УДК 004.056.5

Ю. В. Баришев
В. О. Демченко

АНАЛІЗ ДИНАМКИ ЗМІН В РЕЙТИНГУ OWASP TOP 10

Вінницький національний технічний університет

Анотація

У цій роботі досліджується еволюція вразливостей вебзастосунків відповідно до стандарту OWASP top 10 (2017, 2021 та 2025 роки). Проаналізовано динаміку змін між цими періодами. Представлено графік, який дозволяє наочно спостерігати зміщення трендів щодо зміни пріоритетності певних вразливостей.

Ключові слова: кібербезпека, аналіз вразливостей, OWASP top 10, стандарт, загрози, аналіз, веб-застосунки.

Abstract

This work examines evolution web application vulnerabilities according to the OWASP top 10 standard (2017, 2021 and 2025). Changes dynamics was analyzed between these periods. A graph is presented that allows you to visually observe the displacement focus of vulnerabilities priority changes trends .

Key words: cybersecurity, vulnerabilities analysis, OWASP top 10, standards, threats, analysis, web applications.

Вступ

У сучасному цифровому світі вебзастосунки є критично важливою частиною повсякденного життя, які потребують захисту весь час. Адже варто пам’ятати, що у кіберпросторі відбувається розвиток не лише технологій, а й різних атак та загроз, які можуть не просто зашкодити певному продукту, а і його користувачам. Тому виникає потреба у розробці різних стандартів, які будуть забезпечувати безпеку застосунків. Найвідомішим стандартом для вебзастосунків вважають OWASP top 10 [1-3], які разом з рейтингом CWE top 25 [4], є основними маркерами на які варто звертати увагу в першу чергу під час аналізу вразливостей.

OWASP top 10 є документом, який описує список з найвідомішими та найкритичнішими загрозами для вебзастосунків та зазначає, як запобігти їм. Саме цей стандарт є інструментом, який полегшують роботу розробників, тестувальників та фахівців з безпеки під час аналізу. Оскільки за допомогою нього вони розуміють, на які аспекти першочергово потрібно зосередити свою увагу під час розроблення та/або тестування вебзастосунку, щоб забезпечити йому захист від найбільш актуальних загроз. Також він дозволяє раціонально розподілити часові та технічні ресурси, зосередивши всі зусилля на усунення найбільш критичних вразливостей.

Метою даного дослідження є покращення обізнаності щодо безпеки вебзастосунків шляхом аналізу змін у рейтингах OWASP top 10 та візуалізація динаміків зміни актуальності загроз.

Результати дослідження

Результати порівняльного аналізу, наведені в роботі [5], показали, з одного боку, фокус великих досліджень, покликаних визначити загальні тенденції в розвитку загроз, складно імплементувати для конкретних рішень внаслідок узагальненості цих досліджень. Водночас на етапах техніко-економічного обґрунтування та системного аналізу життєвого циклу розроблення програм важливо мати орієнтир щодо ландшафту кіберзагроз та їх трендів зміни. У випадку розроблення вебзастосунків таким орієнтиром постає рейтинг OWASP top 10. Однак він показує актуальний стан загроз на момент його оприлюднення. Відповідно ці рейтинги, попри те, що останній перегляд відбувся порівняно нещодавно, набувають додаткової цінності, якщо розглядати динаміку змін.

На основі проведеного порівняння рейтингів OWASP top 10 за 2017 [1], 2021 [2] та 2025 [3] роки побудовано графік, який відображає динаміку зміни загроз для вебзастосунків (рис. 1).

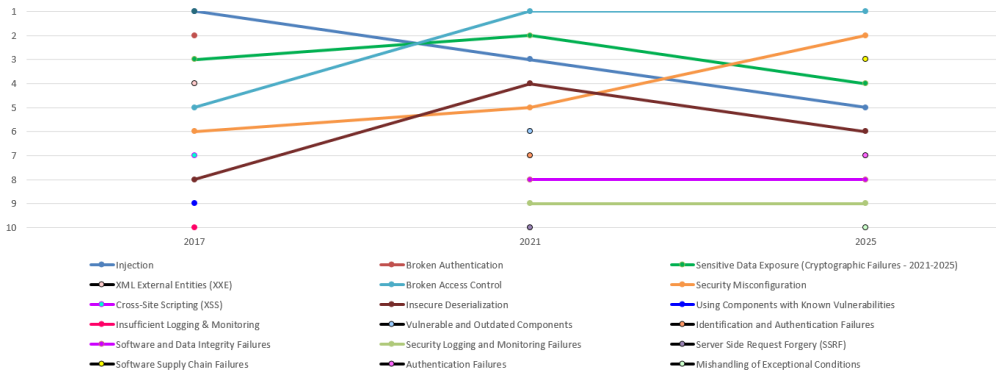

Рисунок 1 – OWASP top 10 за 2017-2025 роки

Аналізуючи графік, наведений на рис. 1 можна одразу помітити, що перелік загроз не є стабільним, оскільки методи атак розвиваються разом із технологіями. Також можна спостерігати, що з кожною новою версією стандарту перелік категорій зазнає суттєвих змін, зокрема неактуальні кіберзагрози вилучаються і з'являються нові. Окрім цього варто розуміти, що більшість загроз не зникають безслідно, а просто змінюють свою назву чи об'єднуються у більш ширші групи. Наприклад, у версіях 2021 та 2025 років вразливість Sensitive Data Exposure отримала назву – Cryptographic Failures.

Відповідно до цього протягом певних періодів спостерігається значне зміщення фокусу безпеки. Зазвичай підвищення пріоритету вказує на зростання актуальності певної вразливості, яке може зумовити збільшенням кількості інцидентів. А зниження пріоритетів свідчить про те, що зменшилася кількість випадків цих атак через те, що фахівці знайшли методи усунення цих вразливостей, але в будь-якому випадку не варто забувати про ці загрози.

Але при цьому найбільш показовим результатом є позиція категорії порушення контролю доступу, яка у 2021 році очолила першу позицію, піднявшись з п'ятого місця. Це сталося через те, що 94% всіх протестованих застосунків мали певні порушення саме контролю доступу, при цьому було зафіксовано понад 318 тисяч випадків цієї вразливості [2]. За версією 2025 року ситуація стала ще критичнішою, оскільки дана категорія так і зберегла першу позицію та 100% протестованих програм виявили ознаки порушення контролю доступу [3]. Це свідчить про те, що на сьогоднішній день зловмисники зменшили кількість спроб «зламати» код за допомогою ін'єкцій (які були топ-1 за версією 2017 року), а використовують прорахунки в логіці авторизації, щоб отримувати конфіденційну інформацію під видом легальних користувачів.

Важливо відзначити появу загроз ланцюгам постачання програмного забезпечення. При цьому, якщо ця загроза не потрапляла раніше в ці рейтинги. В останній версії ця загроза з'явилась одразу на третьому місці. Це можна пояснити і значним розвитком технологій DevOps та інструментів для автоматизації процесів CI/CD, які разом з покращенням швидкості виконання та меншої кількості витрат часу людьми вносять і додаткову площу вразливостей в загальний ландшафт загроз.

Висновки

Дана робота підтверджує, що кіберзагрози весь час розвиваються та адаптуються до нових технологій та методів захисту. Тому важливою складовою для захисту застосунків є регулярний перегляд та оновлення стандартів безпеки. Адже саме вони допомагають мінімізувати ризики та запобігти фінансовим та репутаційних втратах у майбутньому. А безпосередній аналіз та моніторинг самих змін загроз дозволяє простіше та ефективніше будувати системи, які зможуть з легкістю протистояти сучасним загрозам.

Аналогічно до появи загроз ланцюгам постачання в рейтингові 2025 року, варто очікувати в наступному рейтингу появу загроз, пов'язаних із застосування інструментів штучного інтелекту в процесі розроблення та тестування вебзастосунків.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. OWASP Top Ten 2017. *OWASP*. URL: https://owasp.org/www-project-top-ten/2017/ (last accessed: 15.03.2026).
2. OWASP Top 10:2021. *OWASP*. URL: https://owasp.org/Top10/2021/ (last accessed: 15.03.2026).
3. OWASP Top 10:2025. *OWASP*. URL: https://owasp.org/Top10/2025/ (last accessed: 15.03.2026).
4. CWE List Version 4.19.1. Common Weakness Enumeration URL: https://cwe.mitre.org/data/index.html (last accessed: 15.03.2026)
5. Баришев Ю. В., Кравчук І. Ю. Порівняльний аналіз OWASP Top 10 s CWE Top 25. LIV Всеукраїнська науково-технічна конференція факультету інформаційних технологій та комп'ютерної інженерії. Вінниця, 2025. 3 с. URL: https://conferences.vntu.edu.ua/index.php/all-fitki/all-fitki-2025/paper/view/23890/19805 (дата звернення: 15.03.2026).

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

Демченко Вероніка Олександрівна – студентка групи 1БКС-23Б, кафедри захисту інформації факультету інформаційних технологій комп’ютерної інженерії, Вінницький національний технічний університет, м. Вінниця, email: vdemchenkoo.ol@gmail.com

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

Veronika Demchenko – student of group 1BKS-23B, Department of Information Security, Faculty of Information Technology and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, email: vdemchenkoo.ol@gmail.com