РЕАЛІЗАЦІЯ ДВОФАКТОРНОЇ АВТЕНТИФІКАЦІЇ НА ОСНОВІ ФАЙЛУ-КЛЮЧА ДЛЯ СИСТЕМИ КЕРУВАННЯ ВЕБСАЙТАМИ WORDPRESS

Коломійцев С.О., Сєвєрінов О.В., Власов А.В.
Харківський національний університет радіоелектроніки, Харків, Україна

З кожним роком зростає популярність та кількість веб-ресурсів, а тому кількість інформації з якою вони взаємодіють стає все більшою. Також все збільшується кількість систем управління контентом веб-ресурсів.

За даними компанії W3Techs, що займається веденням статистики різних технологій в мережі Інтернет, станом на початок 2023 року, на системі WordPress працює 43% всіх сайтів в інтернеті. Цей відсоток постійно зростає. Найближчий конкурент Shopify має долю лише в 3.8% [1].

Зважаючи на цю популярність, зловмисники приділяють WordPress особливу увагу. Існує безліч програм орієнтованих на злам таких сайтів. Враховуючи відносну простоту реалізації та ефективність, одні з популярних типів атак на дану систему – це атака грубої сили і атака зі словником [2, 3]. Без використання на сайті додаткового програмного забезпечення (плагінів), успішність атак даного типу у більшості випадків залишається питанням часу.

Для системи WordPress реалізовано безліч плагінів, що надають типові методи двофакторної автентифікації [4]. Але вони мають певні недоліки та незручності, найбільші з яких – це необхідність у наявності під рукою мобільного пристрою зі стабільним рівнем сигналу мережі або мобільного інтернету. А також залежність від сторонніх сервісів.

Метою роботи було реалізувати досі не існуючого для WordPress методу двофакторної автентифікації, який зможе поєднати в собі такі властивості як зручність та ефективність.

Розроблений плагін надає власнику вебсайта можливість обрати будь який файл на своєму комп'ютері і перетворити його у персональний ключ, завдяки якому і буде здійснюватись додаткова ідентифікація користувача в системі. В основі лежить використання криптографічних геш-функцій, отримання геш-значення файлу і порівняння його з еталоним геш-значенням що зберігається на сайті.

Список літератури

1. W3Techs statistic URL: https://w3techs.com/technologies/details/cm-wordpress (дата звернення: 31.03.2023).
2. Д'якова Н.Є., Сєвєрінов О.В. Тестування вразливостей сучасних веб-ресурсів, НТУ «ХПІ», 2022.
3. Brute Force Attac URL: https://crashtest-security.com/brute-force-attacks/ (дата звернення: 31.03.2023).
4. Authentication. URL: http://www.webopedia.com/TERM/A/authentication.html (дата звернення: 31.03.2023).