АНАЛІЗ УРАЗЛИВОСТЕЙ В CMS WORDPRESS ТА ЗАПОБІГАННЯ ЇМ

Бєлов А.О., Панченко В.І.
Національний технічний університет «Харківський політехнічний інститут», м. Харків

CMS Wordpress на сьогодні є найпопулярнішою системою управління контентом, на якій працює більше 30% сайтів в інтернеті. Відповідно, на Wordpress припадає близько 80% хакерських атак в порівнянні з іншими фреймворками. Популярність платформи, а також величезна кількість сайтів, які використовують CMS, створює необхідність вживати превентивні заходи для забезпечення безпеки контенту, розміщеного на сайті.

Найбільш відомі атаки на Wordpress: міжсайтове виконання сценаріїв; SQL ін'єкція; перебір паролів; DoS- і DDoS-атаки.

Найчастіше помилки виникають при написанні коду програмістом або на стороні сервера через невірну конфігурацію. Рідше на клієнтській стороні. Популярність і простота Wordpress приваблює молодих і некваліфікованих фахівців, які не можуть на належному рівні писати, підтримувати, тестувати код. Це веде до появи вразливості в роботі сайту і наступних атак на окремі ділянки коду і скріпти. З клієнтської сторони роблять веб-сайт вразливим такі фактори, як, наприклад, небажання використовувати надійні паролі або безпечний хостинг. Дуже часто саме небажання власника сайту обтяжувати себе додатковими витратами і заперечення того факту, що дрібні або невеликі сайти апріорі не можуть зацікавити зловмисника.

Власники сайтів повинні забезпечити максимальний захист своїх інформаційних цінностей і персональну інформацію своїх клієнтів.

В даній роботі виконується розробка програми, яка тестуватиме обраний веб-сайт на наявність уразливостей і надасть рекомендації щодо їх усунення.

Пропонується виконувати наступні кроки:

1. Перевірка аккаунтів користувачів на рівень їх захищеності, скориставшись базою даних найбільш уразливих паролів, яка є у вільному доступі. Виконується аналіз паролів користувачів та порівняння з найбільш уразливими паролями з бази.
2. Перевірка сайту на наявність небезпечної інформації про версію встановленого Wordpress.
3. Перевірка сайту на наявність небезпечних плагінів та можливих скриптів.

Розроблена програма має вигляд плагіну для CMS Wordpress та може встановлюватися до фреймворка та запускатись при потребі. Також вона має декілька налаштувань, наприклад такі, як можливість сповіщення користувача про знайдені уразливості, відображення рекомендації по їх усуненню тощо. Як розвиток в майбутньому планується додати автоматичний режим для усунення знайдених уразливостей.