УДК 004.4'277.2.056.55

К. Ю. Василенко
А. О. Азарова

АНАЛІЗ ЗАСОБІВ ВИЯВЛЕННЯ ТА ПОПЕРЕДЖЕННЯ ВРАЗЛИВОСТЕЙ ВІД XSS-АТАК

Вінницький національний технічний університет

Анотація

У дослідженні вивчено програми, що здійснюють пошук XSS-вразливостей, виявлено їх недоліки, що пов'язані з особливостями створення веб-додатків. Це уможливило пропонування авторами більш конструктивного підходу до детектування XSS-вразливостей на основі аналізу повної картки веб-додатка, що дозволяє підвищити ефективність захисту веб-програми від XSS-атак.

Ключові слова: XSS-вразливість, детектування, веб-ресурс, XSS-атака.

Abstract

The study examined programs that search for XSS vulnerabilities, identified their shortcomings related to the peculiarities of creating web applications. This allowed the authors to propose a more constructive approach to detecting XSS vulnerabilities based on the analysis of the full map of the web application, which allows to increase the effectiveness of protecting the web program from XSS attacks.

Keywords: XSS-vulnerability, detection, web resource, XSS-attack.

Вступ

Забезпечення інформаційної безпеки (ІБ) обчислювальних систем є одним із пріоритетних завдань, які вирішуються будь-якою організацією, у господарській діяльності якої застосовуються алгоритми збирання, оброблення, зберігання, передавання інформації. Багато загроз ІБ стали можливими завдяки поширенню мережі Інтернет. При цьому десять років тому більшість веб-застосунків були статичними і не мали інтерактивних інтерфейсів взаємодії з користувачами, а, отже, вразливостей, які були б використані порушниками. Тому багато розробників ігнорували питання безпеки веб-додатків. Однак на сьогоднішній день існує велика кількість динамічних веб-сайтів із безліччю нових технологій, що використовуються у веб-браузерах. Такі технології дозволяють підключати до веб-застосунків різні модулі, що посилюють взаємодію відвідувачів із веб-ресурсом (наприклад, дошки оголошень, форми зворотного зв'язку тощо). Це створює можливість порушникам для проведення комп'ютерних атак типу «SQL-Injection», «XSS» та ін. [1]. За допомогою впровадженого коду порушник може отримати несанкціонований доступ до даних авторизації користувачів і, видаючи себе за них, здійснювати протиправні дії як на локальних комп'ютерах користувачів, так і в мережевому устаткуванні компанії, змінюючи конфігурацію мережі та програмного забезпечення. Відсутність належних заходів щодо дотримання правил та норм інформаційної безпеки призводить до появи загроз, які можна реалізувати за допомогою комп'ютерних атак, що експлуатують уразливості, пов'язані з використанням шкідливого коду. Одним із таких видів комп'ютерних атак є міжсайтовий скриптинг – XSS [2].

Більшість програм, які здійснюють пошук XSS-вразливостей, мають низку недоліків, що пов'язані з особливостями створення веб-додатків. Існуючі програми детектування XSS-вразливостей здійснюють пошук лише у відкритій частині веб-ресурсу, разом із тим, вразливість може бути в закритій частині веб-ресурсу, яка доступна авторизованим користувачам. Це негативно позначається на рівні захищеності веб-ресурсу, отже, задачею дослідження, проведеного авторами, є розроблення програмного забезпечення, що здійснює пошук XSS-уразливостей на основі аналізу повної картки веб-додатка, що уможливилює підвищення ефективності захисту веб-програми від XSS-атак.

Результати дослідження

Для створення авторами дослідження системи виявлення XSS-атак, що відповідає найновішим вимогам, було розроблено структурну схему роботи аналітичного модуля з виявлення найрізноманітніших вразливостей та їх коригування, що подано на рис. 1.

Рисунок 1. Структурна схема аналітичного модуля XSS-атак

Отже, автори дослідження пропонують такий алгоритм дій щодо виявлення вразливостей під час сканування сайтів.

Крок 1. Якщо мережевий сервіс використовує опублікований протокол (наприклад, встановлений RFC (Requests for Comments) – серія документів IETF під назвою «Запити на коментарі», розпочата в 1969 р., містить опис набору протоколів Інтернет та пов'язану з ними інформацію), то обов'язково необхідно переглянути протокол і знайти опис областей зберігання рядків змінної довжини та масивів даних, оскільки вони можуть бути вразливими до атак переповнення буфера.

Крок 2. Необхідно визначити специфікації протоколу: рядок не повинен бути більшим за встановлену довжину.

Крок 3. Слід встановити зв'язок із мережею, що тестується, і надіслати їй великий масив випадкових даних.

Крок 4. Необхідно встановити зв'язок із мережею, що тестується, і, не надсилаючи жодних даних, дізнатися, скільки часу знадобиться для того, щоб мережева служба видала повідомлення про розрив з'єднання і завершила сеанс.

Висновки

Розроблений алгоритм та його програмна реалізація дозволяють підвищити ефективність захисту веб-додатка від XSS-атак, значно спрощують процес тестування веб-ресурсу розробником завдяки функціоналу формування звіту з рекомендаціями щодо усунення знайдених XSS-вразливостей.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Types of XSS: Stored XSS, Reflected XSS and DOM-based XSS. Acunetix Blog, 17 January 2018. URL : https://www.acunetix.com/websitesecurity/xss/ (Дата звернення 23.04.2022 р.).

2. XSpider. Positive Technologies, 12 May 2013. URL: https://www.ptsecurity.com/ru-ru/products/xspider/ (Дата звернення 23.04.2022 р.).

Василенко Кристина Юріївна – студентка групи КІТС-18Б Факультету менеджменту та інформаційної безпеки, Вінницький національний технічний університет, м. Вінниця, tina.vasylenko@gmail.com

Vasylenko Krystyna Yuriyivna student of KITS-18B group of the Management and Information Security Faculty, Vinnytsia National Technical University, Vinnytsia, tina.vasylenko@gmail.com.

Азарова Анжеліка Олексіївна – к.т.н., професор кафедри МБІС Вінницького національного технічного університету, м. Вінниця, azarova.angelika@gmail.com.

Azarova Anzhelika O. – PhD in technique, Professor of Management and security information systems department of Vinnytsia National Technical University, Vinnytsia, azarova.angelika@gmail.com.