УДК 004.056

Кобзев Ігор, Дроботенко Владислав
Ihor.kobziev@hneu.net, Vladyslav.Drobotenko@hneu.net

Харківській національний економічний університет ім. С. Кузнеця, Харків

ЗАСОБИ ЗАХИСТУ ВЕБ-САЙТІВ, СТВОРЕНИХ НА СИСТЕМІ УПРАВЛІННЯ КОНТЕНТОМ WORDPRESS

У сучасних умовах кіберзагроз безпека веб-сайтів є одним із найважливіших аспектів їх розробки та функціонування. Вибір системи управління контентом (CMS) є ключовим етапом у розробці веб-сайту, оскільки від цього залежить його функціональність, зручність використання та безпека. Серед популярних CMS виділяються WordPress, Joomla, Drupal та Magento. Кожна з них має свої особливості, які впливають на безпеку веб-ресурсу.

Порівняльний аналіз основних CMS за критеріями функціональності, зручності використання, безпеки, SEO-оптимізації, розширюваності, швидкості завантаження, ціни та наявності спільноти розробників показує, що WordPress має середній рівень безпеки, тоді як Joomla та Drupal демонструють вищі показники у цьому аспекті. Це обумовлено тим, що WordPress є найпопулярнішою CMS, що робить її привабливою мішенню для зловмисників [1].

Зважаючи на середній рівень безпеки WordPress, важливо впроваджувати додаткові заходи захисту для забезпечення надійної роботи веб-сайту. Це включає регулярне оновлення ядра CMS, плагінів та тем, використання надійних паролів, встановлення плагінів безпеки, таких як Wordfence Security або iThemes Security, а також налаштування брандмауера веб-додатків (WAF) для захисту від різних видів атак [2].

Атаки brute-force (грубої сили) використовують перебір паролів для отримання доступу до адмін-панелі. Окрім унікального логіна та складного пароля, слід використовувати блокування IP-адрес після певної кількості невдалих спроб входу (плагін Limit Login Attempts Reloaded), вмикати автоматичний вихід із системи після періоду бездіяльності (плагін Inactive Logout), використовувати багатофакторну аутентифікацію (2FA) для додаткового рівня безпеки.

Оскільки SQL-атаки можуть дозволити зловмисникам отримати доступ до бази даних, рекомендується використовувати брандмауер веб-додатків (WAF), який відфільтровує шкідливі SQL-запити (плагін Wordfence або Sucuri Security), встановлювати вхідні дані користувачів через механізм перевірки (плагін WP Security Audit Log допоможе відстежувати підозрілі дії), регулярно оновлювати базу даних MySQL і змінити стандартний префікс wp_ на унікальний.

Щоб зменшити ризики атак міжсайтового скриптингу можна використовувати плагін Wordfence для автоматичного блокування шкідливих запитів, обмежити можливість введення HTML та JavaScript у коментарях та формах, додати Content Security Policy (CSP), який забороняє завантаження шкідливого коду.

Щоб мінімізувати вплив розподілених атак відмови в обслуговуванні, можна використовувати CDN-сервіси (Cloudflare, Sucuri) для обробки великого трафіку, також необхідно вимикати XML-RPC (XML-виклик віддалених процедур) і REST API (інтерфейс, що використовується між двома комп'ютерними системами для безпечного обміну інформацією через Інтернет), якщо вони не використовуються, також можна налаштувати автоматичне блокування бот-трафіку через серверні правила або спеціальні плагіни [3].

Додатково слід звернути увагу на захист файлів та каталогів WordPress. Важливо налаштувати правильні права доступу до файлів (наприклад, wp-config.php має бути доступний лише для читання), обмежити виконання PHP-коду в критичних каталогах, за допомогою файлу .htaccess або правил сервера. Крім того, слід налаштувати обмеження доступу до панелі адміністратора через IP-фільтрацію.

Резервне копіювання є ще одним важливим аспектом безпеки. Для цього можна використовувати такі плагіни, як UpdraftPlus або BackupBuddy, які дозволяють створювати автоматичні резервні копії та зберігати їх у хмарних сховищах (Google Drive, Dropbox, Amazon S3). Це дає змогу швидко відновити сайт у разі злому чи втрати даних.

Список літератури

1. Управління контентом на сайті: як вибрати найкращу систему управління контентом (CMS)? SEO-evolution. URL: https://seo-evolution.com.ua/blog/poleznye-sovety/upravlinnya-kontentom-yak-vibrati-naykraschu-sistemu-upravlInnya

2. Як захистити сайт на WordPress? 20+ рекомендацій безпеки. | KR. Laboratories. KR. Laboratories. URL: https://kr-labs.com.ua/blog/wordpress-security-recommendations/

3. 4 типи атаки на сайт WordPress і як їх уникнути: плагіни та поради. Hostenko.com. URL: https://hostenko.com/wpcafe/tutorials/4-rasprostranennyh-ataki-na-wordpress-i-kak-ih-izbezhat/