УДК 004.056.53

М.О. Мельник, Р.В. Дудко, А.Д. Поліщук

Одеський національний політехнічний університет, Одеса

ОРГАНІЗАЦІЯ ЗАХИСТУ САЙТУ, СТВОРЕНОГО НА ПЛАТФОРМІ WORDPRESS ЗА ДОПОМОГОЮ ПЛАГІНА ITHEMES SECURITY

В роботі було встановлено, що саме за допомогою плагіна iThemes Security можна подолати будь-які загрози безпеки сайту. Плагін iThemes Security створений для запобігання будь-яким спробам несанкціонованого доступу до WordPress за допомогою різноманітних методів.

Ключові слова: *плагін iTHEMES SECURITY, Word Press, концепція електронної безпеки, система управління вмістом (CMS).*

Вступ

За даними лабораторії W3Techs, 25% всіх сайтів мережі Інтернет працюють під управлінням WordPress [4]. Успіх WordPress зумовлений низкою факторів. WordPress має вдалу архітектуру побудови програмного забезпечення. У нього відкритий вихідний код. WordPress безкоштовний і відносно простий в освоєнні. «Ядро» WordPress має базову функціональність, розширити яку можна за допомогою окремих програмних модулів, які називаються плагінами. Дизайн сайту на CMS WordPress реалізується за допомогою так званих «тем», які можна налаштовувати. Це як в порівнянні з автомобілем: «ядро» WordPress – це двигун і шасі, плагіни – це додаткова комплектація (кондиціонер, наприклад), а теми – це дизайн автомобіля, його колір, елементи оформлення, оббивка салону. Така логічність дозволяє відносно просто конструювати проекти різної функціональної складності. На WordPress створено широкий спектр сайтів: від найпростіших блогів до складних порталів, корпоративних сайтів і інтернет-магазинів.

Проблеми безпеки електронних магазинів не втрачають своєї актуальності. З кожним роком відкривається тисячі електронних магазинів, але 85% існують менше року [1]. Така статистика пов`язана не тільки зі складним економічним становищем, а з питаннями безпеки інформації. На сьогоднішній день більшість сайтів представляють собою набір запчастин, пов'язано це з низьким рівнем стандартної розробки, відсутністю єдиної концепції безпеки, використанням декількох акаунтів для одного користувача та ін.

Необхідно звернути увагу на те, що при зміні стандартних налаштувань JS додаткові розширення можуть не працювати. Такі проблеми можуть виникнути, якщо підключити JS скрипт у файлі шаблону, а потім використовувати плагін, якому потрібен цей же скрипт. Таким чином порушується логіка підключення і плагін не буде функціонувати. Найчастіше таке відбувається з JavaScript бібліотеками, наприклад з підключенням jQuery.

Не слід забувати, що у більшості випадків розробники плагінів не мають доступу до файлів шаблону, створеного на платформі WP. Разом з тим розробники повинні гарантувати можливість підключення необхідних скриптів. Тому для розробників одним з кращих варіантом буде використання функція wp_enqueue_script. Ця функція підключає JS файл, якщо він не був підключений раніше, тобто можна викликати її кілька разів для одного і того ж скрипта і, при цьому, скрипт буде вставлений тільки один раз.

Метою статті є аналіз рівня інформаційної безпеки сучасних CMS для електронного магазину, аналіз існуючих засобів захисту та організація захисту адміністративної панелі в електронному магазині. Виявлення недоліків та запропонування розробка вдосконаленого захисту на базі існуючих.

Основна частина

Для досягнення поставленої мети необхідно вирішити наступні задачі

1. Провести аналіз найбільш використовуємих платформ для створення інтернет-магазинів. Вибрати найпоширенішу за наступними факторами: популярність, зручність адміністрування, технічна підтримка.

2. Провести аналіз існуючих засобів для організації захисту адміністративної панелі, розглядаємої платформи для створення інтернет-магазинів. Аналіз недоліків засобів, що пропонуються.

3. Розробка скомпільованого програмного модуля для захисту даних в інтернет-магазинах, створених на обраній платформі.

Аналіз найбільш використовуємих платформ для створення інтернет-магазинів показав, що Word Press є найпоширенішою. Подальші дослідження в роботі будуть пов'язані з платформою WordPress у

зв'язку з її популярністю, зручністю адміністрування, великим співтовариством користувачів і розробників. Так само однією з вагомих переваг є відмінна адаптація до пошукових алгоритмів, що є важливим для подальшого просування електронного магазину [2].

WordPress – це одна з найпопулярніших систем управління контентом в світі і, без всяких сумнівів, одна з найбільш захищених і безпечних платформ в інтернет-просторі. Але все одно, навіть вона вимагає додаткового захисту після установки, а нові користувачі повинні турбуватися про атаки хакерів. Саме це й визначає ***актуальність теми дослідження.***

WordPress є популярною програмою CMS, яку легко використовувати. Ось чому користувачі вибирають WordPress для створення динамічних вебсайтів. Але вони стикаються з труднощами вибору системи безпеки. Оскільки WordPress переповнений різноманітними рішеннями по її забезпеченню, розглянемо провідний плагін захисту сучасних сайтів на WordPress, а саме iThemes Security (в минулому відомого як Better WP Security).

Розглянемо його настройку і можливості, а також визначимо деякі додаткові можливості. Почнемо з установки плагіна iThemes Security.

Установка плагіна iThemes Security (рис. 1):

Рис. 1. Установка плагіна iThemes Security

Налаштування та використання. Налаштувати плагін досить легко, напевно, навіть легше, ніж будь-який з таких же популярних плагінів WordPress.

Розглянемо крок за кроком установку і використання плагіна, враховуючи всі нюанси.

Після успішної установки плагіна повернувшись на сторінку самого плагіна, ми побачимо наступне (рис. 2):

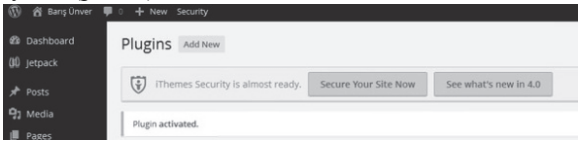

Рис. 2. Сторінка плагіна

Натиснувши на кнопку *Забезпечити свій сайт зараз* (Secure Your Site Now), нижче ми побачимо сторінку з модальним боксом (рис. 3):

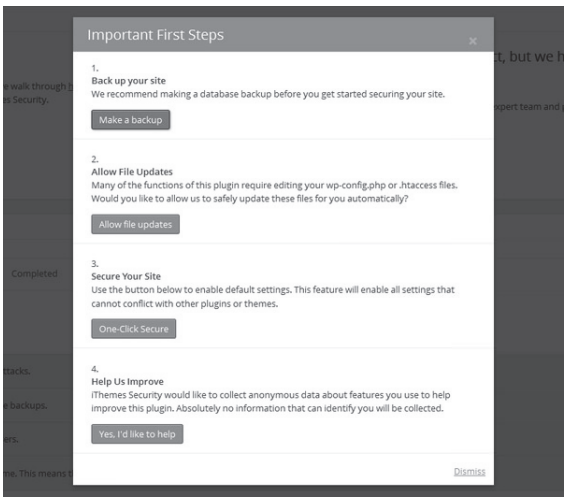

Рис. 3. Сторінка з модальним боксом

Ці кроки потрібно пройти користувачам-новачкам:

– створення резервних копій сайту: створює моментальний знімок установки плагіна на WordPress, що дозволить виправити всі помилки під час налаштування плагіна;

– дозвіл поновлення файлів: дозволяє iThemes Security працювати з основними файлами WordPress, як наприклад, wp-config.php і htaccess;

– безпека сайту: активування деяких рекомендованих налаштувань для забезпечення захисту сайту за допомогою одного кліка;

– покращення роботи з сайтом: отримання даних (анонімно) для поліпшення плагіна.

Після цього можна переходити до дашборду.

Панель управління плагіном (рис. 4):

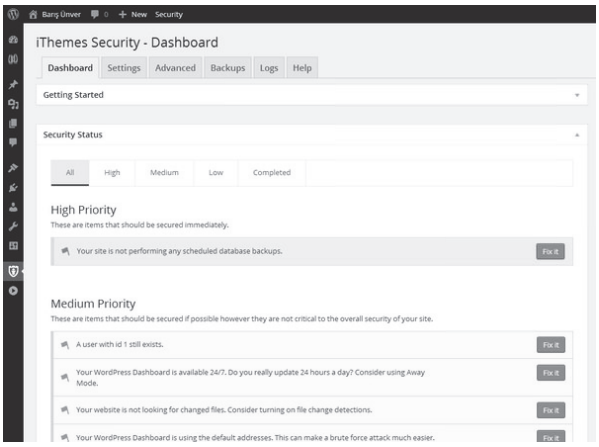

Рис. 4. Панель управління плагіном

На цій сторінці можна перевірити «Статус безпеки» за допомогою перевірки статусу пунктів, які потрібно задіяти. Ці пункти розділені на кілька категорій пріоритетності: високої, середньої, низької та завершені.

Рекомендується звернути особливу увагу на перші два пункти, щоб переглянути пункти з низь-

кою пріоритетністю, з метою переконання в їх корисності для безпеки сайту.

Сторінка налаштувань (рис. 5):

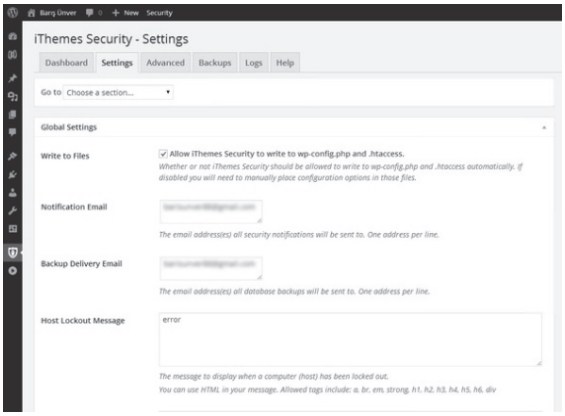

Рис. 5. Сторінка налаштувань

На цій сторінці досить багато інформації для ознайомлення, а саме:

– глобальні налаштування;

– виявлення помилки: сторінки 404;

– режим недоступності «немає на місці»;

– блокування користувачів;

– захист пароля сайту на WordPress від злому (Brute Force Protection);

– створення резервних копій даних;

– виявлення змін файлів;

– приховування поля з логіном;

– протокол захисту даних - Secure Socket Layers (SSL);

– надійні паролі;

– безкоштовна програма System Tweaks для тонкої настройки прихованих параметрів системи;

– плагін WordPress Tweaks для детальної настройки движка WP.

Налаштувати плагін можна на свій розсуд, включати / виключати потрібні параметри і функції.

Розширені налаштування (рис. 6):

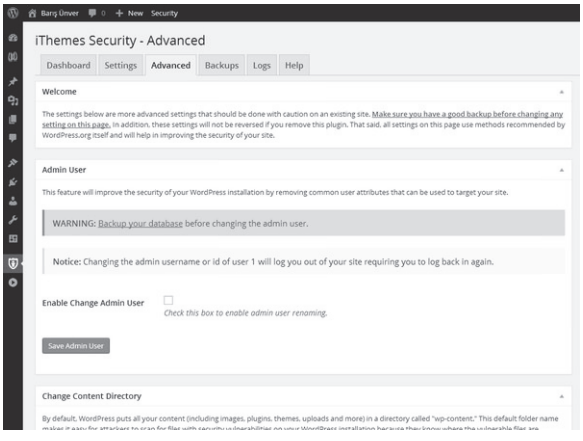

Рис. 6. Розширені налаштування

На відміну від "Сторінки налаштувань", яка має безліч маленьких налаштувань, розширені налаштування включають в себе тільки три дуже важливих інструменти для підвищення безпеки сайту [2]:

1. Зміна адміністратора: адмін на WordPress з номером ID користувача «1» або ім'ям «admin» може нашкодити вашому сайту, якщо він не буде добре захищений в майбутньому. Щоб скоротити ризик злому сайту хакерами невідомими хакерськими методами, потрібно змінити ім'я користувача адміністратора за допомогою цього інструменту.

2. Зміна папки з контентом: хакери можуть просканувати ваш сайт, як це робить пошукова система, і знайти «вразливі» файли, які можна пошкодити. Наприклад, якщо плагін WordPress не володіє гарним захистом, то хакери можуть просканувати сайт паралельно з папками wp-content сайтів на WordPress. Цей інструмент дозволяє змінити назву папки wp-content, щоб її важче було знайти.

3. Зміна префікса бази даних: якщо сервери провайдера використовуваного хостингу «уразливі», то хакери можуть атакувати їх, проникнувши в систему. Як і два попередніх, цей інструмент запобігає ймовірності ризику для сайту за допомогою зміни префікса бази даних wp. Завдяки цьому хакерам буде складніше знайти таблиці бази даних.

Ці настройки є досить «крихкими», якщо взагалі можна так сказати про налаштування. І з ними можуть виникнути проблеми, як наприклад, неможливість увійти в систему, або ж, повне руйнування бази даних.

З цієї причини варто зробити резервне копіювання бази даних перед тим, як внести в неї подібні зміни. У разі виникнення будь-яких проблем можна скасувати всі дії, відновивши резервну копію.

Додаткові поради з безпеки:

– вибір надійного хостинг-провайдера: хакери все одно зможуть нашкодити сайту, якщо його сервери не є достатньо надійними;

– не нехтувати протоколом SSL: хоч і плагін дозволяє використання SSL, ми не зможемо цього зробити, поки не придбаємо відповідний сертифікат. Необхідно зв'язатися з хостинг-провайдером для активації HTTPS-з'єднання на сайті на WordPress;

– захист комп'ютера і поштового акаунта: хакери можуть спробувати усі способи, щоб зламати ваші паролі, тим самим впровадити віруси і отримати облікові дані. І щоб захистити свій комп'ютер і email-аккаунт, необхідно використовувати якісне програмне забезпечення безпеки і надійного інтернет-провайдера;

– пильність: плагін iThemes Security робить все можливе, щоб захистити ваш сайт на WordPress. Але все одно не можна повністю довіритися програмі або будь-який інший системі.

Висновки

В результаті роботи було встановлено:

1. Завдяки «відкритості» WordPress постійно розвивається: розробляються нові плагіни, появляються нові теми, виходять нові версії CMS.

2. WordPress дозволяє з великою легкістю здійснювати найскладніші рішення; підтримує pingback, RSS, trackback, Atom; модулі мають просту і унікальну систему їх взаємодії з основним кодом; підтримка тих чи інших шаблонів дозволяє легко змінювати не тільки сам зовнішній вигляд, а й також різні способи виведення даних; можливість інтеграції форуму, інтернет-магазину або соціальної мережі; підтримка різних медіаформатів; розповсюджується безкоштовно.

3. З використанням плагіна iThemes Security можна подолати будь-які загрози безпеки сайту. Плагін iThemes Security Pro створений, щоб допомогти запобігти будь-яким спробам несанкціонованого доступу до WordPress за допомогою різноманітних методів. Досить сказати, що розробник заклав досить лазівок в безпеці, які раніше були властиві блогам на WordPress.

4. Перераховані методи допоможуть істотно підвищити безпеку ресурсу на платформі WordPress і вберегти його від несанкціонованого доступу.

Список літератури

1. Грачев А. Создаем свой сайт на WordPress. Быстро, легко и бесплатно. Работа с CMS. WordPress 3 / А. Грачев. – СПб.: Питер, 2011. – 288 с.

2. Макдональд М. Создание Web-сайтов. Основное руководство / М. Макдональд; [пер. с англ. М.А. Райтмана]. – М.: Эксмо, 2010. – 768 с.

3. Хассей Т. WordPress для профессионалов / Т. Хассей. – М.: Эксмо, 2012. – 432 с.

4. WordPress: история, преимущества, недостатки, версии Read more at [Електронний ресурс] // INETru.net. – Режим доступу до ресурсу: http://inetru.net/wordpress.html.

Надійшла до редколегії 2.03.2017

Рецензент: д-р техн. наук проф. В.В. Скачков, Військова академія, Одеса.

ОРГАНИЗАЦИЯ ЗАЩИТЫ САЙТА, СОЗДАННОГО НА ПЛАТФОРМЕ WORDPRESS С ПОМОЩЬЮ ПЛАГИНА iTHEMES SECURITY

М.А. Мельник, Р.Н. Дудко, А.Д. Полищук

В работе было установлено, что именно с помощью плагина iThemes Security можно преодолеть любые угрозы безопасности сайта. Плагин iThemes Security создан для предотвращения любых попыток несанкционированного доступа к WordPress с помощью различных методов.

***Ключевые слова**: плагин iTHEMES SECURITY, Word Press, концепция электронной безопасности, система управления содержимым (CMS).*

PROTECTING SITES CREATED BY PLATFORM WORDPRESS WITH PLUGINS iTHEMES SECURITY

M. Melnyk, R. Dudko, A. Polishcyk

In this article it was found that it is through by iThemes Security plugin, you can overcome any site security threats. iThemes Security Plugin is created to prevent any unauthorized access to WordPress using different methods.

***Keywords:** plugin iTHEMES SECURITY, Word Press, electronic security concept, content management system (CMS).*