WPLAMA

# Analýza zranitelnosti WordPress stránky

**www.vasedomena.cz**

1.1. 2019

# 1. Zjištěné informace

- verze WordPress: 4.9.8
- server: Apache/2.4.25
- php: PHP/7.0.30

# 2. Zajímavá místa

*/wp-admin*

*/wp-login.php*
Doporučení: Změňte adresu pro přihlášení. Snížíte tím možnost útoku hrubou silou na váš web.

*/wp-admin/admin-ajax.php*
Doporučení: Je možno zablokovat nicméně je velké riziko, že některé části webu nebudou fungovat.

*/wp-content/debug.log*
Doporučení: Pokud to není nutné, vůbec nenechávejte generovat. Popřípadě odstraňte hned, jak se s tím nebude pracovat. Upravte práva čtení tak, aby nebylo možné zobrazit přes odkaz z prohlížeče.

# 3. Šablony

twentyseventeen – nutná aktualizace. Zvýšená možnost napadení.

# 4. Pluginy

Google-analytics-for-wordpress 7.3.0
Wordpress-seo 9.2.1
akismet
jetpack 6.7
Responsive-lightbox 2.0.5
monarch 1.4.8
tablepress 1.9.1
w3-total-cache
Contact-form-7 0.9.7
mailpoet 3.14.1
bloom 3.17.3

Zjištěna přítomnost MU pluginů.
V aktuálních verzích nejsou u pluginů známa žádná bezpečnostní rizika.

# 5. wp-config.php

Nezjištěna záloha souboru wp-config.php. Soubor je ideální zálohovat mimo prostor webu. Pokud máte hosting, který automaticky zálohuje web, nemusíte zálohovat ručně.

# 6. Databáze

Záloha nezjištěna.

O automatické zálohování by se měl starat hosting. Nedoporučuje se mít zálohu databáze uloženou na hostingu společně se soubory webu.

# 7. Uživatelé

- Admin
- spravce
- petr15
- Kacie
- istiedemann

# 8. Možnost napadení

## Path Traversal

- https://www.vasedomena.cz/themeforest-trziste
- https://www.vasedomena.cz/themeforest-wordpress
- https://www.vasedomena.cz/themeforest

Pravděpodobně se jedná o PrettyLink odkazující na jinou stránku. Nemusí se jednat o chybu u vás, ale na cílovém webu.

## Remote OS Command Injection

http://www.vasedomena.cz/wp-admin/load-styles.php?c=0&dir=ltr&load%5B%5D=dashicons%2Cbuttons%2Cforms%2Cl10n%2Clogin&ver=4.9.8%22%7Ctimeout+%2FT+15

Velmi nízká pravděpodobnost zneužití.

## MySQL Injection

Nalezeno v 17 souborech.
Neprokázalo se v žádném případě. Pravděpodobně zabezpečeno.

## Útok hrubou silou

Nelze uskutečnit.

# 9. Souhrn

**Kritické chyby**
Nenalezeny

**Nekritické chyby**
Nutno provést aktualizace.

O Vašem webu se nám podařilo zjistit průměrné množství informací. V případě, že se některé informace nepodařilo získat, je to dobře. Čím méně se o webu dá zjistit, tím je šance na nalezení bezpečnostní díry menší.

Váš web se nám nepodařilo napadnout.

*naše testy trvají několik dní takže je možné že se verze budou lišit