УДК 004.056

Томасов Р.О., магістрант,
Бродський Ю.Б., к.т.н., доцент
Державний університет «Житомирська політехніка»

АНАЛІЗ НАЙПОШИРЕНІШИХ ТИПІВ ВРАЗЛИВОСТЕЙ У WORDPRESS

Актуальність дослідження даної теми зумовлена домінуючим положенням Wordpress на ринку. Станом на 2025 рік понад 43% усіх вебсайтів світу працюють на WordPress, що робить платформу найбільш привабливою ціллю для автоматизованих і цілеспрямованих атак [1].

Враховуючи таку популярність даної CMS, важливим є систематизувати типові вразливості, які найчастіше експлуатуються зловмисниками. За даними аналітиків безпеки, понад 96% компрометацій сайтів на WordPress пов'язані з недоліками в сторонніх плагінів і темах, тоді як ядро системи залишається відносно захищеним [2]. Нижче наведено огляд найпоширеніших типів вразливостей, з акцентом на їх механізми роботи та потенційні наслідки [3].

Міжсайтовий скриптинг (Cross-Site Scripting, XSS) залишається одним із найпоширеніших типів вразливостей у WordPress. Він виникає через недостатнє екранування вхідних даних користувачів при виведенні на сторінку, що дозволяє зловмиснику додавати та виконувати довільний JavaScript-код в браузері інших користувачів. Найнебезпечнішим серед цього лишається збережений XSS, коли шкідливий код зберігається в базі даних (наприклад, у коментарях чи контенті) і автоматично запускається для кожного відвідувача або адміністратора сайта.

SQL-ін'єкції, попри наявність захищених механізмів у ядрі WordPress, продовжують зустрічатися у сторонніх плагінах. Вразливість з'являється внаслідок неправильного формування SQL-запитів, зокрема через конкатенацію невідфільтрованих даних користувача. Наслідком успішної атаки може бути повне отримання вмісту бази даних, зміна або повне знищення всіх даних.

Підробка міжсайтових запитів (Cross-Site Request Forgery, CSRF) становить серйозну загрозу для дій, що змінюють стан системи. Вразливість виникає через відсутність або некоректного використання токенів при обробці POST-запитів. Зловмисник таким чином може змусити автентифікованого користувача виконати небажану дію (наприклад, змінити пароль чи видалити певний контент).

Довільне завантаження файлів є поширеною вразливістю в плагінах, що відповідають за імпорт, резервне копіювання або роботу з

файлами. Через недостатню перевірку типу та вмісту завантажених файлів зловмисник отримує можливість розмістити на сервері виконуваний скрипт (веб-шел або бекдор), що забезпечує стійкий доступ до системи жертви для хакера.

Порушення контролю доступу є критичною проблемою в темах та плагінах, де некоректно реалізована перевірка прав користувача. Вона проявляється через дозвіл на виконання адміністративних дій (наприклад, редагування налаштувань чи видалення контенту) для користувачів з низькими привілеями. Потенційні наслідки включають несанкціоноване маніпулювання сайтом, встановлення бекдорів або навіть повне перехоплення контролю.

Ескалація привілеїв часто зустрічається в плагінах для керування користувачами та реєстрації, де вразливість дозволяє неавтентифікованому зловмиснику створювати облікові записи з правами адміністратора. Механізм базується на помилках у функціях обробки реєстрації без належного контролю ролей. Успішна експлуатація вразливості призводить до переходу повного контролю над сайтом в руки зловмисника.

Таким чином проведений аналіз показав, що попри відносну стійкість ядра, безпека WordPress все ще вкрай залежить від якості сторонніх розширень, які лишаються головним вектором атак. Найпоширеніші вразливості, а також недоліки в контролі доступу та обробці завантажень файлів виникають через фундаментальні помилки під час розробки плагінів, що включає некоректну валідацію вхідних даних та недостатнє розмежування прав доступу. Успішна експлуатація цих недоліків може призвести до несанкціонованого виконання зловмисного коду, викрадення даних або повного захоплення контролю над сайтом, що вимагає від власників ресурсів налаштування процесу постійного моніторингу, регулярного оновлення та вибору лише перевірених сторонніх плагінів і тем.

Список використаних джерел:

1. Usage statistics and market share of WordPress. URL: https://w3techs.com/technologies/details/cm-wordpress

2. 2024 Annual WordPress Security Report by Wordfence. URL: https://www.wordfence.com/blog/2025/04/2024-annual-wordpress-security-report-by-wordfence/

3. WordPress vulnerability guide. URL: https://www.liquidweb.com/wordpress/security/vulnerability/