УДК 004.056.53
Я. Рій
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

РОЗРОБКА ПРОГРАМНОГО ПРОДУКТУ ДЛЯ АНАЛІЗУ РІВНЯ ВРАЗЛИВОСТІ САЙТУ ДО XSS-АТАК

UDC 004.056.53
Y. Rii

SOFTWARE PRODUCT DEVELOPMENT FOR ANALYSIS OF THE SITE VULNERABILITY LEVEL TO XSS-ATTACKS

Атаки міжсайтових скриптів (XSS) – це тип ін’єкції, під час якої шкідливі скрипти впроваджуються на безпечні й надійні веб-сайти. Атаки XSS відбуваються, коли зловмисник використовує веб-додаток для надсилання шкідливого коду, як правило, у формі скрипта браузера іншому кінцевому користувачеві. Недоліки, які дозволяють цим атакам досягати успіху, є досить поширеними і виникають у будь-якому місці, де веб-додаток використовує вхідні дані користувача для отримання результатів, не перевіряючи чи не кодуючи їх[1].

Зловмисник може використовувати XSS, щоб надіслати шкідливий скрипт користувачеві. Браузер кінцевого користувача не може дізнатися, що скрипту не можна довіряти, і виконає його. Оскільки він вважає, що сценарій надійшов із надійного джерела, шкідливий сценарій може отримати доступ до будь-яких файлів cookie, маркерів сеансу або іншої конфіденційної інформації, яку зберігає браузер і використовується на цьому сайті[2].

Основною задачею даної наукової роботи є розробка програмного продукту який дозволить визначити рівень вразливості веб-ресурсу до XSS атак на етапі розробки, що дозволить своєчасно запобігти можливим подальшим проблемам в роботі та небажаній втраті даних. Для цього було розроблено нову методику встановлення рівня небезпеки проводячи атаку на сайт використовуючи «безпечні» скрипти, кожен з яких має свій умовний коефіцієнт небезпеки виражений у числовому значені. Результат даної процедури являє собою суму коефіцієнтів усіх успішних атак виражений у числовому значені яку можна зобразити формулою:

$$R=\sum a \times k,$$

де R – числове значення результату; a – успішність проведеної атаки (1 – вдала, 0 – невдала); k – коефіцієнт небезпеки скрипта.

Для реалізації даного програмного продукту було вирішено використовувати мову програмування C# із використанням технології .NET Framework. Також було використано бібліотеки HtmlAgilityPack для визначення елементів веб-ресурсу та системні бібліотеки для створення POST/GET запитів.

Література.

1. Cross Site Scripting (XSS) | OWASP Foundation – [Електронний ресурс] – Режим доступу: https://owasp.org/www-community/attacks/xss/
2. Types of XSS | OWASP Foundation – [Електронний ресурс] – Режим доступу: https://owasp.org/www-community/Types_of_Cross-Site_Scripting