РОЗРОБКА ТЕХНОЛОГІЇ ПІДВИЩЕННЯ РІВНЯ ЗАХИСТУ ІНФОРМАЦІЙНОГО САЙТУ ДЛЯ ДИЗАЙНЕРІВ

***Гордєєв А.С.**, професор, кафедра КСіТ, ХНЕУ ім. С. Кузнеця*
***Єфіменко О.В.**, магістр, кафедра КСіТ, ХНЕУ ім. С. Кузнеця*

Для підвищення рівня захисту сайту на платформі Joomla необхідно приділити належну увагу комплексному аналізу і впровадженню заходів безпеки. Основною метою є забезпечення надійності та захищеності інформації, що зберігається на веб-сайті, а також запобігання можливим атакам та злому. У зв'язку з постійним розвитком технологій і методів злому, заходи безпеки повинні бути постійно оновлюваними та адаптивними до нових загроз.

Одним із перших кроків у підвищенні безпеки сайту на Joomla є оновлення програмного забезпечення до останньої версії. Розробники регулярно випускають нові версії з виправленнями потенційних вразливостей безпеки, тому важливо слідкувати за оновленнями та вчасно їх встановлювати. Додатково до оновлень Joomla, також слід періодично перевіряти оновлення для всіх встановлених розширень і шаблонів, оскільки вони також можуть містити потенційні вразливості.

Для забезпечення додаткового рівня безпеки можна використовувати надійні розширення, ретельно перевірені на вразливості та шкідливий код. При виборі розширень варто керуватися рейтингами, відгуками користувачів та репутацією розробників. Перевірка джерела завантаження, виявлення відкритих джерел ризику, які можуть використовувати атакувальники для проникнення в систему, є також важливим аспектом при виборі розширень для Joomla [1-3].

Представимо технологічну схеми підвищення рівня захисту інформаційного сайту для дизайнерів у вигляді основних етапів на рис. 1.

Ще одним важливим аспектом забезпечення безпеки є встановлення SSL-сертифікату. SSL (Secure Sockets Layer) забезпечує шифрування даних між веб-сервером і веб-браузером, що забезпечує конфіденційність та цілісність переданих даних. Використання SSL-сертифіката дозволяє уникнути простих атак на перехоплення чутливої інформації, такої як паролі чи особисті дані користувачів.

Додатковим заходом захисту є застосування захисту від DDoS атак. DDoS (розподілений деніал-сервіс) – це атака, яка спрямована на збої роботи сервера шляхом перевантаження його великою кількістю запитів. Використання спеціалізованих рішень для виявлення та блокування таких атак допоможе забезпечити безперервну роботу веб-сайту [4-6].

Зміна стандартних ідентифікаторів користувача та пароля адміністратора є необхідним кроком для уникнення простих атак з перебору паролів. Важливо використовувати складні та унікальні паролі, які складаються з комбінації великих і малих літер, цифр та спеціальних символів. Використання двофакторної аутентифікації також додатково підвищить безпеку доступу до адміністративної панелі Joomla, запобігаючи несанкціонованому входу.

Рисунок 1 – Технологічна схема підвищення рівня захисту інформаційного сайту для дизайнерів

Паралельно з цим, варто розглянути можливість використання файрволу, який забезпечить фільтрацію та блокування небажаних запитів на рівні веб-сервера. Файрвол може реагувати на підозрілу або атакуючу активність, що дозволить ефективно захистити сайт від потенційних загроз.

Список літератури

1. Al'boschiy, O., Dorokhov, O., Hrabovskyi, Y., & Naumenko, M. (2022). Automated balancing method of vector illustration and its software implementation. Bulletin of the Transilvania University of Brasov, Series III: Mathematics and Computer Science, 2(1), 177-192.

2. Pushkar, O., Hrabovskyi, Y., & Gordyeyev, A. (2020). Development of a Method for Optimizing the Site Loading Speed. Eastern-European Journal of Enterprise Technologies, 6(2(108)), 21-29. doi: 10.15587/1729-4061.2020.216993.

3. Babenko, V., Hrabovskyi, Y., Ivashura A., & Protasenko, O. (2020). Development of the Methodology for the Choice of Polygraph Equipment for Printing on Cloth. WSEAS Transactions on Environment and Development, (16), 305-315.

4. Hrabovskyi, Y., Kots, H., & Szymczyk, K. (2022). Justification of the innovative strategy of information technology implementation for the implementation of multimedia publishing business projects. Proceedings on Engineering Sciences, 4(4), 467-480. DOI: https://doi.org/10.24874/PES04.04.008

5. Hrabovskyi Ye. (2021). Methods of creating a multimedia online gallery. Збірник наукових праць Харків-го нац-го ун-ту Повітряних Сил, 2(68), 102-107.

6. Hrabovskyi, Y. (2018). Designing the intelligent user interface for electronic education support systems. ScienceRise, (11), 36-39.