Секція 1

ЗАХИСТ ВЕБ-САЙТУ

Оганян В. Ю.
Національний аерокосмічний університет ім. М. Е. Жуковського
«Харківський авіаційний інститут»
Науковий керівник Пєвнєв В. Я.

Актуальність. Одним з найважливіших завдань при розробці сайтів є їх захист. Адже інтернет є небезпечним місцем, а незахищений сайт може бути легко відключений зловмисниками, через несанкціонований доступ, що призведе до втрати довіри, репутації, часу і грошей людини або компанії, яка володіє тим чи іншим сайтом [1]. У зв'язку з цим захист веб-додатків від різних загроз стає актуальною проблемою.

Метою даної роботи є аналіз існуючих в даний час різних загроз, які можуть викликати некоректну роботу сайту, і розглянути сучасні способи захисту від шкідливого програмного забезпечення.

У доповіді наведені найбільш відомі і поширені засоби захисту, такі як [2,3]:

- Web Application Firewall (WAF);
- засоби захисту від DDoS-атак;
- сканери захищеності веб-додатків (WASS);
- засоби аналізу веб-сайтів на віруси.

Основні положення. Для захисту від втрати даних, SQL-ін'єкцій, отруєння файлами cookie, підбору паролів і використання різних вразливостей в веб-додатках використовується WAF – це файрволл, який сьогодні використовується як універсальний засіб захисту від багатьох видів загроз. Для захисту від DDoS-атак, спрямованих на так званий вид атак на відмову в обслуговуванні, які призводять до відсутності доступу до певного веб-сайту або сервісу на невизначений термін, до декількох тижнів, і, як наслідок, до втрати часу і грошових ресурсів, використовуються різні засоби захисту від DDoS. Захист здійснюється декількома способами: на краю мережі, через локальний центр очищення або шляхом перенаправлення трафіку в хмару. WASS-сканери та інструменти для аналізу сайтів на наявність вірусів, як випливає з назви, сканують сайти на наявність певних вразливостей, помилок, вірусів, сторонніх рекламних та інших шкідливих програм.

У доповіді також наведені існуючи вразливості. До кожного наведеного виду уразливості був розглянутий сценарій можливої атаки

з боку зловмисника. Також були запропоновані методи для розробників, які дозволяють утилізувати дані уразливості та розробити безпечний веб-застосунок [4].

Висновки. Підводячи підсумки, можна побачити, що без засобів захисту зловмисники можуть легко нашкодити сайту. А уникнути цього допоможе спільне використання всіх раніше перерахованих технологій і методів захисту сайтів. Такий підхід, використовуючи різні доступні засоби захисту, забезпечить найвищий і багаторівневий рівень безпеки, і заподіяти будь-яку шкоду буде набагато складніше. І навіть якщо це вдасться, вона не буде такою великою, як могла б бути без цих захистів, що, до того ж, допоможе швидко виявити проблему, якщо вона з'явиться, і усунути її. Тому всі власники різноманітних сайтів і ресурсів повинні ознайомитися з сучасними засобами захисту і використовувати їх.

Список літератури

1. Захист веб-додатків: чому це важливо? *Itbiz*. URL: https://itbiz.ua/ru/stati-i-obzory/ruzashhita-veb-prilozhenij-pochemu-eto-vazhnozaxist-veb-dodatkiv-chomu-ce-vazhlivo/ (дата звернення: 12.11.2021)

2. Hoffman A. Web Application Security : Exploitation and Countermeasures for Modern Web Applications. Sebastopol: O'Reilly Media, Inc, 2020. 450 p.

3. Welling Uk., Thomson L. PHP and MySQL Web Development. Hoboken, New Jersey: Addison-Wesley Professional, 2016. — 688 p.

4. Pevnev V., Popovichenko O., Tsokota Ya. Web application protection technologies Advanced Information Systems. 2020. Vol. 4, No.1. 2020, P. 219-223

Відомості про авторів

Оганян Вячеслав Юрійович, бакалавр кафедри комп'ютерних систем, мереж і кібербезпеки, м.т. 096-313-58-16, v.ohanian@student.csn.khai.edu

Пєвнєв Володимир Яковлевич, доцент кафедри комп'ютерних систем, мереж і кібербезпеки, д.т.н., доцент, v.pevnev@csn.khai.edu