УДК 004.45
О.Р. Оробчук, доктор філософії, Р. В. Гарматій
Тернопільський національний технічний університет імені Івана Пулюя

АКТУАЛЬНІСТЬ ІНФОРМАЦІЙНИХ СИСТЕМ ДЛЯ АВТОМАТИЗОВАНОГО ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ У ВЕБДОДАТКАХ

O.R. Orobchuk, Dr, R. V. Harmatii

INFORMATION SYSTEM FOR AUTOMATED VULNORABILITY DETECTION IN WEB APPLICATION

Дослідження та впровадження автоматизованих систем виявлення вразливостей у веб-додатках наразі є критично важливими у сфері інформаційної безпеки. Веб-технології, які є основними компонентами сучасних інформаційних систем, знаходять широке застосування в різних секторах, у тому числі в тих, які мають велике значення щодо інформаційної безпеки[1]. І навпаки, базові атаки на ці системи не обов'язково вимагають від зловмисників високого технічного досвіду, оскільки інформація про типові вразливості та методи атак широко поширюється в загальнодоступних джерелах.

Важливість цього дослідження підкреслюється різноманітністю веб-додатків, які задовольняють різні функціональні потреби в таких сферах, як фінанси, охорона здоров'я, зв'язок тощо[1]. Поширення таких додатків сприяє збільшенню потенційної вразливості та ризиків для інформаційної безпеки, що вимагає систематичного та ефективного підходу до виявлення потенційних недоліків.

Вищезазначені обставини підкреслюють актуальність впровадження автоматизованих систем виявлення вразливостей у веб-додатках. Ці системи відіграють ключову роль у запобіганні потенційним атакам і усуненні вразливостей, перш ніж їх можна буде використати для компрометації інформації.

У цьому контексті необхідність постійного моніторингу та вдосконалення систем виявлення стає невід'ємною частиною стратегії кібербезпеки. Розробка та впровадження передових технологій у цій галузі сприяє не лише покращенню захисту веб-додатків від потенційних загроз, але й зміцненню довіри користувачів до цих систем. Такий підхід дозволяє активно адаптуватися до змін загроз, забезпечуючи постійну безпеку в цифровому ландшафті, що швидко розвивається.

Автоматизовані системи виявлення вразливостей не лише вирішують безпосередні проблеми безпеки веб-додатків, але й сприяють досягненню головної мети сприяння культурі проактивної безпеки. Постійно скануючи вразливі місця, організації можуть зміцнити свій захист від нових загроз і адаптуватися до нових тактик, які використовують зловмисники[2].

Тонкощі цих додатків, які часто взаємопов'язані з різними базами даних і зовнішніми інтерфейсами, створюють складні проблеми для забезпечення надійної безпеки. Оскільки організації все більше покладаються на веб-платформи для критично важливих операцій, потенційні наслідки порушень безпеки мають далекосяжні наслідки, включаючи фінансові втрати, шкоду репутації та правові наслідки.

Література

1. Bandr Siraj Fakiha. 2020. Effectiveness of Security Incident Event Management (SIEM) System for Cyber Security Situation Awareness. International Journal of Forensic Medical and Toxicological Sciences. [online] Available at: https://medicopublication.com/index.php/ijfmt/article/view/11587/10679

2. Safe Exam Browser. https://safeexambrowser.org/about_overview_en.html