КОМП'ЮТЕРНІ НАУКИ

УДК 004.056 DOI: https://doi.org/10.32515/2664-262X.2024.10(41).2.3-10

О.А. Ревнюк, асп. **Н.В. Загородна,** доц., канд. техн. наук
Тернопільський національний технічний університет імені Івана Пулюя, м. Тернопіль, Україна
e-mail: revo0708@gmail.com
О.С. Улічев, канд. техн. наук
Центральноукраїнський національний технічний університет, м. Кропивницький, Україна
e-mail: askin79@gmail.com

Адаптивна методологія розрахунку кількісного показника стану захищеності вебзастосунків

Розроблена методологія оцінки захищеності вебзастосунків враховує різні аспекти безпеки на основі вимог OWASP ASVS, з яких сформовано релевантну вибірку. Розроблено структурований набір критеріїв з чіткими правилами оцінювання кожної вимоги. Введено систему вагових коефіцієнтів для критеріїв та вимог, що дозволяє адаптовуватись під архітектуру, функціонал та вимоги щодо захисту вебсайту. Підхід дозволяє отримувати кількісні метрики виконання кожної вимоги, розділу та інтегровану оцінку безпеки сайту.
web application security, quantitative assessment, OWASP ASVS, evaluation criteria, security assessment

Постановка проблеми. У сучасному світі інформаційних технологій вебдодатки стали невід'ємною частиною життєдіяльності багатьох організацій та користувачів. Вони використовуються у різноманітних сферах – від електронної комерції до державних сервісів і соціальних мереж – забезпечуючи зручний доступ до послуг, автоматизацію бізнес-процесів і керування даними у реальному часі. Проте з розвитком веб-технологій зростає і загроза кіберзлочинності, яка постійно еволюціонує та пристосовується до нових технічних реалій. Кількість кібератак, спрямованих на веб-додатки, зростає щороку [1], що ставить питання їх безпеки у пріоритетний ряд завдань для розробників, аналітиків та фахівців з кібербезпеки.

Атаки на системи безпеки вебсайтів не є новими і відбуваються з початку епохи Web 2.0. Вразливості на вебсайтах притаманні як звичайним компаніям, так і брендовим. Наприклад, збитки від кібератак для відомих брендів у 2018–2019 роках оцінюються у понад 350 мільйонів доларів [2–4]. Постійна загроза кіберзлочинності призводить до необхідності впровадження нових, більш ефективних методів і засобів забезпечення захищеності вебдодатків. За даними міжнародних звітів з кібербезпеки [5, 6], більшість кібератак орієнтовані саме на веб-інтерфейси, де зловмисники використовують різноманітні техніки для проникнення у системи та компрометації даних. Особливого значення набули такі загрози, як несанкціонований доступ до конфіденційних даних, атаки типу SQL-ін'єкції, Cross-Site Scripting (XSS) [7], атаки на сеанси користувачів та вразливості в системах автентифікації. Подібні уразливості призводять до масштабних інцидентів, результатами яких є втрати даних, порушення конфіденційності та збої у роботі систем.

Основний напрямок для зменшення кількості атак – це систематичне тестування безпеки та оцінка вразливостей. Крім того, з розвитком хмарних обчислень і поширенням архітектур на базі мікросервісів питання захищеності веб-додатків стає ще більш складнішим. Веб-додатки не лише повинні захищати дані, але й забезпечувати

їхню цілісність і доступність у розподілених середовищах, де багато компонентів взаємодіють один з одним через відкриті інтерфейси. Така складність архітектур ускладнює процес захисту, оскільки кожен елемент системи може стати потенційною точкою входу для атак. Отже, забезпечення належного рівня захищеності вебдодатків потребує комплексного підходу, що враховує як традиційні методи захисту, так і новітні рішення для протидії сучасним кіберзагрозам.

Аналіз останніх досліджень і публікацій. З початку XXI століття дослідження безпеки вебсайтів зазнали значної еволюції, тісно пов'язаної з бурхливим розвитком веб-технологій. На початку 2000-х років фокус досліджень був зосереджений на обмеженому спектрі вразливостей, характерних для тогочасних веб-додатків, таких як міжсайтовий скриптінг (XSS) та SQL-ін'єкції. Проте стрімкий розвиток веб-технологій, поява нових архітектурних підходів (AJAX, Web 2.0) та розширення функціональності веб-додатків призвели до значного ускладнення ландшафту веб-безпеки та виникнення нових векторів атак.

Сучасні дослідження у сфері безпеки вебсайтів характеризуються комплексним підходом, який охоплює як традиційні аспекти безпеки, так і нові виклики, пов'язані з розвитком хмарних технологій, мікросервісної архітектури та прогресивних веб-додатків. Особлива увага приділяється автоматизованим засобам виявлення вразливостей, включаючи розробку більш досконалих сканерів безпеки та методів статичного і динамічного аналізу коду.

На ринку існує безліч інструментів для збору інформації та оцінки вразливостей, проте вони не можуть забезпечити 100% точності та рішення для виявлення конкретних вразливостей відповідно до CWE (Common Weakness Enumeration). До такого висновку дійшли науковці Dixitkumar .V та Prajapati1, які проводили дослідження [8] інструментів для оцінки вразливостей та збору інформації різних форматів й функціональних можливостей. Вони запропонували власний підхід, який полягає в об’єднанні кількох інструментів для збору інформації та оцінки вразливостей, що дозволяє досягти більш високого рівня покриття та точності виявлення вразливостей.

Дослідження [9] авторів Nikhil Rane та Amna Qureshi висвітлює порівняння автоматизованого сканування та ручного тестування вебсайтів на проникнення для оцінки ефективності цих методів у виявленні вразливостей. Експериментальні результати підтвердили, що ручне тестування на проникнення є більш ефективним, ніж автоматизоване, з точки зору точності та глибини аналізу. Дослідники дійшли висновку, що практичні дослідження підкреслюють важливість навичок і досвіду фахівця з тестування на проникнення у виявленні та використанні слабких місць у безпеці. Автоматизовані інструменти, хоча й корисні для початкового сканування, можуть генерувати хибнопозитивні результати та пропускати специфічні вразливості.

Важливим етапом у розвитку досліджень стало формування галузевих стандартів та рекомендацій від провідних організацій з інформаційної безпеки, таких як OWASP (Open Web Application Security Project) [10], NIST (National Institute of Standards and Technology) [11] та SANS Institute [12]. Ці стандарти, зокрема OWASP Top 10, не лише систематизували знання про відомі вразливості та методи захисту, але й сприяли розробці єдиної методологічної бази для проведення досліджень та аудиту безпеки веб-додатків на різних етапах життєвого циклу вебдодатка.

Незважаючи на інтенсивний розвиток методологічних баз та ініціатив стандартизації у галузі інформаційної безпеки, спостерігається суттєва прогалина в інструментарії оцінки захищеності вебресурсів. Існуючі автоматизовані системи сканування безпеки, хоча й забезпечують визначення широкого спектру вразливостей, демонструють істотні обмеження у верифікації критичних параметрів захисту. Зокрема,

поза межами їх функціональності залишається багато речей, що потрібно перевіряти вручну, таких, для прикладу, як аналіз політики парольної автентифікації для доступу до персоналізованих інтерфейсів користувача та валідація коректності імплементації механізмів журналювання безпекових інцидентів під час здійснення кібератак тощо.

Чинні галузеві стандарти та нормативні документи у сфері вебзахисту здебільшого зосереджуються на класифікації та категоризації потенційних вразливостей вебзастосунків, проте не пропонують уніфікованої методології кількісної оцінки рівня їх захищеності. З огляду на різноманітність функціонального навантаження сучасних вебресурсів та диверсифікацію їх архітектурних рішень, актуалізується проблематика детермінації необхідного та достатнього обсягу тестування безпеки. Відсутність стандартизованої системи обчислення коефіцієнта захищеності вебресурсу суттєво ускладнює розуміння ситуації, процес ідентифікації потенційних векторів компрометації та розробки рішень покращення захисту вебсайту.

Постановка завдання. Метою дослідження є розробка адаптивної методології кількісної оцінки рівня захищеності вебдодатку шляхом динамічного розрахунку коефіцієнта безпеки з урахуванням індивідуальних характеристик проекту, зокрема специфіки його функціоналу та архітектури.

Виклад основного матеріалу. У сучасному ландшафті кібербезпеки спостерігається зростання популярності OWASP Application Security Verification Standard (ASVS) [13] - комплексного стандарту, що регламентує вимоги до захищеності веб-додатків. ASVS надає чітко структурований набір контролів безпеки структурований по 14 розділах, спрямованих на забезпечення конфіденційності, цілісності та доступності інформаційних активів.

Даний стандарт позиціонується як практичний інструментарій для проведення всебічної оцінки безпеки веб-додатків протягом усього життєвого циклу розробки програмного забезпечення - від стадії проектування до виведення з експлуатації. Важливою перевагою ASVS є його інтеграція з загальновизнаною системою класифікації вразливостей Common Weakness Enumeration (CWE) [14]. Це сприяє стандартизації підходів до ідентифікації та усунення потенційних загроз безпеці. Проте, незважаючи на свою масштабність та практичну цінність, ASVS не надає методологічних засад для формування кількісної оцінки захищеності веб-сайту.

Існуюча структура стандарту орієнтована на якісний аналіз безпеки, що включає перевірку 282 вимог, що розподілені по 14 розділах. Слід зазначити, що на практиці можливість перевірки кожної з вимог залежить від багатьох факторів, зокрема від доступу до інформації, яку має аудитор (доступ до технічної документації, вихідного коду чи розробників), від архітектури та функціоналу досліджуваного вебсайту. Крім того даний стандарт містить вимоги, які необхідно перевірити, проте не дає чітких рекомендацій для їх перевірки. Велика кількість вимог та відсутність єдиної методології їх перевірки ускладнює процес об'єктивного вимірювання та порівняння рівня захищеності різних веб-додатків.

На першому етапі розробки даної методології, було детально проаналізовано вміст кожного розділу та зменшено вибірку вимог для подальшої роботи до 133 вимог, розподілених в межах 13 розділів. Наступним кроком стала розробка авторами множини критеріїв для перевірки кожної з вимог. Для кожного критерію було запропоновано методологію оцінювання за шкалою з трьома градаціями: "0 балів" (відсутність реалізації функціоналу, що відповідає критерію), "0,5 бала" (часткова реалізація) та "1 бал" (повна реалізація або наявність адекватного механізму безпеки).

Для прикладу, розглянемо вимогу: "Verify that the application or framework enforces a strong anti-CSRF mechanism to protect authenticated functionality, and effective anti-automation or anti-CSRF protects unauthenticated functionality".

Ця вимога стосується перевірки та впровадження механізмів захисту від атак Cross-Site Request Forgery (CSRF), які спрямовані на захист аутентифікованих функцій вебдодатка та захист від автоматизованих атак для неавтентифікованих функцій, застосовуючи CAPTCHA або інші методи. Важливо забезпечити правильну обробку помилок, щоб уникнути розкриття чутливої інформації, і належне інформування користувачів у разі невдалих запитів через CSRF-захист. Система повинна вести логування та моніторинг всіх відмов у запитах через CSRF-захист і регулярно тестуватися для виявлення можливих вразливостей. Нижче приведено два з десяти критеріїв оцінювання вимоги:

1. Чи використовуються унікальні CSRF-токени для кожної сесії користувача?
   - 0 балів: CSRF-токени не використовуються для сесій користувачів.
   - 0.5 бала: Токени використовуються, але не для всіх сесій або не генеруються унікально.
   - 1 бал: Унікальні CSRF-токени генеруються для кожної сесії користувача.
2. Чи перевіряються CSRF-токени на кожен запит, що змінює стан?
   - 0 балів: CSRF-токени не перевіряються на змінюючі запити.
   - 0.5 бала: Токени перевіряються на деякі запити, але не на всі дії, що змінюють стан.
   - 1 бал: CSRF-токени перевіряються на всі запити, що змінюють стан.

Проте оцінки за окремими критеріями не дають загального уявлення про якість виконання окремої вимоги чи оцінку безпеки вебдодатку загалом. Крім того, для врахування особливостей архітектури вебдодатку, діючого функціоналу та наявної документації було запропоновано ввести коефіцієнти важливості вимог та критеріїв. Цей етап передбачає суб'єктивну оцінку експертом, який, спираючись на власний досвід та розуміння критичності функціоналу, присвоює коефіцієнти важливості кожній вимозі в межах розділу та кожному критерію в межах вимоги. Для кращого розуміння розглянемо структуру методології, зображену на рисунку 1.

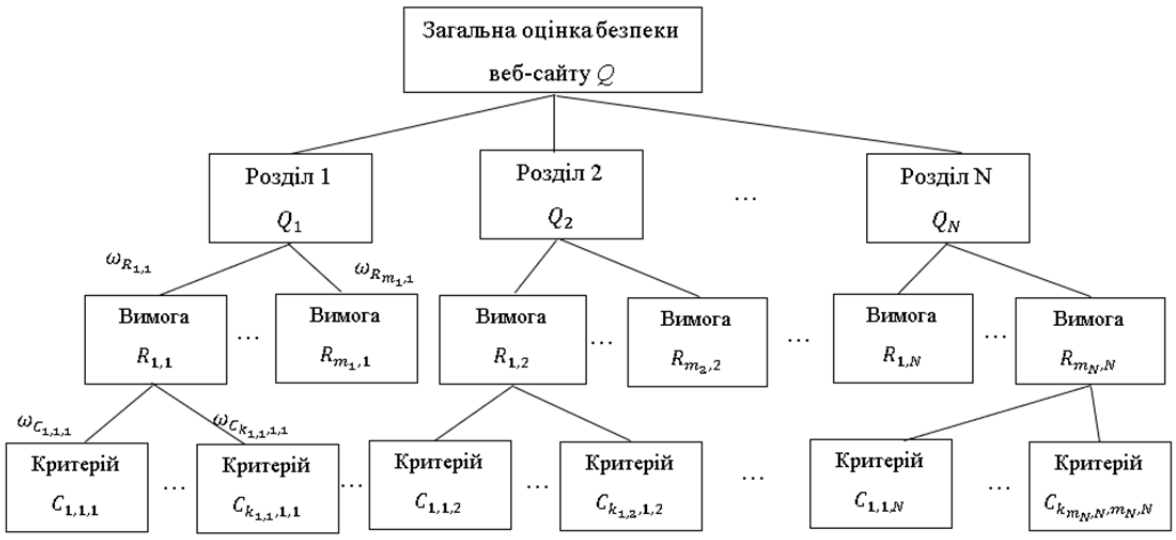

Рисунок 1 – Загальна структура адаптивної методології для оцінювання вебдодатку

Джерело: розроблено авторами

Для кращого розуміння суті рисунку розпишемо детальніше використані позначення:

$R_{m,n}$ – оцінка *m-oї* вимоги в межах *n-го* розділу, $m = 1..m_n$, $n = 1..N$, m_n - кількість вимог в межах *n-го* розділу, причому $m_1 + m_2 + ...+,_N = M$, M - загальна кількість вибраних вимог, N - загальна кількість вибраних розділів зі стандарту ASVS.

$C_{k,m,n}$ – значення *k-го* критерію *m-oї* вимоги в межах *n-го* розділу, $k = 1..k_{m,n}$, $k_{m,n}$ - кількість розроблених авторами критеріїв для оцінювання *m-oї* вимоги *n-го* розділу. Нагадаємо що оцінка кожного критерію відбувається за одним з трьох значень “0”, “0,5” та “1”.

$\omega_{C_{k,m,n}}$ – коефіцієнт важливості *k-го* критерію *m-oї* вимоги *n-го* розділу, що визначається технічним експертом з врахуванням того, як даний критерій впливає на виконання вимоги, до якої він застосовується. Ці коефіцієнти визначені авторами методології апріорі. Однак, експерт, який проводить оцінку, має можливість коригувати ці значення, враховуючи специфіку досліджуваного веб-сайту та вибравши зручну для себе шкалу оцінювання.

$\omega_{R_{m,n}}$ – коефіцієнт важливості *k-го* критерію *m-oї* вимоги *n-го* розділу, що визначається для кожної вимоги аудитором, що проводить оцінку безпеки веб-сайту в залежності від наявної інформації, архітектури та функціоналу системи, а також з огляду на бізнес-контекст, вимоги до захисту інформації. Аудитор може вибрати зручну для себе шкалу для оцінювання важливості вимог. В даній роботі запропоновано використовувати шкалу від 0 (вказує на відсутність функціоналу, що відповідає даній вимозі, в вебдодатку) до 10 (критично важлива вимога для безпеки функціоналу).

На першому кроці обчислень необхідно провести оцінку виконання кожної вимоги. Для цього спершу здійснимо нормалізацію коефіцієнтів важливості критеріїв в межах даної вимоги за формулою:

$$\varpi_{C_{k,m,n}} = \frac{\omega_{C_{k,m,n}}}{\sum_{k=1}^{k_{m,n}} \omega_{C_{k,m,n}}}, \quad (1)$$

де $\varpi_{C_{k,m,n}}$ – нормалізований ваговий коефіцієнт *k-го* критерію *m-oї* вимоги *n-го* розділу; $\sum_{k=1}^{k_{m,n}} \omega_{C_{k,m,n}}$ – загальна сума вагових коефіцієнтів критеріїв *m-oї* вимоги *n-го* розділу.

Тоді інтегральну оцінку виконання *m-oї* вимоги *n-го* розділу можна отримати як збалансовану ваговими коефіцієнтами суму оцінок експерта безпеки функціоналу веб-сайту за критеріями в межах даної вимоги:

$$R_{m,n} = \sum_{k=1}^{k_{m,n}} \varpi_{C_{k,m,n}} \cdot C_{k,m,n} . \quad (2)$$

Для отримання оцінок для кожного розділу необхідно спершу нормалізувати коефіцієнти важливості вимог. Це можна зробити за формулою:

$$\varpi_{R_{m,n}} = \frac{\omega_{R_{m,n}}}{\sum_{m=1}^{m_n} \omega_{R_{m,n}}}, \quad (3)$$

де $\varpi_{R_{m,n}}$ – нормалізований ваговий коефіцієнт *m-ої* вимоги *n-го* розділу;

$\sum_{m=1}^{m_n} \omega_{R_{m,n}}$ – сума вагових коефіцієнтів вимог *n-го* розділу.

Наступним етапом розрахунків є визначення кількісної оцінки захищеності вебсайту для певного розділу. Оцінку безпеки *n-го* розділу з врахуванням особливостей структури сайту та індивідуального підходу аудитора можна обчислити як:

$$Q_n = \sum_{k=1}^{m_n} \varpi_{R_{m,n}} \cdot R_{m,n} . \quad (4)$$

Завершальним етапом є інтегрована оцінка безпеки сайту, яку можна обчислити, як середню оцінку безпеки всіх розділів

$$Q = \frac{\sum_{i=1}^{N} Q_n}{N}. \quad (5)$$

Отже, в основі розробленої методології лежить диференційований підхід до класифікації вимог безпеки, що враховує рівень критичності захисту даних та специфіку функціональних компонентів веб-додатку і дозволяє отримати кількісну метрику оцінки безпеки вебсайту.

Висновки. Запропонована нова методологія кількісної оцінки рівня захищеності вебзастосунків, яка враховує індивідуальні характеристики проекту, включаючи специфіку функціоналу, архітектуру та рівень критичності даних. Розроблена система показників дозволяє оцінити рівень безпеки вебзастосунку у числовому вимірі та визначити його відповідність встановленим вимогам як на етапі планування проекту, так і на етапі його експлуатації. Запровадження такого адаптивного підходу до оцінювання рівня захисту надасть можливість експерту створення індивідуальних наборів вимог залежно від архітектури, функціоналу та галузі застосування конкретного веб-додатку методом налаштувань коефіцієнтів важливості. Така гнучка модель дозволить отримувати більш точні результати, які відображатимуть реальні потреби додатку у сфері безпеки. Крім цього, адаптація до конкретних потреб користувачів дозволить уникнути випадків штучного зниження оцінок через відсутність нерелевантних для вебдодатка вимог, що, своєю чергою, забезпечить справедливість і об’єктивність оцінювання.

Практичне значення даної методології полягає у можливості підвищення ефективності процесів розробки та тестування вебзастосунків з врахуванням кіберризиків. Важливо зазначити, що запропонована система показників, яка враховує індивідуальні характеристики вебзастосунків не має аналогів, що робить її унікальною та інноваційною.

Подальші дослідження будуть спрямовані на верифікацію та валідацію запропонованої методології, а також на розробку інструментів автоматизації процесу оцінювання.

Список літератури

1. Zahid A. Vulnerability detection and prevention: an approach to enhance cybersecurity. *MS Computer Science*. 2024. DOI: 10.13140/RG.2.2.31687.71841
2. Humayun. M., Niazi, M., Jhanjhi. N. Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study / M. Humayun et al. *Arabian Journal for Science and Engineering*. 2020. T. 45(4). 3171–3189. DOI: 10.1007/s13369-019-04319-2.

3. Asaduzzaman M. Security Aspects of ePayment System and Improper Access Control in Microtransactions. *EasyChair*. 2020.
4. 2024 Data Breach Investigations Report. *Verizon Business*. URL: https://www.verizon.com/business/resources/reports/2024-dbir-data-breach-investigations-report.pdf.
5. Lella I., Theocharidou M., Magonara E. Enisa threat landscape 2024. ENISA, 2024. 130 c.
6. Ravindran U., Potukuchi R. V. A review on web application vulnerability assessment and penetration testing. *Review of Computer Engineering Studies*. 2022. T. 9, № 1. C. 1–22. DOI: 10.18280/rces.090101
7. Pentest monkey. URL: https://pentestmonkey.net/
8. I. Yaqoob, S.A. Hussain, S. Mamoon. Penetration Testing and Vulnerability Assessment. *Journal of Network Communications and Emerging Technologies (JNCET)*. 2017. T. 7, № 8.
9. N. Rane, A. Qureshi. Comparative Analysis of Automated Scanning and Manual Penetration Testing for Enhanced Cybersecurity. *12th International Symposium on Digital forensics and security* : : матеріали конференції, м. San Antonio, 29 квіт. 2024 р. San Antonio, 2024.
10. OWASP Foundation, the Open Source Foundation for Application Security. URL: https://owasp.org
11. National Institute of Standards and Technology. URL: https://www.nist.gov
12. Cyber Security. URL: https://www.sans.org/emea
13. A. van der Stock, D. Cuthbert, J. Manico. OWASP Application Security Verification Standard 4.0.3. 2021. 71 c.
14. CWE - Common Weakness Enumeration. URL: https://cwe.mitre.org.

References

1. Zahid A. (2024) Vulnerability detection and prevention: an approach to enhance cybersecurity. *MS Computer Science*. https://doi.org/10.13140/RG.2.2.31687.71841
2. Humayun. M., Niazi. M., & Jhanjhi. N. (2020). Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study / M. Humayun et al. *Arabian Journal for Science and Engineering*. (Vol. 45(4)). (pp 3171–3189). https://doi.org/10.1007/s13369-019-04319-2.
3. Asaduzzaman M. (2020). Security Aspects of ePayment System and Improper Access Control in Microtransactions. *EasyChair*.
4. (2024) Data Breach Investigations Report. *Verizon Business*. https://www.verizon.com/business/resources/reports/2024-dbir-data-breach-investigations-report.pdf.
5. Lella I., Theocharidou M., Magonara E. (2024). Enisa threat landscape. ENISA, 2024.
6. Ravindran U., Potukuchi R. V. (2022). A review on web application vulnerability assessment and penetration testing. *Review of Computer Engineering Studies*. (Vol. 9(1)). https://doi.org/ 10.18280/rces.090101
7. Pentest monkey. https://pentestmonkey.net/
8. I. Yaqoob, S.A. Hussain, & S. Mamoon. (2017) Penetration Testing and Vulnerability Assessment . *Journal of Network Communications and Emerging Technologies (JNCET)*. 2017. (Vol. 7(8)).
9. N. Rane, & A. Qureshi. (2024). Comparative Analysis of Automated Scanning and Manual Penetration Testing for Enhanced Cybersecurity. *12th International Symposium on Digital forensics and security* : Conference. San Antonio.
10. OWASP Foundation, the Open Source Foundation for Application Security. https://owasp.org
11. National Institute of Standards and Technology. https://www.nist.gov
12. Cyber Security Training. https://www.sans.org/emea
13. A. van der Stock, D. Cuthbert, & J. Manico. (2021). OWASP Application Security Verification Standard 4.0.3.
14. CWE - Common Weakness Enumeration. https://cwe.mitre.org.

Oleksandr Revniuk, post-graduate, **Nataliya Zagorodna**, Assoc. Prof., PhD tech. sci.
Ternopil Ivan Puluj National Technical University, Ternopil, Ukraine
Oleksandr Ulichev, PhD tech. sci.
Central Ukrainian National Technical University, Kropyvnytskyi, Ukraine

Adaptive Methodology for Computing the Quantitative Security Status Indicator of Web Applications

This article proposes an adaptive methodology for quantitative security assessment of web applications based on standardized requirements from the OWASP Application Security Verification Standard (ASVS). This methodology takes into account various aspects of website security, including authentication, authorization, data protection, input handling, and others.

The proposed approach allows obtaining quantitative metrics for the level of compliance with each requirement, thus ensuring objectivity and transparency of the evaluation process for both auditors and web application owners. The use of clearly defined numerical metrics facilitates unambiguous interpretation of results and avoids subjectivity in determining the security level of a web application. Based on the analysis of OWASP ASVS requirements, a relevant subset of requirements was formed to assess the security of websites of varying complexity. It was assumed that the expert conducting the assessment possesses the necessary technical competencies and has access to web application development documentation. For each requirement, a structured set of criteria was developed with clearly defined evaluation rules to obtain quantitative indicators. A system of weight coefficients was introduced to determine the significance of each criterion and requirement, and their normalization was performed. The weight coefficients of requirements are established considering the functionality, website architecture, and availability of access to technical documentation or source code. To ensure methodology adaptivity, the auditor has the ability to modify any weight coefficients.

The implementation of an adaptive approach to security assessment allows forming individual requirements based on architecture and functionality of a web application by adjusting weight coefficients. This flexible model ensures more accurate results that reflect the website's actual security state.

web application security, quantitative assessment, OWASP ASVS, evaluation criteria, security assessment

Одержано (Received) 11.11.2024 *Прорецензовано (Reviewed) 13.12.2024*
Прийнято до друку (Approved) 23.12.2024