УДК 004.056.53

Богданова Вероніка Валеріївна

студентка 4 курсу Харківського національного університету радіоелектроники

Олешко Інна Вікторівна,

к.т.н., доцент, доцент кафедри безпеки інформаційних технологій Харківського національного університету радіоелектроники

ПОРІВНЯЛЬНИЙ АНАЛІЗ ВРАЗЛИВОСТЕЙ ВЕБЗАСТОСУНКІВ НА ОСНОВІ ДОКУМЕНТІВ OWASP

Анотація. Розглянуто основні класи вразливостей вебзастосунків за класифікацією OWASP Top 10 редакцій 2021 та 2025 років. Виконано порівняльний аналіз зміни рейтингу категорій ризиків і виявлено тенденцію зміщення уваги від окремих помилок у коді до системних недоліків проєктування, конфігурації та ланцюга постачання програмного забезпечення. Запропоновано методи виявлення для різних типів вразливостей. Зроблено припущення щодо актуальності та ранжування вразливостей вебдодатків в наступній редакції OWASP Top 10. Результати можуть бути використані під час планування тестування на проникнення та вибору заходів захисту вебзастосунків.

Ключові слова: вебзастосунок, вразливість, OWASP Top 10, контроль доступу, ін’єкції, ланцюг постачання, кіберстійкість.

Постановка проблеми. На сьогодні вебзастосунки є одним із головних засобів надання цифрових послуг, тому їхній рівень захисту має суттєве значення для кібербезпеки організацій. З розвитком технологій розроблення змінюються й основні загрози для таких систем. Передусім, використання мікросервісної архітектури, хмарних середовищ, API та сторонніх програмних компонентів створює загрози й може призводити до появи нових вразливостей. З цієї причини важливо досліджувати та

порівнювати основні види вразливостей вебзастосунків, щоб визначити найбільш критичні з них і визначити пріоритетні напрями захисту.

Мета роботи. Порівняти вразливості вебзастосунків за класифікацією OWASP Top 10 редакцій 2021 та 2025 років і визначити тенденції їх змін.

Класифікація OWASP Top 10 є документом підвищення обізнаності, який систематизує найкритичніші ризики безпеки вебзастосунків [1]. У версії 2025 року використані дані про понад 175 тисяч записів CVE, які зіставлено зі слабкостями CWE та згруповано в десять категорій [1]. З метою порівняння цих категорій враховано три основні ознаки: їхнє місце в рейтингу, фактори виникнення вразливостей (помилки під час реалізації, недоліки проєктування або проблеми з конфігурацією і використанням системи), а також можливість автоматичного знаходження таких вразливостей. Порівняння двох редакцій наведено в табл. 1.

Таблиця 1 – Порівняння категорій OWASP Top 10 у редакціях 2021 та 2025 років

Категорія	**2021**	**2025**	**Зміна**
Broken Access Control	A01	A01	Лідер; поглинула SSRF
Security Misconfiguration	A05	A02	Зростання
Software Supply Chain Failures	A06*	A03	Розширення категорії
Cryptographic Failures	A02	A04	Зниження
Injection	A03	A05	Зниження
Insecure Design	A04	A06	Зниження
Authentication Failures	A07	A07	Без змін
Software or Data Integrity Failures	A08	A08	Без змін

Категорія	2021	2025	Зміна
Security Logging and Alerting Failures	A09	A09	Без змін
Mishandling of Exceptional Conditions	–	A10	Нова категорія
Server-Side Request Forgery (SSRF)	A10	у складі A01	Об’єднано

* A06:2021 – Vulnerable and Outdated Components.

З таблиці 1 бачимо, що лідером серед вразливостей є Broken Access Control, тобто порушення контролю доступу. За даними OWASP за 2021 рік, ту чи іншу форму цієї вразливості знайшли у 94 % перевірених застосунків [2]. У рейтингу 2025 року до цієї категорії додали ще й SSRF, яка раніше була окремою категорією[1]. В обох випадках є спільна риса: сервер не перевіряє, чи має користувач право виконувати запит. API стає все більше, тож з’являється більше місць, де можна помилитися з авторизацією. Це видно й за списком OWASP API Security Top 10, де на першому місці стоїть порушення авторизації на рівні об’єктів [3, 4]. Саме тому правильний розподіл прав доступу лишається одним із головних завдань при захисті вебзастосунків.

Вразливість Security Misconfiguration піднялася з п’ятого місця на друге в новій редакції. Пояснюється це тим, що зміни в середовищах випускають частіше, ніж їх встигають перевіряти, а у хмарних сервісах багато параметрів, які легко налаштувати неправильно [4]. Категорію Vulnerable and Outdated Components замінила ширша Software Supply Chain Failures, яка охоплює залежності, а також збирання й доставку програмного забезпечення [1]. Такі вразливості важко знайти автоматичними сканерами, тому в даних про них мало записів. Цю категорію до списку внесли насамперед за результатами опитування фахівців [1, 4]. Яскравими

прикладами є компрометація оновлення SolarWinds та шкідливий код у сторонніх скриптах [4]. Отже, зловмисники все частіше атакують не сам код застосунку, а середовище, де його створюють і запускають.

В OWASP Top 10 2025 Injection опустилася з третього місця на п’яте. Це пов’язано з тим, що інструменти тестування краще перевіряють саме такі вразливості, а не з тим, що зловмисники втратили інтерес до них [4]. Можливо, також допомагають фреймворки із вбудованим захистом, але це припущення потребує перевірки. Нова категорія Mishandling of Exceptional Conditions включає 24 слабкості CWE: неправильну обробку помилок, логічні помилки та випадки, коли система при збої переходить у небезпечний стан [1]. Простий приклад – повідомлення про помилку, яке показує службову інформацію. Варто також пам’ятати, що, за словами самого OWASP, рейтинг ґрунтується на раніше отриманих даних, тому нові ризики в ньому можуть бути враховані не повністю [1].

Для виявлення кожного типу вразливостей доцільно застосовувати різні підходи. Помилки реалізації можна знаходити за допомогою статичного та динамічного аналізу коду. Для виявлення недоліків проектування важливими є моделювання загроз і ручне тестування логіки роботи застосунку. Натомість експлуатаційні недоліки потребують перевірки залежностей, контролю конфігурацій і постійного моніторингу системи. Отже, використання лише одного методу перевірки не дає змоги виявити всі можливі вразливості, тому найкращим підходом є поєднання різних методів тестування [5].

Висновки. Порівняння документів OWASP Top 10 2021 та 2025 років показало зміщення уваги від окремих помилок у коді до системних проблем: контролю доступу, конфігурації та ланцюга постачання програмного забезпечення. Найвпливовішою залишається категорія Broken Access Control, яка зберегла перше місце й поглинула SSRF. Найбільше зросла вага Security Misconfiguration (з п’ятого місця на друге) та Software

Supply Chain Failures, яка замінила Vulnerable and Outdated Components. Injection, Cryptographic Failures та Insecure Design опустилися в рейтингу. Нижча позиція в рейтингу сама по собі не означає меншої небезпеки, оскільки рейтинг ґрунтується на раніше отриманих даних. Додаткового аналізу потребують Insecure Design, Security Logging and Alerting Failures і нова категорія Mishandling of Exceptional Conditions: їх важко виявити автоматично, тому вони менш помітні. Те саме стосується атак на ланцюг постачання, які часто не мають присвоєних CVE. Щодо наступної редакції можна припустити, що Broken Access Control, Security Misconfiguration, Software Supply Chain Failures і Authentication Failures збережуть високі позиції, оскільки пов’язані із системними проблемами розроблення та експлуатації. Вразливість Injection, найімовірніше, поступово спуститься на нижчі позиції рейтинга завдяки вбудованому захисту фреймворків і кращим інструментам тестування. Подальші дослідження доцільно спрямувати на тестування вразливостей вебзастосунків та методам захисту від них.

Список використаних джерел:

1. OWASP Top 10:2025 [Електронний ресурс] / OWASP Foundation. 2025. URL: https://owasp.org/Top10/2025/ (дата звернення: 30.10.2026).
2. OWASP Top 10:2021 [Електронний ресурс] / OWASP Foundation. 2021. URL: https://owasp.org/Top10/ (дата звернення: 30.10.2026).
3. OWASP API Security Top 10 – 2023 [Електронний ресурс] / OWASP Foundation. 2023. URL: https://owasp.org/API-Security/editions/2023/en/0x11-t10/ (дата звернення: 30.10.2026).
4. What Changed in OWASP Top 10 2025 and Recommendations for Each Category [Електронний ресурс] / Qualys. 2026. URL: https://blog.qualys.com/qualys-insights/2026/06/15/what-changed-in-owasp-top-10-2025-and-recommendations-for-each-category (дата звернення: 30.10.2026).
5. Scarfone K., Souppaya M., Cody A., Orebaugh A. Technical Guide to Information Security Testing and Assessment: NIST Special Publication 800-115. Gaithersburg: NIST, 2008. 80 p. URL: https://csrc.nist.gov/pubs/sp/800/115/final (дата звернення: 30.10.2026).
6. CWE Top 25 Most Dangerous Software Weaknesses [Електронний ресурс] / MITRE. URL: https://cwe.mitre.org/top25/ (дата звернення: 30.10.2026).