

ПОРІВНЯЛЬНИЙ АНАЛІЗ OWASP TOP 10 І CWE TOP 25

Вінницький національний технічний університет;

Анотація

У роботі здійснено порівняльний аналіз двох основних стандартів, що використовуються для забезпечення безпеки програмного забезпечення: OWASP Top 10 та CWE Top 25. Визначено особливості кожного з цих стандартів та встановлено кореляцію між ними. Представлено відображення вразливостей в цих переліках, що дало можливість виявити розбіжності в них.

Ключові слова: кібербезпека, вразливості, OWASP Top 10, CWE Top 25, веб-застосунки, програмне забезпечення, загрози, аналіз.

Abstract

The work provides a comparative analysis of two main standards used to ensure software security: OWASP Top 10 and CWE Top 25. The peculiarities of both these standards are defined and the correlation between them is determined.. A mapping of the vulnerabilities in these lists is presented, which makes it possible to identify discrepancies in them.

Keywords: cybersecurity, vulnerabilities, OWASP Top 10, CWE Top 25, web applications, software, threats, analysis.

Вступ

У сучасному світі програмне забезпечення є основою багатьох технологій, що впливають на всі аспекти повсякденного життя, від онлайн-платформ до критичних інфраструктур. Зі зростанням кількості кіберзагроз з'являється потреба у розробці стандартів і рекомендацій, що сприяють забезпеченню безпеки програмних продуктів. Одними з найбільш відомих і широко використовуваних підходів є OWASP Top 10 [1] та CWE Top 25 [2].

OWASP Top 10 це документ, який надає список десяти найбільш поширених і критичних вразливостей веб-застосунків, що є важливим довідником для розробників і фахівців із безпеки. CWE Top 25, у свою чергу, охоплює найбільш небезпечні програмні помилки, які можуть призвести до серйозних вразливостей у програмному забезпеченні загалом.

Метою даного дослідження є збільшення стійкості веб-застосунків шляхом підвищення їх стійкості до критичних вразливостей на основі порівняння OWASP Top 10 та CWE Top 25. Оскільки обидва стандарти є важливими для створення безпечних програмних продуктів, розуміння їхніх особливостей та відмінностей дозволяє будувати більш ефективні стратегії безпеки та мінімізації ризиків.

Результати дослідження

OWASP Top 10 – це перелік найбільш критичних вразливостей веб-застосунків. Даний стандарт є основним довідником для розробників і фахівців з безпеки, надаючи їм список найпоширеніших і найбільш небезпечних загроз. OWASP Top 10 охоплює такі типи вразливостей, як порушення контролю доступу, криптографічні помилки, ін'єкції, неправильна обробка аутентифікації, а також проблеми з налаштуваннями і компонентами [1]. Він є важливим довідником для розробників веб-застосунків, оскільки дозволяє їм зосередити увагу на найбільш критичних аспектах безпеки, що допомагає створювати програмні продукти з високим рівнем захисту.

CWE Top 25 – це перелік найнебезпечніших програмних помилок, що можуть призвести до серйозних вразливостей у програмному забезпеченні. CWE Top 25 надає загальний опис помилок, які можуть виникнути на різних етапах розробки програмного продукту, від введення даних до обробки пам'яті [2]. Він охоплює більше технічних аспектів програмування, включаючи переповнення буфера, некоректне використання пам'яті, а також вразливості, пов'язані з неправильною обробкою даних. Даний каталог є універсальним і застосовується до всіх типів програмних систем, а не лише до веб-застосунків.

У таблиці 1 представлено результати порівняльного аналізу OWASP Top 10 і CWE Top 25.

Таблиця 1 – Порівняння OWASP Top 10 і CWE Top 25

OWASP TOP 10	CWE TOP 25
A01:2021-Broken Access Control	CWE-352 Cross-Site Request Forgery (CSRF)
	CWE-22 Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
	CWE-200 Exposure of Sensitive Information to an Unauthorized Actor
A02:2021-Cryptographic Failures	-
A03:2021-Injection	CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
	CWE-89 Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
	CWE-78 Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
	CWE-94 Improper Control of Generation of Code ('Code Injection')
	CWE-20 Improper Input Validation
	CWE-77 Improper Neutralization of Special Elements used in a Command ('Command Injection')
A04:2021-Insecure Design	CWE-434 Unrestricted Upload of File with Dangerous Type
A05:2021-Security Misconfiguration	CWE-863 Incorrect Authorization
	CWE-862 Missing Authorization
A06:2021-Vulnerable and Outdated Components	CWE-190 Integer Overflow or Wraparound
A07:2021-Identification and Authentication Failures	CWE-287 Improper Authentication
	CWE-269 Improper Privilege Management
	CWE-798 Use of Hard-coded Credentials
	CWE-306 Missing Authentication for Critical Function
A08:2021-Software and Data Integrity Failures	CWE-502 Deserialization of Untrusted Data
A09:2021-Security Logging and Monitoring Failures	-
A10:2021-Server-Side Request Forgery	CWE-918 Server-Side Request Forgery (SSRF)

Продовження таблиці 1

OWASP TOP 10	CWE TOP 25
Інші	CWE-787 Out-of-bounds Write
	CWE-125 Out-of-bounds Read
	CWE-416 Use After Free
	CWE-119 Improper Restriction of Operations within the Bounds of a Memory Buffer
	CWE-476 NULL Pointer Dereference
	CWE-400 Uncontrolled Resource Consumption

З таблиці 1 видно, що стандарти орієнтовані на виявлення та класифікацію вразливостей, проте вони мають різні цілі та області застосування.

CWE Top 25 не розглядає криптографічні вразливості, питання журналювання та моніторингу безпеки, оскільки його мета – ідентифікація найбільш небезпечних програмних помилок, що можуть спричинити критичні вразливості у будь-якому типі програмного забезпечення. Натомість OWASP Top 10 фокусується саме на веб-застосунках та містить категорії, які охоплюють специфічні аспекти безпеки веб-систем, зокрема криптографічні помилки та проблеми контролю доступу. Це пояснюється різницею в методології: OWASP базується на аналізі реальних атак і вразливостей у веб застосунках, тоді як CWE формує перелік на основі глибокого технічного аналізу загроз програмної безпеки.

Висновки

OWASP Top 10 і CWE Top 25 є важливими стандартами для підвищення безпеки програмного забезпечення, проте вони мають різні підходи та сфери застосування. OWASP Top 10 орієнтований на веб-застосунки та відображає найбільш поширені вразливості на основі реальних атак. Натомість CWE Top 25 охоплює найнебезпечніші програмні помилки, незалежно від типу програмного забезпечення, ґрунтуючись на технічному аналізі. Як показало виконане дослідження сфокусованість або ж навпаки – занадто узагальнений фокус – відомих найкращих практик безпеки програмного забезпечення ускладнюють їх застосування для конкретних засобів. Це може бути або відсутність врахування певних аспектів у випадку спеціалізації найкращих практик, або потребі у витрачанні ресурсів на аналіз нерелевантних вразливостей. Відповідно актуальним для подальших досліджень є розроблення низки спеціалізованих баз вразливостей, які враховують особливості конкретного виду програмних засобів.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. CWE List Version 4.16. Mode of access: <https://cwe.mitre.org/data/index.html> (accessed: 19.03.2025).
2. OWASP Top Ten:2021. Mode of access: <https://owasp.org/Top10/> (accessed: 19.03.2025).

Баришев Юрій Володимирович — к. т. н., доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця, email: yuriy.baryshev@vntu.edu.ua.

Кравчук Іван Юрійович — студент групи ІБС-24м, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, email: mailosng@gmail.com

Yurii Baryshev — PhD (eng), associated professor of information protection department, Vinnytsia National Technical University, Vinnytsia, email: yuriy.baryshev@vntu.edu.ua

Ivan Kravchuk — student of ІБС-24м group, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, email: mailosng@gmail.com