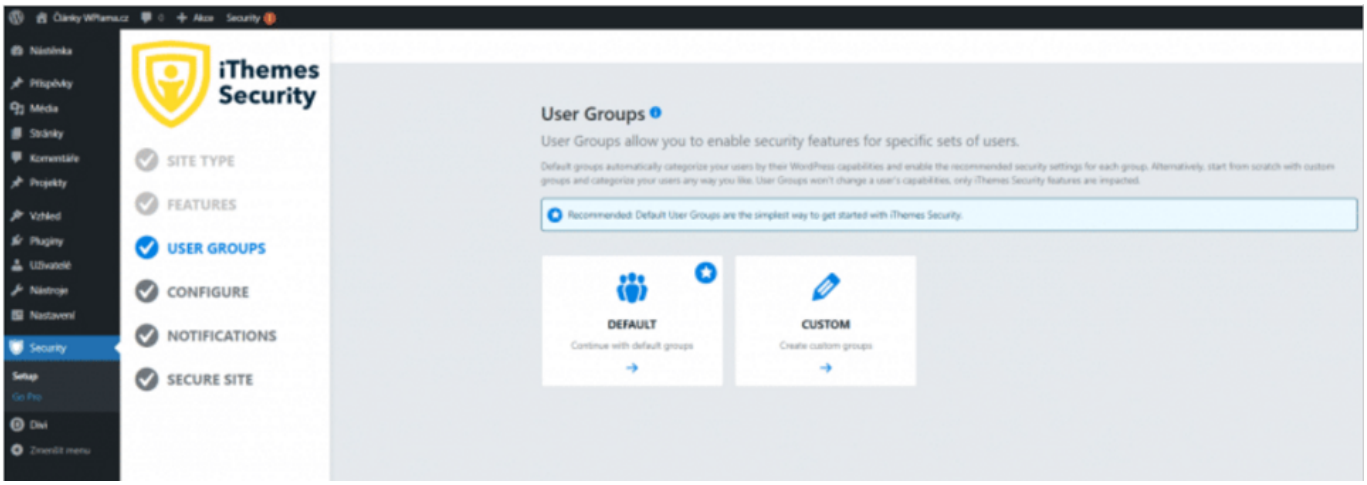
- Security Check Pro – kontrola IP adresy používateľa pri prihlásení.

5. User Groups

V tomto kroku si môžete upraviť jednotlivé nastavenia pre používané používateľské skupiny.

Na výber máte z možností:

- Default (Predvolené) – v drvivej väčšine prípadov využite toto
- Custom



V prípade, že ste zvolili predvolené používateľské skupiny, môžete si teraz upraviť ich jednotlivé nastavenia.

Ide o skupiny Administrátor, Editor, Spolupracovník, Autor, Návštevník a ostatné.

Nastavenie pre jednotlivé používateľské roly je:

Global Settings

- Manage iThemes Security – povoliť úpravu nastavenia iThemes Security

Security Dashboard

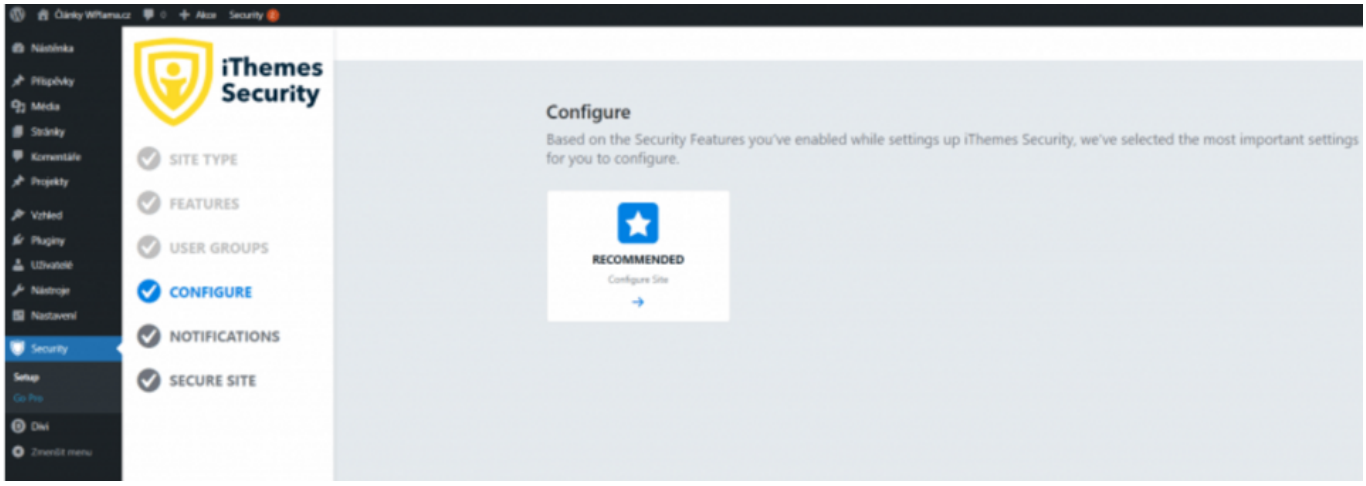
- Enable Dashboard Creation – prístup na nástenku pluginu.

Password Requirements

- Strong Passwords – silné heslá, po aktivácií budú používatelia pri registrácii prinútení zvoliť silné heslo (podľa WordPress hodnotení).
- Refuse Compromised Passwords – vynútenie použitia hesla, ktoré sa neobjavilo v žiadnej databáze uniknutých hesiel.

6. Configure

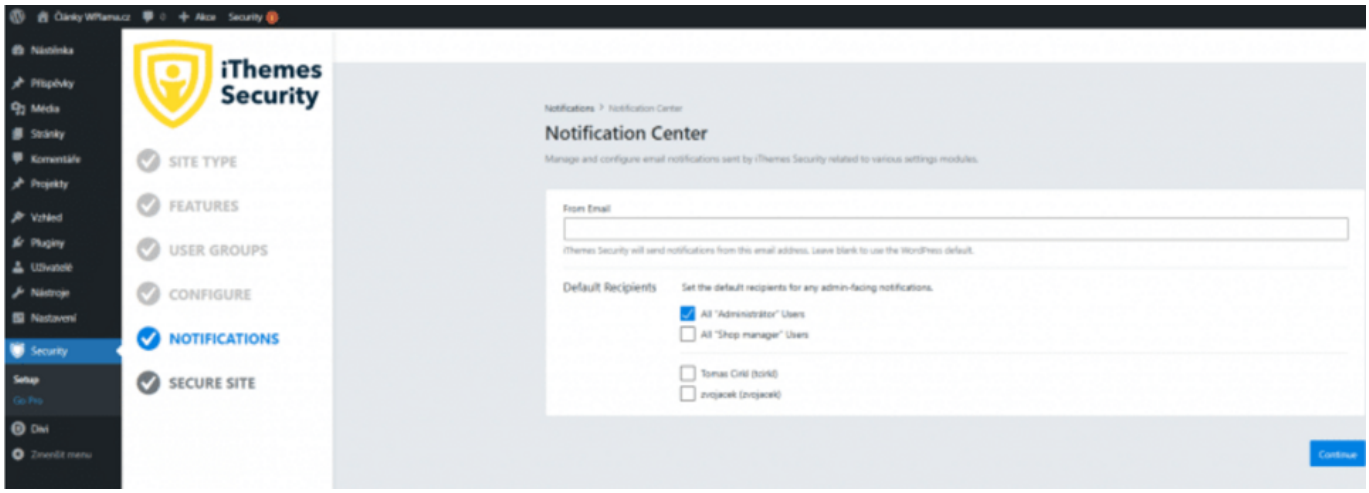
Základné nastavenie pluginu a prístupov.



- Authorized Hosts – tu si môžete pridať IP adresy overených používateľov, tieto IP sa zaradia na whitelist a nemôže pri nich dôjsť k banu.
- API Configuration – zadajte e-mail na aktiváciu Network Brute Force.

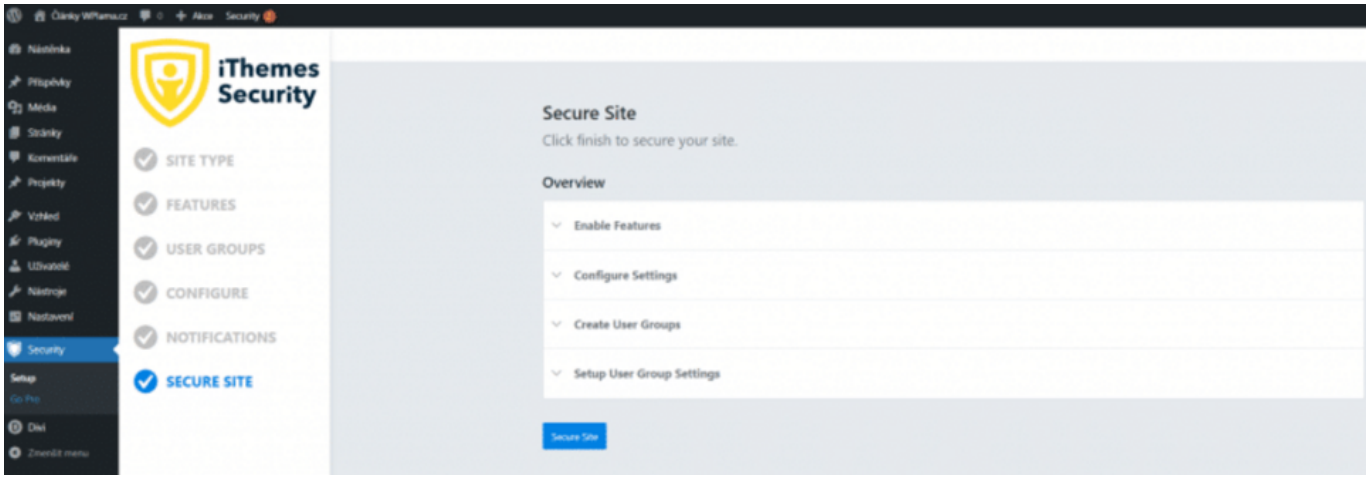
7. Notification Center

V centre notifikácií si môžete nastaviť pravidlá, na aký e-mail, prípadne akej používateľskej role príde upozornenie pri bezpečnostnej udalosti.



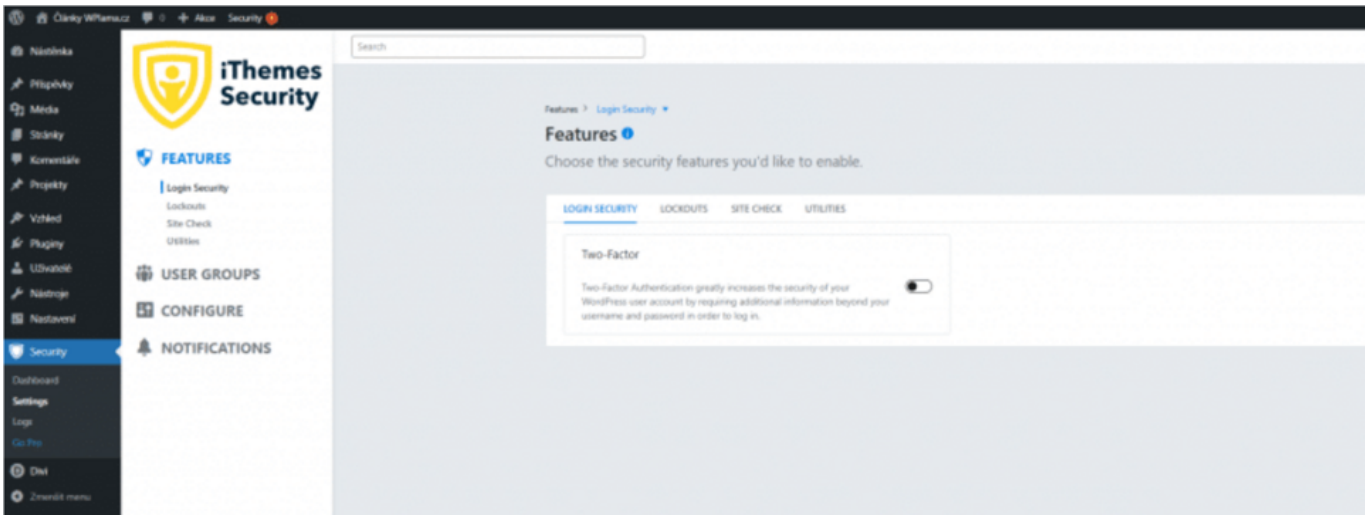
8. Secure Site

Posledným krokom základného nastavenia je zhrnutie a uloženie.



Ďalšie voliteľné nastavenia iThemes Security

Okrem základného nastavenia má plugin aj ďalšie možnosti, ktoré si predstavíme nižšie.



Features:

Login Security

- **Two-Factor –** dvojfázové overenie pomocou e-mailu, pri prihlásení zašle na e-mail používateľa kód, ktorým sa overí jeho identita.

Lockouts

- **Ban Users –** povolí funkciu banovania používateľov.
- **Local Brute Force –** povolí funkciu ochrany proti útoku hrubou silou.
- **Network Brute Force –** povolí prihlásenie do systému iThemes, kde sa predávajú informácie o „zlých IP“, potom je používateľ z tejto IP automaticky zablokovaný.

Site Check

- **File Change –** funkcia, ktorá detekuje zmeny v súboroch vašej WordPress inštalácie. Po jej aktivácii sa vám môže zobraziť upozornenie, že pri aktuálnom nastavení maximálnej pamäte pre PHP skripty môže prísť k deaktivácii webu práve kvôli chybe pri nedostatku pamäte. Na bežnom hostingu asi bude s touto funkciou problém. Ak máte VPS s aspoň 256 MB PHP pamäte, nemali by nastať problémy. Musíte si však funkciu otestovať na svojom nastavení.

Utilities

- **Enforce SSL –** vynútenie použitia SSL.
- **Database Backups –** pretože základom bezpečnosti akejkoľvek internetovej stránky je práve zálohovanie, iThemes Security sa dokáže postarať o automatické

pravidelné zálohy databázy a ich odosielanie na email alebo ukladanie na server.
- **Security Check Pro –** kontrola IP adresy používateľa pri prihlásení.

User Groups

Global Settings

- **Manage iThemes Security –** povoliť úpravu nastavenia iThemes Security

Security Dashboard

- **Enable Dashboard Creation –** prístup na nástenku pluginu.

Password Requirements

- **Strong Passwords –** silné heslá, po aktivácii budú používatelia pri registrácii prinútení zvoliť si silné heslo (podľa WordPress hodnotení).
- **Refuse Compromised Passwords –** vynútenie použitia hesla, ktoré sa neobjavilo v žiadnej databáze uniknutých hesiel.

Configure

Global Settings

- **Write to Files –** povolí zapisovať pluginu iThemes Security do súborov wp-config.php a .htaccess.
- **Lockouts**
  – Minutes to Lockout – čas, počas ktorého bude používateľ zabanovaný po dosiahnutí limitu počtov prihlásení.
  – Days to Remember Lockouts – časové okno, v ktorom musí používateľ daného počtu banov dosiahnuť
  – Ban Repeat Offender – ak túto možnosť zaškrtnete, bude používateľ po určitom množstve (nastavíte neskôr) dočasných banov pridaný na čiernu listinu, čo znamená, že bude zabanovaný navždy. Niektorí roboti sú nepoučiteľní a stále sa vracajú, týmto dôjde k ich úplnému zablokovaniu.
  – Ban Threshold – po koľkých blokáciách (dočasných banoch, lockoutoch) dôjde k pridaniu na čiernu listinu.
- **Lockout Messages**
  – Host Lockout Message – táto správa sa zobrazí pri zablokovaní serveru (IP adresy), môžete použiť niektoré HTML tagy (ich zoznam je pod formulárom

– User Lockout Message – správa pre zablokovaného používateľa (zvyčajne, ak je zabanovaný kvôli veľkému množstvu neúspešných pokusov o prihlásenie).
– Community Lockout Message – táto správa sa zobrazí používateľovi, ktorý bol zablokovaný na základe nesprávnej IP adresy.

- **Authorized Hosts**
  – Automatically Temporarily Authorize Hosts – po prihlásení používateľa ho iThemes pridá na 24h na whitelist.
  – Authorized Hosts – IP adresy autorizovaných používateľov.
- **Logging**
  – How should event logs be kept – kam by sa mali ukladať logy (odporúčame databázy).
  – Days to Keep Database Logs – na ako dlho uchovávať logy.
- **IP Detection**
  – Proxy Detection – typ detekcie IP adresy
- **UI Tweaks**
  – Hide Security Menu in Admin Bar – ukryje iThemes Security položku z hornej WordPress lišty.
  – Enable Grade Report – povolí Grade Report správy pri notifikáciách.

Lockouts

- **Default Ban List –** touto možnosťou okamžite zabanujete všetky IP adresy uvedené v zozname, ktorý dal dokopy Jim Walker z HackRepair.com, **odporúčame nezapínať**, Seznam bot je súčasťou banu.
- **Enable Ban Lists** – povolí funkciu banovania používateľov.
- **Automatically ban „admin“ user –** automaticky zabanuje používateľa, ktorý sa chce prihlásiť s používateľským menom admin.
- **Login Attempts**
  – Max Login Attempts Per Host – maximálny počet pokusov o prihlásenie z IP.
  – Max Login Attempts Per User – maximálny počet pokusov o prihlásenie pre používateľa.
- – Minutes to Remember Bad Login (check period) – obdobie, počas ktorého si plugin pamätá neúspešné pokusy.
- **Ban Reported IPs –** banovať zlé IP.

Utilities

- **Scheduling**
  – Schedule Database Backups – zaškrtnutím povolíte pravidelnú zálohu databázy.
- **Configuration**

– Backup Method – spôsob zálohovania (e-mailom, na hosting).
- – Compress Backup Files – povoliť kompresiu zálohy.
- **Backup Tables –** aké tabuľky databázy sa budú zálohovať.

Notifications

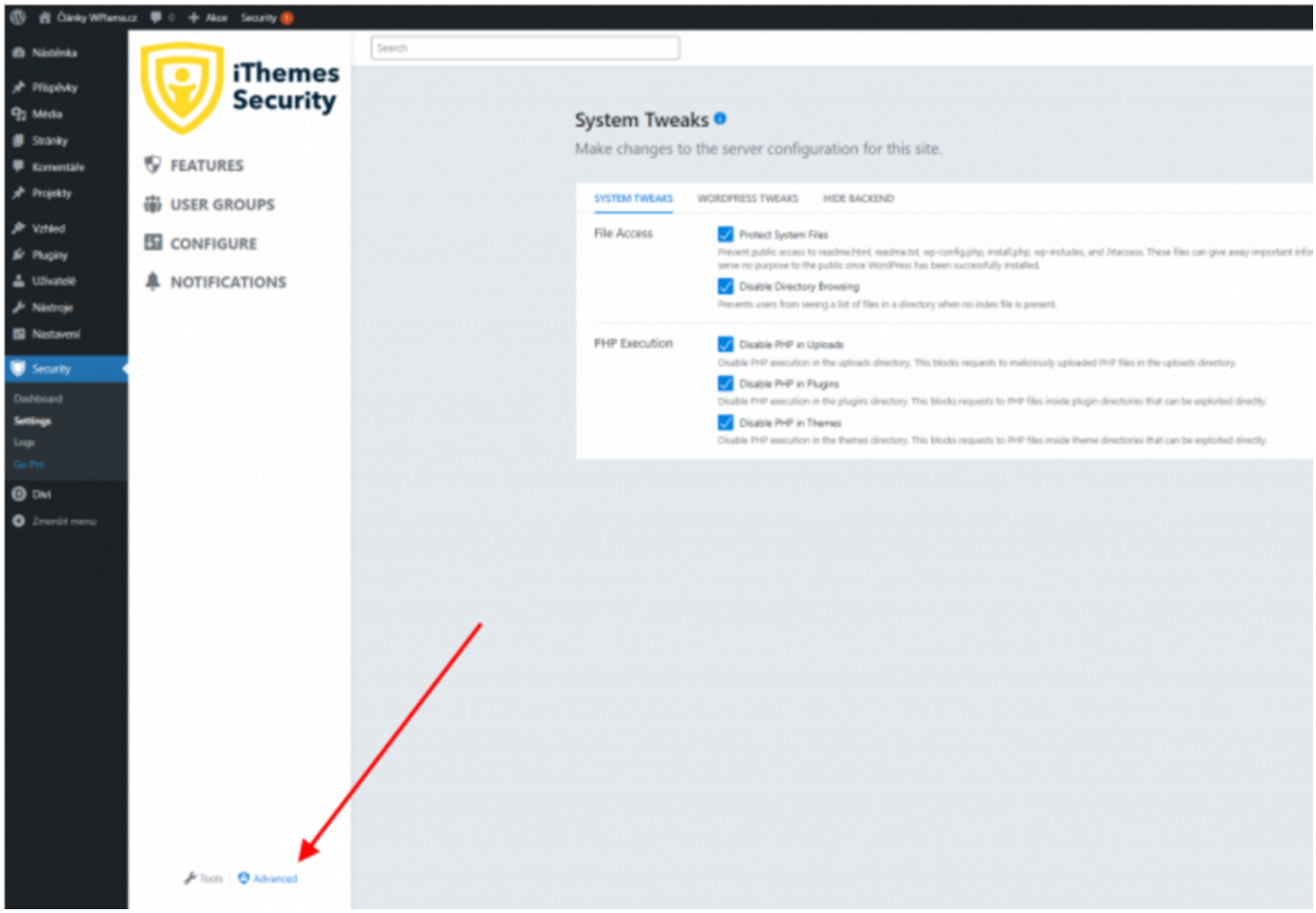
From Email – nastavenie e-mailu použitého ako odosielateľ.

Default Recipients – predovlená príjemci upozornení. Zaškrtnite vybrané.

- – Enabled – aktivuje toto upozornenie.
  – Customize – zmena predmetu e-mailu.
  – Schedule – frekvencia odosielania upozornení.
  – Recipient – príjemcovia upozornení.
- **Security Digest –** denná súhrnná správa s informáciami o bezpečnosti webu.
  – Enabled – aktivuje toto upozornenie.
  – Customize – zmena predmetu e-mailu.
  – Recipient – príjemci upozornení.
- **Site Lockouts –** upozornenie pri zabanovaní používateľa. Pozor, pri väčšom útoku na web môžete naraz dostať aj stovky e-mailov. Aktiváciu preto zvážte.
  – Enabled – aktivuje toto upozornenie.
  – Customize – zmena predmetu e-mailu.
- – Recipient – príjemci upozornení.
- **Database Backup –** upozornenie po vytvorení zálohy databázy.
  – Customize – zmena predmetu e-mailu.
  – Recipient – príjemci upozornení.

Pokročilé nastavenie v iThemes Security

V ľavom dolnom rohu v nastavení pluginu nájdete odkaz na pokročilé nastavenie. Poďme sa pozrieť, na jednotlivé možnosti, ktoré tu máte k dispozícii.



System Tweaks – Úpravy v nastavení serveru.

- **File Access**
  – Protect System Files – touto funkciou zamedzíte komukoľvek zobraziť súbory readme.html, readme.txt, wp-config.php, install.php, wp-includes a .htaccess, ktoré môžu prezradiť dôležité informácie (napríklad verziu WordPressu).
  – Disable Directory Browsing – zamedzí používateľom zobrazovať adresáre, kde nie je žiadny index súbor. Zamedzí hackerom poznať adresárovú štruktúru vášho webu. Túto znalosť by mohol skúsený hacker zneužiť.
- **PHP Execution**
  – Disable PHP in Uploads – zabráni vykonávaniu PHP skriptov v adresári Uploads.
  – Disable PHP in Plugins – zabráni vykonávaniu PHP skriptov v adresári Plugins.
  – Disable PHP in Themes – zabráni vykonávaniu PHP skriptov v adresári Themes (WordPress šablóny).

System Tweaks – Úpravy v správaní WordPressu.

- **Disable File Editor**
  – základná bezpečnostná funkcia, ktorá vypne editor kódu v administrácii.

- **API Access**
  – XML-RPC – deaktivácia XML-RPC funkcie. Odporúčame vypnúť, ale následne vám nebudú fungovať niektoré pluginy, ktoré XML-PRC vyžadujú (napr. JetPack).
  – REST API – deaktivácia REST API.
- **Users**
  – Login with Email Address or Username – povolí možnosť prihlásenia pomocou e-mailu, používateľského mena alebo jedného z nich.
  – Force Unique Nickname – pri registrácii a aktualizácii profilu bude WordPress vyžadovať unikátne používateľské meno.
  – Disable Extra User Archives – vypne zobrazovanie profilov používateľov (Author Page), ktorí na vašu stránku neprispievajú, vďaka čomu sa zamedzí zhromažďovaniu používateľských mien rôznymi robotmi.

Hide Backend – Presun prihlasovacieho formulára na inú adresu než /wp-admin, wp-login.php a ďalšie predvolené adresy WordPressu je jedným zo základných prvkov obrany proti hackerom a rôznym botom.

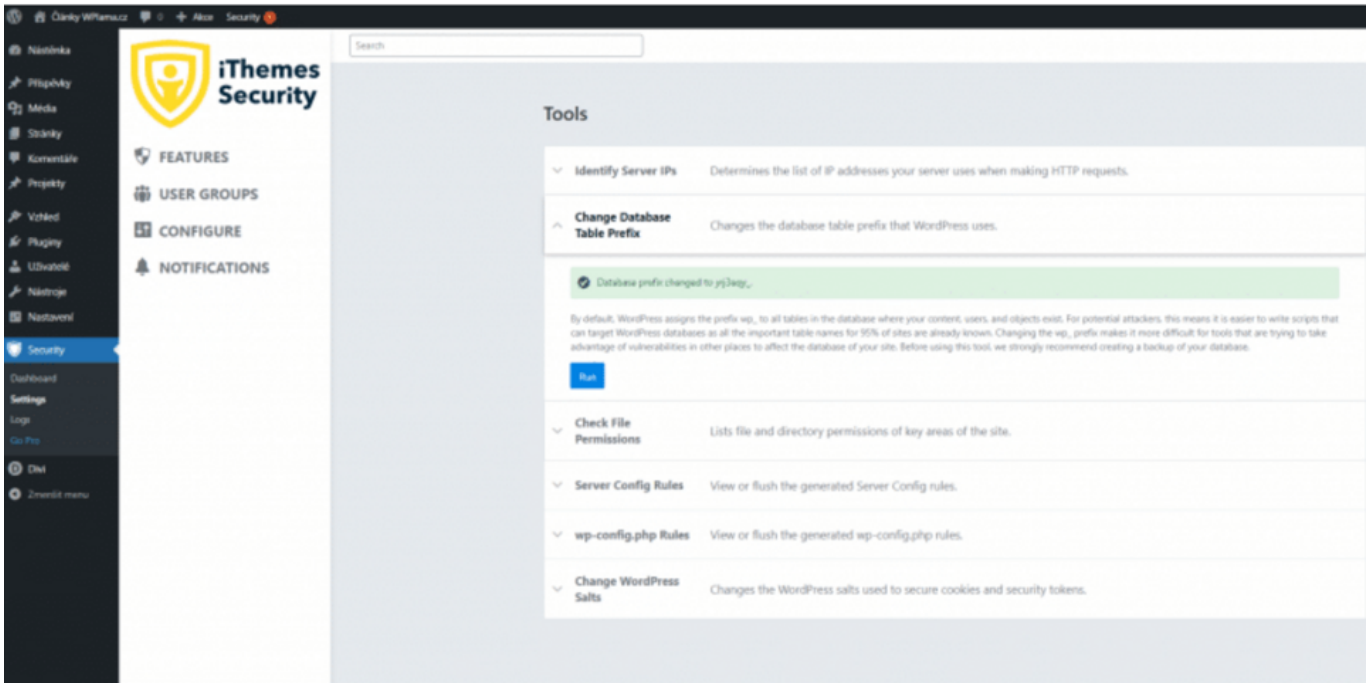
WordPress je dnes už notoricky známym redakčným systémom pre všetkých, ktorí majú niečo spoločné s tvorbou webu, takže každý vie, kde sa prihlasovacia obrazovka nachádza.

Aby sme hodili ďalšie poleno pod nohy všetkým hackerom, zmeníme si adresu na login do administrácie.

- **Hide Backend**
  – aktivujte na „ukrytie“ všetkých formulárov na prihlásenie.
- **URLs**
  – Login Slug – slovo, ktoré bude použité na stránke s prihlasovacím formulárom. Predvolený je „wplogin“ – odporúčame nastaviť na iné slovo ako „logintowp“, „wpprihlasenie“ a pod. V prípade „logintowp“ by ste potom prihlásenie do administrácie našli na adrese www.vasadomena.sk/logintowp.
  – Register Slug – slovo na registráciu.
- **Redirection**
  – Enable Redirection – povolí presmerovanie.
  – Redirection Slug – slovo, kam bude presmerovaný používateľ pri zadaní zablokovaného štandardného prihlasovacieho formulára.
- **Advanced**
  – Custom Login Action – WordPress používa na obsluhu prihlasovania/odhlasovania premennú action, ktorá môže nadobúdať najrôznejšie hodnoty. iThemes Security zvláda tie základné, ale niektoré šablóny alebo pluginy môžu vyžadovať vlastnú akciu. Ak o nejakej podobnej akcii viete, môžete ju pridať

(zvyčajne to však nie je potrebné).

Change Database Prefix – zmena prefixu databázy



Poznámka: Pred touto zmenou odporúčame spraviť si zálohu databázy.

Databáza je asi najdôležitejším prvkom celej WordPress inštalácie, a preto jej bezpečnosť neradno podceňovať.

Jedným zo základných zabezpečovacích krokov je uvedenie iného než predvoleného prefixu tabuliek („wp_“).

Zmena prefixu je s pluginom iThemes Security veľmi jednoduchá:

1. V **Settings** vyberte v ľavom dolnom rohu **Tools**.
2. Tu je rozbaľovacia položka **Change Database Prefix**.
3. Po rozbalení kliknite na **Run** a prefix databázy je zmenený.

Sekcia Logs

Logy nájdete v ľavom WordPress menu **Security → Logs**.

V logoch môžete nájsť všetky problémy odhalené pluginom iThemes Security.

Ak napríklad niekto uskutoční neúspešný pokus o prihlásenie, uvidíte to tu. Ak sa niekomu objaví chyba 404, hlásenie bude aj v logu.

Čas od času je dobré sa do logov pozrieť, aj napriek tomu, že o dôležitých udalostiach budete upozornení e-mailom (ak ste si to tak nastavili v **Settings → Nastavenie**).

Na záver

Zabezpečenie WordPressu by sa určite nemalo podceňovať a iThemes Security je skvelý plugin schopný odstrániť široké spektrum bezpečnostných problémov, ktorými WordPress trpí.

Dúfame, že článok vám trochu pomôže s nastavením bezpečnosti na vlastnom webe.