АНАЛІЗ РІВНЯ БЕЗПЕКИ WEB-РЕСУРСІВ

Сєвєрінов О.В., Баклан Я.А.
Харківський національний університет радіоелектроніки, Харків, Україна

В роботі розглянуті методи оцінки рівня безпеки web-ресурсів.

Аналіз показав, що основні області, де сайт може бути вразливим: системне адміністрування, програмна частина та серверна частина [1].

Найбільш поширені атаки на веб-ресурси [2]: 1) отримання доступу до бази даних за допомогою впровадження SQL-коду (SQL Injection). У своїй найбільш поширеній формі дана атака дає доступ до конфіденційної інформації. Спосіб захисту – ретельно обробляти вхідні параметри, значення яких використовуються для побудови SQL-запиту. 2) Міжсайтовий скриптинг. XSS (Cross Site Scripting) – тип атаки, при якій зловмисник впроваджує шкідливі скрипти у форми введення. Найчастіше при даній атаки відбувається крадіжка Cookies, де деякі сайти зберігають логіни і паролі (частіше їх геш коди) користувачів, і відповідно зловмисник може отримати доступ до вашого аккаунту. Захист від даних атак – валідація вхідних параметрів, тобто перевірка змінних, щоб вони містили коректний введення.

Метою дослідження є аналіз поточний стан безпеки web-ресурсів. У разі низького рівня захищеності Web-застосунків можлива реалізація загрози з боку зовнішнього порушника, наслідком цього може стати необхідність виділення додаткового бюджету на роботи з мінімізації ризиків [3].

Мета аналізу захищеності web-ресурсів полягає в підвищенні рівня безпеки програми в умовах обмеженого бюджету. Для цього найкраще організувати процес аналізу ресурсу методом «сірого ящика» з використанням інструментального підходу до його обстеження з частковими перевірками, виконаними вручну.

За підсумком роботи, можна зробити висновок, що загальний рівень захищеності веб- застосунків недостатньо високий. Для підвищення рівня безпеки слід проводити аналіз, виходячи з області дослідження. Так, якщо мета аналізу полягає в демонстрації можливості проникнення, порушення штатного режиму роботи програми або демонстрації компрометації чутливої інформації, тоді аналіз варто організувати за принципом «чорного ящика» без обмежень по проведеним перевіркам.

Список літератури

1. Web Application Security Statistics [Електронний ресурс] – Режим доступу до ресурсу: http://projects.webappsec.org/f/wasc-wafec-v1.0.pdf.

2. Сєвєрінов О.В., Хрєнов А.Г., Поляков А.О. Аналіз сучасних методів атак на автоматизовані системи управління військами та інформаційні мережі //Системи обробки інформації. – 2015. – №. 9. – С. 101-104.

3. Lysakov V., Sievierinov O., Taran I. Security of Web Applications Using AWS Cloud Provider //COMPUTER AND INFORMATION SYSTEMS AND TECHNOLOGIES. – 2021.