УДК 004.056.53 DOI: 10.30748/soi.2017.148.23

М.О. Мельник, Н.С. Константинова, О.В. Бескупський

Одеський національний політехнічний університет, Одеса

ОРГАНІЗАЦІЯ ЗАХИСТУ ІНТЕРНЕТ-РЕСУРСУ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ ТА ПРОГРАМНИЙ ЗАХИСТ АВТОРСЬКИХ ПРАВ

У роботі була обрана найпоширеніша платформа для створення як персональних сайтів, так і комерційних порталів – CMS WordPress. Критеріями для вибору системи управління вмістом послугували: кількість встановлень, якість технічної підтримки та доступність інформаційних матеріалів. Було переглянуто готові рішення для задоволення кінцевих потреб. Проведений аналіз недоліків та вразливостей готових рішень. Розроблено план захисту та індивідуальне програмне рішення з урахуванням виявлених недоліків.

Ключові слова: *сайт, розширення, плагін, Word Press, аутентифікація, авторизація, водний знак, система управління вмістом (CMS), IP-адреси.*

Вступ

На сьогоднішній день великою популярністю користується ведення бізнесу через мережу інтернет: перепродаж товарів за допомогою невеликих інтернет магазинів, просування сервісних послуг через сайти-візитки, продаж своєї handmade продукції (товари ручної роботи) та інше [1].

Найчастіше для створення таких сайтів використовуються так звані системи управління вмістом (Content management system, CMS). Перевагами такого підходу є мала ціна розробки сайтів, велика кількість спеціалістів, простота адміністрування сайту, велика кількість готових рішень (плагінів та розширень).

Недоліки випливають з цих же переваг. Відкритий програмний код, передбачає те, що людина з достатнім рівнем знань може дослідити систему та виявити вразливість, велика кількість спеціалістів та низька ціна може бути причиною низької якості виконання робіт.

Найпоширенішою системою управлінням вмістом на момент написання статті є WordPress. Вона проста, нараховує найбільшу спільноту розробників та гнучка.

Об`єкт дослідження – готовий сайт-візитка, націлений на продаж послуги малювання портретів по фото на замовлення. У цій сфері діяльності існує дві потенційні загрози: несанкціонований доступ з метою псування інформації або її викрадення та викрадення фотографій робіт з метою удавання їх за свої [2].

Wordpress має готові плагіни для вирішення обох проблем. Для безпечної аутентифікації та авторизації використовують плагіни, які обмежують кількість неправильних введень пароля, обмежують доступ за IP-адресами, які мають право доступу. У другому випадку дієвими способами є: нанесення водяних знаків (watermark), блокування контекстного меню під час натискання правої кнопки миші та підміна файлу в момент його завантаження.

Метою статті є аналіз рівня безпеки CMS Wordpress та виявлення можливих шляхів її покращення. Крім цього, буде проаналізовано набір готових рішень для захисту авторських прав та можливих способів їх удосконалення.

Основна частина

Дослідження поділимо на дві частини:

1. Проведення заходів щодо виявлення оптимальних способів захисту адміністративної панелі.

2. Аналіз існуючих засобів для захисту зображень на сайті.

3. Розробка скомпільованого програмного модуля для захисту даних в інтернет-магазинах, створених на обраній платформі [4; 5].

Самий головний та водночас простий засіб захисту – складний пароль. Крім цього, необхідно своєчасно оновлювати саму CMS, якщо у старій версії є вразлива ділянка коду, швидше за все у новій версії її усунули. Також необхідно встановити плагін для обмеження кількості невдалих спроб авторизації, який захистить від підбору пароля. Для захисту бази даних простіше всього замінити префікс бази даних у файлі wp_config.php наприклад, на $table_prefix = 'wp4FZ52Y_. Ще хорошою практикою буде створення нового запису адміністратора та видалення старого, тому що запис за умовчуванням має назву ‘admin’ та id=1, що стає передбачуваною мішенню для зловмисника.

Після розбору захисту адміністративної панелі перейдемо до захисту зображень. Перше, що спадає на думку – нанести на зображення водяний знак (Watermark). Є кілька недоліків використання такого

способу: якщо наносити знак на середину зображення, це погіршить сприйняття та загальне враження від сайту. В іншу чергу, якщо наносити знак на куток або край зображення, то зловмисник може його просто відрізати і використовувати у своїх цілях. На щастя є ще декілька способів захисту. Відключення на сайті контекстного меню, яке викликається натисканням правої кнопки миші. Цей спосіб добре працює проти непідготовлених користувачів. Той, хто розуміє як працює сайт, може просто натиснути комбінацію клавіш у браузері, яка покаже вихідний код сайту, у якому можна знайти пряме посилання на зображення і завантажити зображення за допомогою нього. Нажаль повністю захистити зображення від викрадення неможливо, так як при відвідуванні сайту всі переглянуті зображення кешуються на комп'ютері користувача і їх можна дістати з кешу. Тому обов`язково необхідно вказувати, що зображення та тексти на сайті захищені авторським правом. До речі, текст теж можна захистити від копіювання, встановивши пагін, який забороняє виділяти текст.

Час від часу слід перевіряти дубляж матеріалів за допомогою пошукових систем та напряму зв'язуватись з порушниками, у більшості випадків людина погодиться видалити ваш контент [3].

Далі продемонструємо деякі способи у роботі. Плагіни WordPress можна встановити двома способами: через адміністративну панель та через FTP з`єднання.

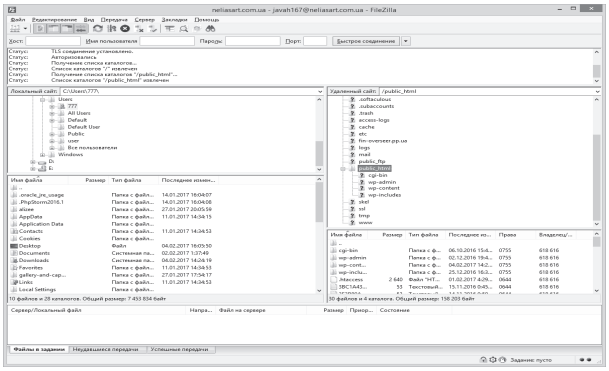


Рис. 1. З`єднання через FTP клієнт

Зручніше, якщо плагін присутній у загальній базі плагінів, встановити через панель. Встановимо WP Content Copy Protection – рис. 2.

Після встановлення цього плагіна одразу вирішуються більшість проблем захисту авторського контенту. Блокується натискання правої кнопки миші, стає неможливим виділення тексту та зображень, блокується перетягування змісту і найголовніше – вихідний код неможливо переглянути стандартними засобами браузера, наприклад комбінаціями Ctrl+Shift+I, Ctrl+U, F12.

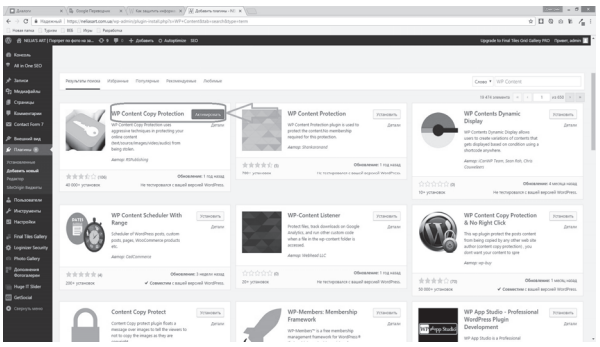


Рис. 2. Встановлення плагіна

Наступним кроком буде встановлення водяних знаків на фотографії. На сайті використовується плагін для галереї під назвою Photo Gallery, у ньому є необхідний засіб [5].

Перш за все підготуємо зображення, яке буде виконувати роль захисного. Це буде логотип з назвою сайту на прозорому фоні. Після цього переходимо до панелі з налаштуваннями (рис. 3).

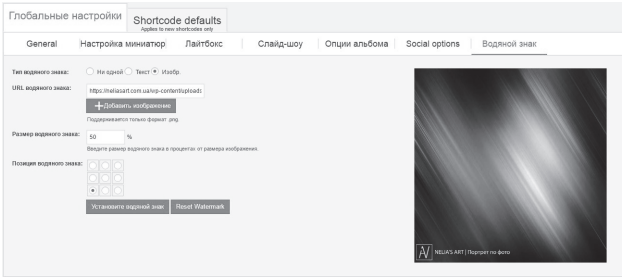


Рис. 3. Панель налаштувань водяного знаку

Із можливих налаштувань нам представлені: можливість вибору типу знаку (текст або зображення), розмір зображення у відсотках відносно його початкового розміру та його розташування. Після збереження налаштувань на кожному зображенні, яке зберігається у Photo Gallery, встановиться водний знак.

Далі, коли з захистом контенту завершено роботу, захистимо адміністративну панель. Пароль нас задовольняє, так як він складається з більш ніж 16 символів та включає в себе цифри, букви у нижньому і верхньому регістрах. По даним KasperskyLab, схожий пароль буде підбиратися 1548 століть звичайним комп'ютером та 17 днів самим найшвидшим комп'ютером у світі (Tianhe-2 Supercomputer). А для того, щоб шансів не було навіть у суперкомп'ютера, встановимо плагін Loginizer. Якщо декілька спроб входу буде хибними, він заблокує IP адресу зловмисника на 20 хвилин.

Далі йде оновлення версії Wordpress та її приховування [5].

Приховувати встановлену версію слід для того, щоб хакер не знав, по якому алгоритму йому діяти.

Зробити це можна додавши до файлу functions.php такий код: remove_action(‘wp_head’, ‘wp_generator’).

Основою захисту всього сайту виступає файл .htaccess, він містить у собі налаштування швидкодії та безпеки.

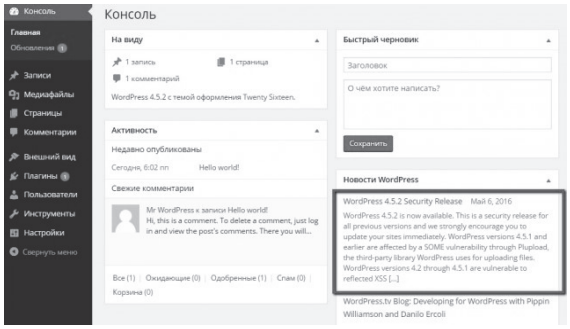
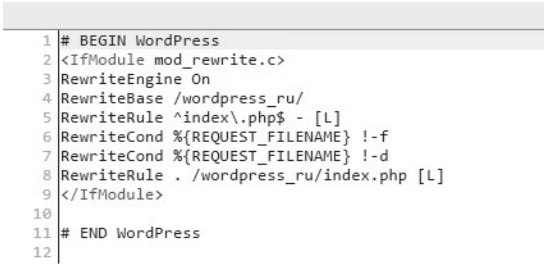


Рис. 4. Інформація про наявність нової версії



```
# BEGIN WordPress
<IfModule mod_rewrite.c>
RewriteEngine On
RewriteBase /wordpress_ru/
RewriteRule ^index\.php$ - [L]
RewriteCond %{REQUEST_FILENAME} !-f
RewriteCond %{REQUEST_FILENAME} !-d
RewriteRule . /wordpress_ru/index.php [L]
</IfModule>

# END WordPress
```

Рис. 5. Стандартний вигляд .htaccess

Додамо деякий код:

```
<Files wp-config.php>
order allow, deny
deny from all
</Files>
```

Цей фрагмент заблокує доступ до файлу wp_config.php, у якому зберігаються дані вашої бази даних.

А цей фрагмент заблокує доступ до самого .htaccess:

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

Якщо ви маєте статичну IP адресу (а це є бажаним), то наступний код заблокує доступ до адміністративної панелі усім крім вас:

```
AuthUserFile /dev/null
AuthGroupFile /dev/null
AuthName «Access Control»
AuthType Basic
order deny, allow
deny from all
allow from X.X.X.X (IP-адреса)
```

Також необхідно мати захист від хотлінкінга (Хотлінкінг – це вставка зображення з вашого сайту на чужий сайт. Трафік при цьому йде на ваш сервер):

```
RewriteEngine On
RewriteCond %{HTTP_REFERER}
!^http://(.+\.)?yourdomain\.com/ [NC]
RewriteCond %{HTTP_REFERER} !^$
RewriteRule .*\.(jpe?g|gif|bmp|png)$
/images/nohotlink.jpg [L]
```

І на кінець код, який захищає від SQL-ін`єкцій (найпоширеніший спосіб атак на сайти Wordpress):

```
RewriteCond %{QUERY_STRING}
(\<|%3C).*script.*(\>|%3E) [NC, OR]
RewriteCond %{QUERY_STRING}
GLOBALS(=|\[|\%[0 — 9A-Z]{0, 2}) [OR]
RewriteCond %{QUERY_STRING}
_REQUEST(=|\[|\%[0 — 9A-Z] {0,2})
RewriteRule ^(.*)$ index.php [F.L]
```

Висновки

В результаті роботи було зроблено наступне:

1. Проведений аналіз вразливостей працюючого реального сайту.

2. Побудований план необхідних заходів захисту за двома напрямками: захист адміністративної панелі та захист авторського контенту від копіювання.

3. Реалізація плану по захисту контенту за допомогою плагіна WP Content Copy Protection та вбудованих можливостей Photo Gallery.

4. Виконання засобів захисту адміністративної панелі як зі сторони форми входу, так і зі сторони атак на файли сервера.

Слід звернути увагу, що повністю бути впевненим у захищеності авторських фотографій і текстів не можна, так як при відкритті сайту, все наповнення кешується на комп’ютері користувача і при достатньому рівні підготовки він зможе дістати файли з кешу. Просто слід іноді засобами пошуку перевіряти чи дублюється ваш контент де інде і зв’язуватись з порушником. Як правило, вони погоджуються усунути порушення.

Що стосується захисту адміністративної панелі – найбільшу увагу слід звернути на конфігурацію файлів wp_config.php, та .htaccess. Зазвичай їх можливостей буде достатньо для того, щоб зупинити середньостатистичного хакера.

Велику увагу варто звернути на захист бази даних. В першу чергу слід змінити основний адміністративний обліковий запис та змінити префікси таблиць, щоб зловмисник не зміг звернутися до таблиць по їх назвам.

Список літератури

1. Орлов Л.В. Как создать электронный магазин в Интернет, 2е изд. / Л.В. Орлов. – М: Бук пресс, 2006. – 384 с.

2. Мельник М.А. Цикл поисковой оптимизации как основа поисковой оптимизации электронных магазинов / М.А. Мельник, А.С. Ганенко // Інфокомунікації – сучасність та майбутнє: матеріали четвертої міжнародної наук.-пр. конф. м. Одеса 30-31 жовт. 2014р. – Ч.4. – Одеса: ОНАЗ, 2014. – С. 116-117.

3. Алексунин В. Электронная коммерция и маркетинг в Интернете / В. Алексунин, В. Родигин. – М: Дашков и Ко, 2009. – 216 с.

4. Мельник М.А. Створення вдосконаленого плагіна захисту інформації для інтернет-магазину на платформі WordPress / М.А. Мельник ,А.Р. Агадженян, Я.Г. Маховська // Інформатика та математичні методи в моделюванні. – 2015. – Т.1, №1. – С. 65-70.

5. [Електронний ресурс]. – Режим доступу до ресурсу: http:// wordpress.org.

Надійшла до редколегії 24.02.2017

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

ОРГАНИЗАЦИЯ ЗАЩИТЫ ИНТЕРНЕТ-РЕСУРСОВ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА И ПРОГРАММНАЯ ЗАЩИТА АВТОРСКИХ ПРАВ

М.А. Мельник, Н.С. Константинова, О.В. Бескупский

В работе была выбрана самая распространённая платформа для создания как персональных сайтов, так и коммерческих – CMS WordPress. Критериями для выбора системы управления содержанием послужили: количество установок, качество технической поддержки и доступность информационных материалов. Были пересмотренные готовые решения для удовлетворения конечных нужд. Проведен анализ недостатков и уязвимостей готовых решений. Разработан план защиты и индивидуальное программное решение с учетом выявленных недостатков.

Ключевые слова: *сайт, расширение, плагин, Word Press, аутентификация, авторизация, водяный знак, система управления содержимым (CMS), IP-адреса.*

ORGANIZATION OF PROTECTION OF INTERNET RESOURCES FROM UNAUTHORIZED ACCESS AND PROGRAM PROTECTION OF COPYRIGHTS

M. Melnyk, N. Konstantynova, O. Beskupskiy

In this work was chosen the most common platform for creating a personal sites, and commercial - CMS WordPress. The criteria for selection of content management systems served as: the number of installations, the quality of technical support and the availability of information materials. Complete solutions has been revised to satisfy the final needs. Analyzed the weaknesses and vulnerabilities of ready solutions. Developed a protection plan and individual software solutions appropriate to identified deficiencies.

Keywords: *site, extension, plugin, plug-in, Word Press, authentication, authorization, watermark, content management system (CMS), IP-adresses.*