УДК 004.056
DOI: 10.31471/1993-9965-2024-2(57)-107-119

МЕТОДОЛОГІЯ КІЛЬКІСНОЇ ОЦІНКИ ЗАХИЩЕНОСТІ ВЕБДОДАТКУ ЕЛЕКТРОННОЇ КОМЕРЦІЇ НА ЕТАПІ ЕКСПЛУАТАЦІЇ

О. А. Ревнюк*, Н. В. Загородна

Тернопільський національний технічний університет імені Івана Пулюя;
46001, Тернопіль, вул. Руська, 56, e-mail: r e v o 0 7 0 8 @ g m a i l . c o m

Запропоновано загальний підхід кількісної оцінки захищеності вебдодатків електронної комерції на основі вимог стандарту OWASP ASVS, який містить 13 розділів, що враховують специфіку різних аспектів безпеки, включаючи автентифікацію, управління сесіями, контроль доступу, валідацію даних, захист файлів та конфігурацію системи. Розроблена методологія дозволяє отримувати кількісні показники рівня виконання кожної вимоги, що робить оцінювання об'єктивним і зрозумілим для аудиторів та власників вебдодатків.На основі проведеного аналізу загального переліку вимог OWASP ASVS було відібрано множину вимог для оцінки безпеки функціонуючого інтернет-магазину за припущення, що у виконавця аудиту відсутня технічна документація щодо розробки вебдодатку. Для кожної з вимог був сформований структурований набір критеріїв з чіткими правилами їх оцінювання для отримання кількісних показників. У дослідженні використано тестове середовище "OWASP Juice Shop", яке дозволило провести апробацію методології на реальному прикладі, що містить низку наперед відомих вбудованих вразливостей. Даний вебдодаток є прототипом типового інтернет-магазину, що робить його ідеальним об'єктом для даного дослідження. Як і очікувалось, результати оцінки досліджуваного додатку засвідчили низький рівень впровадження безпекових практик у таких аспектах, як управління сесіями, валідація введених даних та захист файлів, тоді як автентифікація та контроль доступу мали середній рівень відповідності стандартам. Запропонована методологія робить власний внесок у розвиток практик забезпечення захищеності вебдодатків електронної комерції, надаючи ефективний інструмент для оцінки безпеки та пошуку вразливостей на етапі експлуатації вебдодатку.

Ключові слова:безпека вебдодатків, інтернет-магазин, OWASP ASVS, критерії оцінювання, оцінка безпеки.

The article proposes a general approach to the quantitative assessment of e-commerce web application security based on the OWASP ASVS standard, which includes 13 sections addressing various aspects of security, such as authentication, session management, access control, data validation, file protection, and system configuration. The developed methodology enables obtaining quantitative indicators for the level of compliance with each requirement, making the evaluation objective and understandable for auditors and web application owners.Based on an analysis of the general list of OWASP ASVS requirements, a subset of requirements was selected for assessing the security of an operational online store, assuming that the auditor lacks technical documentation about the web application's development. For each requirement, a structured set of criteria with clear evaluation rules was developed to derive quantitative indicators. The study utilized the "OWASP Juice Shop" test environment, allowing the methodology to be tested on a practical example containing a range of predefined built-in vulnerabilities. This web application serves as a prototype of a typical online store, making it an ideal subject for this research.As expected, the assessment results revealed a low level of implementation of security practices in areas such as session management, input data validation, and file protection, while authentication and access control demonstrated a medium level of compliance with the standards. The proposed methodology contributes to advancing practices for ensuring the security of e-commerce web applications by providing an effective tool for security assessment and vulnerability identification during the operational phase of a web application.

Keywords**:** web application security, online store, OWASP ASVS, evaluation criteria, security assessment.

Вступ

Еволюція цифрових технологій призвела до трансформації традиційних моделей споживання та сприяла розвитку електронної комерції. Інтернет-магазини, як ключовий елемент цієї еволюції, забезпечують безпрецедентний доступ до товарів та послуг, нівелюючи географічні та часові обмеження. Цей феномен суттєво впливає на соціально-економічні процеси, змінюючи парадигму роздрібної торгівлі та формуючи нові моделі взаємодії між споживачами та продавцями. Дослідження свідчать [1-2] про кореляцію між розвитком інтернет-магазинів та економічним зростанням. Збільшення обсягів онлайн-торгівлі стимулює розвиток логістичної інфраструктури, створює нові робочі місця у

сфері IT та цифрового маркетингу, а також сприяє підвищенню конкурентоспроможності бізнесу.

Найчастіше в зоні ризику опиняються інтернет-магазини та електронна комерція [3], які сьогодні є основою ведення бізнесу для багатьох компаній. Онлайн-торгівля стала не лише зручним способом продажу товарів і послуг, а й ключовим інструментом для розширення ринків, зниження витрат і підвищення конкурентоспроможності. Електронна комерція забезпечує мільйонам користувачів доступ до товарів і послуг з будь-якого куточка світу та водночас, може становити небезпеку для конфіденційності їхніх особистих даних. Адже, зростання популярності інтернет-магазинів робить їх привабливою ціллю для кіберзлочинців. Вразливості у вебдодатках електронної комерції можуть призводити до серйозних наслідків: викрадення фінансових даних, компрометації особистої інформації клієнтів, втрати довіри користувачів та значних фінансових втрат для компаній. Кіберзлочинці постійно шукають нові способи атаки на інтернет-магазини, тому необхідно завжди бути напоготові та вдосконалювати системи захисту. Особливо небезпечними є атаки на платіжні системи, які є майже в будь-якого інтернет-магазину, а також порушення у роботі баз даних, що може призвести до збоїв у функціонуванні бізнесу. Таким чином, питання безпеки для інтернет-магазинів є критично важливим аспектом, що визначає не лише успішність бізнесу, але й його здатність підтримувати стабільну та безпечну роботу у сучасному цифровому середовищі. Успіх інтернет-магазину безпосередньо залежить від довіри клієнтів, а забезпечення надійного захисту їхніх даних є фундаментом цієї довіри.

Автоматизовані інструменти, сканери вразливостей і тестування на проникнення, які широко використовуються у практиці інформаційної безпеки, мають свої обмеження. Вони не завжди здатні виявити складні атаки, спрямовані на злом бізнес-логіки або експлуатацію багатошарових вразливостей. Це змушує розробників постійно вдосконалювати підходи до забезпечення безпеки та розробляти нові методи для більш глибокого аналізу вразливостей. Водночас традиційні підходи до забезпечення безпеки не завжди є ефективними для виявлення та нейтралізації сучасних загроз, що виникають у сучасних вебдодатках.

Мета дослідження

Метою дослідження є демонстрація методики кількісної оцінки вебсайту електронної комерції з типовим функціоналом на етапі експлуатації в рамках авторської методології, яка дозволяє кількісно оцінювати рівень захищеності вебдодатку, забезпечуючи прозорість і об'єктивність процесу.

Аналіз сучасних закордонних і вітчизняних досліджень і публікацій

На сьогоднішній день існує низка наукових досліджень, які охоплюють різні аспекти забезпечення безпеки вебдодатків, а також загальних систем управління інформаційною безпекою (ISMS). Одним з важливих напрямів досліджень є аналіз ефективності контролю систем інформаційної безпеки на основі міжнародних стандартів. Наприклад, дослідження, присвячене впровадженню методів вимірювання ефективності контролів у системах управління інформаційною безпекою [4], базується на стандартах ISO/IEC 27004:2013 [5] та ISO/IEC 27002:2013 [6]. Автори цієї роботи розробили набір метрик та індикаторів для оцінки того, наскільки успішно організація впроваджує заходи безпеки та контролює їх ефективність. Це дослідження підкреслює важливість кількісного підходу до вимірювання результатів безпекових заходів і надає конкретні рекомендації щодо впровадження цих методів у практичну діяльність організації. Проте визначені метрики є загальними та універсальними для інформаційних систем та не адаптованими для оцінки безпеки вебдодатків.

Існують дослідження [7], спрямовані на оцінку відповідності безпеки сервісів існуючим стандартам та регуляціям. Такі дослідження розглядають впровадження системного підходу до забезпечення відповідності стандартам інформаційної безпеки, зокрема у фінансовій та інших високоризикових сферах. Використовуючи методи динамічного та статичного аналізу, автори пропонують методологію, яка дозволяє автоматизувати процеси перевірки на відповідність вимогам безпеки. Це дослідження показало ефективність впровадження таких підходів на прикладі онлайн-платіжних сервісів, що допомагає підвищити захищеність даних і відповідність сервісів до міжнародних стандартів, таких як PCI-DSS [8] та ISO 27002. Незважаючи на це – загадані дослідження не вирішують питання кількісної оцінки захищеності вебдодатка в цілому.

ISSN 1993–9965 print ISSN 2415–3524 online
Науковий вісник ІФНТУНГ 2024. № 2(57)

Ще одним важливим напрямком є розробка концептуальних моделей для класифікації вебдодатків на основі їх операційної та поточної критичності. Наприклад, у дослідженні [9] було запропоновано використання двох ключових показників: операційної критичності (OC) та критичності даних (DC). Це дозволяє організаціям більш точно визначати вимоги до безпеки залежно від важливості вебдодатків для операційної діяльності компанії та конфіденційності обробки даних. Такий підхід дає змогу уникати надмірних витрат на непотрібні заходи безпеки і водночас забезпечувати адекватний рівень захищеності критичних для організації додатків. Та попри все, часто виникають ситуації, коли власник інтернет-магазину може змінити саму концепцію магазину, замінити методи оплати та взагалі повністю змінити власний продукт. І після імплементації нового функціоналу - знову ж таки виникає потреба оцінити та проаналізувати поточний рівень захищеності вебдодатку та наявності потенційних вразливостей, якими можуть скористатись кіберзлочинці.

З огляду на постійне зростання загроз для безпеки вебдодатків, з'являється дедалі більше стандартів, спрямованих на забезпечення інформацією належного рівня захисту інформаційних систем. Однією із таких систем є Common Weakness Enumeration (CWE) [10]. Це загальнодоступний реєстр типових слабких місць у програмному забезпеченні, створений для полегшення ідентифікації, аналізу та управління вразливостями у програмних системах. CWE був розроблений та підтримується організацією MITRE у співпраці з експертами у галузі кібербезпеки.

Однією з основних переваг CWE є його універсальність. Він не обмежується виключно вебдодатками, а охоплює всі типи програмного забезпечення. Більше того, CWE застосовується на всіх етапах життєвого циклу розробки програмного забезпечення: від етапу проєктування та кодування до тестування, впровадження та експлуатації. Такий підхід робить його цінним інструментом не лише для окремих проєктів, а й для організаційного управління ризиками.

Попри свою потужність та гнучкість, CWE має певні обмеження. Він не надає кількісної оцінки рівня захищеності програмного забезпечення, а лише ідентифікує потенційні вразливості. Іншими словами, CWE слугує базою для аналізу ризиків, але не дає прямої відповіді на питання, наскільки безпечним є вебдодаток.

Не менш відомим та широко використовуваним веб-розробниками стандартом у сфері веб-технологій є OWASP Application Security Verification Standard (ASVS) [11]. ASVS – це структурований набір вимог до безпеки вебдодатків, який використовується для тестування, оцінювання та вдосконалення безпеки програмного забезпечення на різних етапах його життєвого циклу. Цей стандарт слугує основним інструментом для архітекторів, розробників, тестувальників та фахівців з інформаційної безпеки, забезпечуючи їм надійні рекомендації для виявлення потенційних загроз та розробки відповідних контрзаходів.

Однією з ключових переваг ASVS є його комплексний підхід, що охоплює широкий спектр функціональних і нефункціональних аспектів безпеки - від проєктування до впровадження та подальшого супроводу вебдодатків. Стандарт забезпечує чітку структуру для впровадження контролів на різних етапах розробки, надаючи можливість адаптації вимог безпеки до конкретних умов використання.

ASVS виділяє три рівні перевірки безпеки, кожен з яких призначений для вебдодатків із різним ступенем критичності та ризиків. Перший рівень орієнтований на застосунки з низьким рівнем ризику і може бути повністю протестований за допомогою тестування на проникнення без необхідності доступу до вихідного коду. Другий рівень призначений для вебдодатків, що обробляють конфіденційну інформацію, тож вимагає більш глибокої перевірки, зокрема доступу до документації та вихідного коду. Цей рівень рекомендовано для більшості сучасних веб-застосунків, оскільки він надає збалансований підхід до забезпечення безпеки. Третій рівень призначений для критично важливих вебдодатків, таких як фінансові або медичні системи, які виконують транзакції з високим ступенем ризику і вимагають найвищого рівня захищеності.

Кожен рівень ASVS включає перелік вимог щодо захищеності, які співвідносяться з конкретними функціями безпеки, що повинні бути інтегровані в архітектуру та процеси розробки вебдодатків. Ці вимоги охоплюють всі аспекти безпеки, включно з автентифікацією, управлінням сесіями, контролем доступу, обробкою помилок, захистом даних та іншими ключовими елементами, що впливають на надійність вебдодатків. Завдяки своїй універсальності та широкій сфері застосування ASVS є важливим інструментом для забезпечення відповідності вебдодатків сучасним вимогам безпеки. На рисунку 1 відображені всі рівні стандарту перевірки безпеки застосунків OWASP4.0.

Рисунок 1 – Рівні стандарту перевірки безпеки додатків OWASP 4.0 [11]

Таким чином, OWASP ASVS надає відкритий інструментарій для розробки та перевірки вебдодатків, охоплюючи широкий спектр загроз та вразливостей на кожному етапі їх життєвого циклу. Це дозволяє ефективно інтегрувати безпекові заходи в процес розробки та забезпечити високу надійність програмного забезпечення у відповідь на сучасні виклики кібербезпеки.

Попри широке застосування стандартів CWE та OWASP ASVS, їх використання має певні обмеження. Наприклад, для повноцінного застосування ASVS часто потрібен доступ до вихідного коду, документації або навіть до внутрішніх процесів розробки, що може бути недоступним для сторонніх аудиторів або організацій. Крім того, ці стандарти виконують переважно інформаційну функцію про потенційні вразливості та контрзаходи ще на етапі проєктування продукту та не забезпечують механізмів кількісного оцінювання рівня безпеки на етапі експлуатації.

Такий підхід не вирішує проблеми оцінювання загального рівня захищеності вебдодатків, що часто є необхідністю у власників уже готових інтернет-магазинів для прийняття управлінських рішень. Тому розробка методології, яка б дозволила кількісно оцінювати рівень захищеності веб-сайтів електронної комерції на етапі експлуатації, є досить актуальною, оскільки це дозволить забезпечити прозорість і об'єктивність процесу оцінки рівня безпеки вебдодатка. Таке рішення дозволить не лише отримати рекомендаційну інформацію про те, що мало б бути імплементоване розробниками в продукт для захисту від вразливостей, але й оцінювати рівень захищеності в числовому вигляді, що зробить процеси аналізу безпеки більш об'єктивними та доступними для розуміння звичайних користувачів та власників вебсайтів. Це, в свою чергу, дозволить організаціям оцінити поточний стан захищеності своїх вебдодатків та прийняти подальші міри для вдосконалення власного продукту.

Опис розробленої системи оцінювання

На першому етапі даного дослідження був проведений детальний аналіз вимог стандарту OWASP ASVS версії 4.0.3. Даний стандарт містить 13 розділів, які структуровані за підрозділами, кожен з яких, в свою чергу, характеризується вичерпним переліком вимог для перевірки визначеного аспекту захищеності вебдодатку. Загалом даний стандарт містить 282 вимоги, які можуть бути обов'язковими або необов'язковими для перевірки, що залежить від рівня критичності вебдодатку. Автори стандарту відзначають, що лише перший рівень вебзастосунків можна протестувати без доступу до документації, коду, конфігурації та людей, залучених до процесу розробки. Слід також зазначити, що стандарт містить перелік вимог для перевірки захищеності веб-сайту, проте не надає чітких критеріїв перевірки валідності виконання цих вимог та оцінки безпеки вебзастосунку.

В даному дослідженні ми сфокусувались на оцінці безпеки типового інтернет-магазину за припущення відсутності будь-якої технічної документації. Тому на першому етапі був проведений аналіз усіх вимог вже згаданого стандарту ASVS з метою придатності до тестування на проникнення на етапі експлуатації вебзастосунку електронної комерції без доступу до інформації, що стосується питання його розробки. Після детального аналізу було виділено 7 основних розділів для даного випадку. Окремі розділи не потрапили до даного переліку, оскільки містили лише вимоги, які неможливо перевірити без технічної документації. Загалом, для нашої задачі було відібрано множину, обсягом з майже 50 вимог, які можливо перевірити на етапі експлуатації сайту. Окрім різної кількості вимог щодо захищеності у розділах, важливо зазначити, що кожен розділ може містити різну кількість підрозділів. Наприклад, розділ "Files and Resources" має лише два підрозділи: "File Upload" і "File Download", тоді як розділ "Authentication" включає три підрозділи, що

ISSN 1993–9965 print
ISSN 2415–3524 online
Науковий вісник ІФНТУНГ
2024. № 2(57)

Таблиця 1 - Статистика підрозділів, вимог та критеріїв для оцінки веб-сайту інтернет-магазину

Назва розділу	Кількість підрозділів	Кількість вимог	Кількість критеріїв
Authentication	3	12	85
Session Management	4	10	54
Access Control	3	5	43
Validation, Sanitization and Encoding	2	6	57
Data Protection	3	6	52
Files and Resources	2	3	30
Configuration	2	7	44

охоплюють такі аспекти, як "Безпека паролів", "Загальна безпека автентифікатора", " Відновлення облікових даних" тощо.

В основу запропонованої методології покладено розробкусукупності критеріїв для перевірки кожної вимоги та способу їх оцінювання. Для спрощення кожен критерій оцінювався за дискретною шкалою від 0 до 1 з кроком 0,5. Критерії оцінки кожної вимоги формувались таким чином, щоб всебічно здійснити її перевірку, фокусуючи увагу на ключових аспектах захисту.

Таблиця 1 містить перелік відібраних розділів із кількістю вибраних вимог та кількістю побудованих критеріїв для перевірки цих вимог. Оскільки максимальна оцінка кожного критерію - "1", то кількість критеріїв фактично і визначає максимальну кількість балів оцінювання за розділ. Для кожного розділу було визначено максимальну кількість балів, яку можна одержати, оцінюючи всі відібрані вимоги захищеності за допомогою розроблених критеріїв оцінювання до кожної вимоги. Ці бали варіюються залежно від кількості вимог та переліку критеріїв оцінювання для них у кожному розділі.

У межах даного дослідження кожна із відібраних вимог безпеки була структурована відповідно до запропонованої методології, що дозволяє забезпечити чіткість і прозорість процесу оцінювання. Ключовими елементами запропонованого підходу кількісної оцінки веб-сайту є наступні:

– опис вимоги, де детально викладено зміст вимоги та її значення для безпеки вебдодатка;

– формування переліку критеріїв оцінки, що дозволяє перевірити виконання кожної вимоги;

– детальний опис критеріїв оцінки та роз'яснення шкали оцінювання;

– приклад підрахунку по балів для конкретної вимоги;

– Загальний підрахунок балів розділу, який надає кількісну оцінку виконання всіх вимог у межах розділу;

– обчислення відносного показника виконання критеріїв, що виконує роль оцінки захищеності веб-застосунку з даною вимогою.

Така структура дозволяє стандартизувати процес оцінювання та забезпечити його гнучкість для різних типів вебдодатків. Щоб зрозуміти процедуру оцінювання вимог, розглянемо, для прикладу, вимогу: "Переконайтеся, що функціонал зміни пароля вимагає введення поточного та нового пароля.".

Вимога "Переконайтеся, що функціонал зміни пароля вимагає від користувача введення поточного та нового пароля" спрямована на забезпечення безпечного та надійного процесу зміни пароля в системі. Забезпечення цього процесу є важливим елементом загальної безпеки облікових записів користувачів, оскільки він гарантує, що тільки авторизовані користувачі можуть змінювати свої паролі.

Одним із ключових аспектів цієї вимоги є впровадження політики, яка вимагає від користувача введення поточного пароля перед зміною на новий. Це дозволяє переконатися, що зміна пароля ініційована саме власником облікового запису, а не зловмисником. Додатково система повинна перевіряти нові паролі на відповідність вимогам безпеки, таким як довжина, складність і унікальність, щоб мінімізувати ризики використання слабких паролів.

Важливою також є безпека процесу зміни пароля, яка включає використання багатофакторної автентифікації та захист від brute-force атак. Ці заходи забезпечують додатковий рівень захисту, запобігаючи несанкціонованим змінам паролів.

Крім того, вимога охоплює питання моніторингу та аудиту процесу зміни пароля, що дозволяє вчасно виявляти і усувати порушення безпеки. Наявність чіткого механізму для реагування на виявлені порушення є критично ва-

жливою для підтримання високого рівня захисту системи та її користувачів.

Загалом, ця вимога підкреслює важливість забезпечення надійного та безпечного процесу зміни пароля, що включає перевірку поточного пароля, відповідність нового пароля вимогам безпеки, використання багатофакторної автентифікації та регулярний аудит для підтримки високих стандартів безпеки.

Визначення критеріїв оцінки вимоги

Для кількісної оцінки такого аспекту, як забезпечення вимоги введення поточного та нового пароля при зміні пароля, можна розробити систему оцінювання, яка базується на ключових критеріях оцінки вимоги, що визначають дотримання безпекових вимог до процесу зміни пароля.

Оцінювання виконується на основі детальних питань, відповіді на які дозволяють визначити ступінь виконання кожної з вимог. кожен критерій оцінюється за шкалою від 0 до 1, де 0 означає відсутність виконання вимоги, 0,5 — часткове виконання, а 1 — повне виконання вимоги. Нижче наведено конкретні критерії для оцінки вимоги.

1. Політика зміни пароля.

● Чи вимагається введення поточного пароля при зміні пароля?

Цей критерій оцінює, чи система вимагає від користувача ввести поточний пароль перед тим, як дозволити зміну на новий. Це забезпечує захист від несанкціонованої зміни пароля, якщо обліковий запис залишився незаблокованим або відкритим.

0 балів: Введення поточного пароля не вимагається, що знижує безпеку. Приклад: користувач може змінити пароль, не вводячи поточний, що дозволяє будь-кому, хто має доступ до облікового запису, легко змінити пароль без перевірки.

0,5 бала: Введення поточного пароля вимагається, але з певними винятками, або в деяких випадках можна обійти цю вимогу. Приклад: система зазвичай вимагає поточний пароль, але якщо користувач вже авторизований на іншому пристрої, ця вимога може бути пропущена.

1 бал: Введення поточного пароля завжди вимагається для зміни пароля. Приклад: перед тим як користувач може змінити свій пароль, він повинен ввести поточний пароль для підтвердження своєї особи.

● Чи вимагається введення нового пароля при зміні пароля?

Цей критерій оцінює, чи система вимагає від користувача ввести новий пароль для зміни поточного. Це критично важливо для успішної зміни пароля і захисту облікового запису.

0 балів: Введення нового пароля не вимагається, що робить зміну пароля неможливою або безглуздою. Приклад: система дозволяє користувачу змінити пароль без введення нового, залишаючи старий пароль без змін, що створює проблеми з безпекою.

0,5 бала: Введення нового пароля вимагається, але є можливість залишити старий пароль, що знижує ефективність безпеки. Приклад: система дозволяє користувачу ввести той самий пароль, що і раніше, що не забезпечує покращення безпеки.

1 бал: Система завжди вимагає введення нового пароля для зміни поточного. Приклад: при зміні пароля користувач повинен ввести новий пароль, який не збігається зі старим.

2. Виконання вимог політики.

● Чи є механізм перевірки правильності поточного пароля?

Цей критерій оцінює, чи система перевіряє правильність введеного поточного пароля перед зміною на новий. Це необхідно, щоб запобігти несанкціонованій зміні пароля.

0 балів: Перевірка правильності поточного пароля не здійснюється, що дозволяє змінити пароль без підтвердження особи. Приклад: користувач може ввести будь-який пароль, і система дозволить змінити його на новий без перевірки.

0,5 бала: Перевірка здійснюється, але з можливістю обійти цю вимогу, наприклад, через авторизацію на іншому пристрої. Приклад: система перевіряє правильність поточного пароля, але якщо користувач авторизований на іншому пристрої, перевірка може бути пропущена.

1 бал: Система завжди перевіряє правильність поточного пароля перед зміною на новий. Приклад: користувач не може змінити пароль, поки не введе правильний поточний пароль, інакше система видає помилку.

● Чи є механізм для перевірки нових паролів на відповідність вимогам безпеки?

Цей критерій оцінює, чи система перевіряє нові паролі на відповідність політиці безпеки, включаючи вимоги до довжини, складності та інших аспектів.

0 балів: Перевірка нових паролів не здійснюється, що дозволяє встановлювати небезпечні паролі. Приклад: користувач може встановити новий пароль, який не відповідає вимогам до довжини або складності, наприклад, користувач вводить новий пароль: "12345". Система приймає цей пароль, незважаючи на те, що він за-

ISSN 1993–9965 print
ISSN 2415–3524 online
Науковий вісник ІФНТУНГ
2024. № 2(57)

надто короткий і є поширеним шаблоном, який легко зламати. Пароль "password" також приймається системою без зауважень, хоча він є типовим і широко відомим слабким паролем.

0,5 бала: Перевірка здійснюється, але з певними обмеженнями або недоліками, які дозволяють встановити слабкий пароль. Приклад: система перевіряє довжину пароля, але не враховує інші аспекти, такі як використання спеціальних символів або цифр. Користувач вводить пароль "11111111". Система перевіряє довжину пароля (8 символів) і приймає його, але не враховує, що пароль складається з одного повторюваного символу, що робить його слабким. Пароль "password123" приймається, оскільки він містить літери та цифри, але система не вимагає використання спеціальних символів або перевірки на наявність у базах скомпрометованих паролів.

1 бал: Система завжди перевіряє нові паролі на відповідність усім вимогам безпеки. Приклад: при спробі встановити новий пароль, який не відповідає політиці, система видає помилку і вимагає введення більш складного пароля. Користувач намагається встановити пароль "Qwerty123". Система відхиляє його із повідомленням: "Пароль повинен містити принаймні один спеціальний символ, наприклад: @, #, $.". Користувач вводить пароль "12345Password!". Система перевіряє його на наявність у базах скомпрометованих паролів і відхиляє із повідомленням: "Цей пароль використовується в базах зламаних паролів. Будь ласка, виберіть інший". Пароль "Secure@2023!" успішно проходить перевірку, оскільки відповідає всім вимогам: мінімум 12 символів, наявність великих і малих літер, цифр, спеціальних символів та відсутність у базах скомпрометованих паролів.

- Чи є механізм підтвердження зміни пароля через електронну пошту або інший канал зв'язку?

Цей критерій оцінює, чи система надсилає користувачеві підтвердження про зміну пароля через електронну пошту або інший канал зв'язку, щоб повідомити його про зміни в обліковому записі.

0 балів: Підтвердження не надсилається, що може призвести до непоміченої зміни пароля зловмисником. Приклад: користувач не отримує жодного повідомлення після зміни пароля, що дозволяє зловмиснику змінити пароль без відома користувача.

0,5 бала: Підтвердження надсилається, але лише через один канал або з обмеженнями. Приклад: користувач отримує повідомлення про зміну пароля тільки через електронну пошту, але немає можливості налаштувати інші канали зв'язку.

1 бал: Система завжди надсилає підтвердження про зміну пароля через кілька каналів зв'язку, забезпечуючи додатковий рівень безпеки. Приклад: після зміни пароля користувач отримує підтвердження через електронну пошту, SMS або інші налаштовані канали зв'язку.

3. Безпека процесу зміни пароля.

- Чи використовується багатофакторна автентифікація (MFA) під час зміни пароля?

Цей критерій оцінює, чи система використовує багатофакторну автентифікацію для додаткового захисту під час зміни пароля.

0 балів: Багатофакторна автентифікація не використовується, що знижує рівень безпеки. Приклад: користувач може змінити пароль, ввівши лише поточний пароль без додаткової перевірки особи.

0,5 бала: MFA використовується, але не завжди або з певними обмеженнями. Приклад: багатофакторна автентифікація вимагається лише в деяких випадках, наприклад, при зміні пароля з нового пристрою.

1 бал: Багатофакторна автентифікація завжди використовується під час зміни пароля. Приклад: після введення поточного пароля користувач повинен підтвердити свою особу через SMS-код або інший фактор автентифікації.

- Чи є захист від brute-force атак під час зміни пароля?

Цей критерій оцінює, чи система захищена від атак перебору (brute-force) під час спроб зміни пароля.

0 балів: Захист від brute-force атак не передбачений, що дозволяє зловмисникам багаторазово вводити різні паролі. Приклад: користувач може необмежено вводити нові паролі, що дозволяє зловмисникам здійснювати атаки перебору.

0,5 бала: Захист від brute-force атак є, але з обмеженими можливостями або недоліками в реалізації. Приклад: система блокує спроби зміни пароля після кількох невдалих спроб, але цей захист можна обійти, використовуючи різні методи.

1 бал: Система повністю захищена від brute-force атак під час зміни пароля, з обмеженнями на кількість спроб і додатковими заходами безпеки. Приклад: після кількох невдалих спроб зміни пароля система блокує доступ і вимагає додаткову перевірку особи, наприклад, через MFA.

4. Моніторинг та аудит.

● Чи проводиться регулярний аудит для перевірки процесу зміни пароля?

Цей критерій оцінює, чи здійснюється регулярний аудит процесу зміни пароля для виявлення можливих порушень або вразливостей.

0 балів: Аудит процесу зміни пароля не проводиться, що може призвести до не виявлених порушень безпеки. Приклад: компанія не проводить жодних перевірок процесу зміни пароля, що дозволяє існувати вразливостям або іншим проблемам без виявлення.

0,5 бала: Аудит проводиться, але не регулярно або охоплює лише певні аспекти процесу зміни пароля. Приклад: перевірки здійснюються тільки після великих змін у системі, тоді як регулярний аудит відсутній.

1 бал: Регулярний аудит процесу зміни пароля проводиться, що дозволяє виявляти і виправляти можливі порушення безпеки. Приклад: компанія регулярно перевіряє всі аспекти процесу зміни пароля, включаючи журнали подій, щоб виявити і усунути можливі загрози.

● Чи існує механізм для реагування на виявлені порушення у процесі зміни пароля?

Цей критерій оцінює, чи існує механізм для швидкого реагування на виявлені порушення в процесі зміни пароля, щоб запобігти загрозам безпеці.

0 балів: Механізму для реагування на виявлені порушення немає, що може призвести до невжиття заходів у разі виникнення проблем. Приклад: навіть якщо під час аудиту виявляються порушення, компанія не вживає жодних заходів для їх виправлення.

0,5 бала: Механізм існує, але його виконання не обов'язкове або не завжди здійснюється. Приклад: система повідомляє про виявлені порушення, але користувачі або адміністратори можуть відкласти їх виправлення.

1 бал: Існує чіткий механізм реагування, який забезпечує негайне усунення виявлених порушень у процесі зміни пароля. Приклад: якщо виявляється порушення, система автоматично виправляє його або блокує зміну пароля до вирішення проблеми.

Схожим способом було визначено критерії та методи їх оцінювання для кожної вимоги, що дозволило побудувати кількісну систему оцінювання безпеки вебдодатків, яка враховує специфіку кожного із розділів стандарту. Запропонована система оцінювання дозволяє отримати кількісні показники, що відображають рівень виконання вимог захищеності у кожному розділі.

Експериментальна оцінка захищеності веб-сайту "OWASP Juice Shop" для розділу "Автентифікація"

Для забезпечення відповідності нормативно-правовим вимогам і дотримання авторських прав у даному дослідженні застосовано загальновідомий навчальний вебдодаток "OWASP Juice Shop" [12]. Цей ресурс є спеціалізованим середовищем для тестування безпеки, що містить широкий спектр завчасно впроваджених вразливостей та офіційно дозволений для використання в освітніх цілях.

OWASP Juice Shop виступає репрезентативним зразком електронної комерції, оскільки включає всі ключові функціональні можливості, властиві сучасним інтернет-магазинам. Додаток забезпечує управління каталогом продукції з підтримкою пошуку, сортування та детального перегляду товарів, функціонал кошика для маніпуляцій із товарами, а також інтегровані механізми оформлення замовлень. Він підтримує багаторівневу систему доступу, включаючи реєстрацію й авторизацію користувачів із розподілом на ролі (наприклад, звичайний користувач і адміністратор), що реалізовано через впровадження JWT токенів. Серверна частина додатку побудована на фреймворці Node.js, яка забезпечує високу продуктивність і масштабованість, тоді як SQLite використовується для зберігання даних, таких як інформація про товари, користувачів та замовлення. Фронтенд реалізовано за допомогою фреймворку Angular, що дозволяє створювати динамічний та зручний інтерфейс користувача.

Більше того, OWASP Juice Shop спеціально розроблений із впровадженими вразливостями, включаючи SQL-ін'єкції, міжсайтовий скриптинг (XSS) і атаки типу CSRF. Це дозволяє імітувати реальні кіберзагрози, характерні для систем електронної комерції, і розробляти стратегії їх виявлення та нейтралізації. Завдяки підтримці контейнеризації через Docker, додаток забезпечує спрощене налаштування середовища тестування як для локальних, так і для хмарних інфраструктур. Таким чином, OWASP Juice Shop є важливим інструментом для систематичного аналізу ризиків і вивчення принципів забезпечення безпеки у сфері електронної комерції.

Крім того, OWASP Juice Shop дозволяє проводити тестування широкого спектра сценаріїв, включаючи перевірку вразливостей, пов'язаних із недостатньою валідацією даних, використанням застарілого або небезпечного програмного забезпечення, а також некоректною конфігурацією серверної частини. Це за-

ISSN 1993–9965 print ISSN 2415–3524 online Науковий вісник ІФНТУНГ 2024. № 2(57)

безпечує інтеграцію реальних кейсів у навчальний процес.

Додаток також підтримує реалізацію принципу DevSecOps завдяки можливості інтеграції із сучасними інструментами CI/CD. Це дозволяє проводити автоматизоване тестування безпеки на кожному етапі розробки.

У контексті досліджень у сфері кібербезпеки, OWASP Juice Shop надає платформу для емпіричного аналізу ефективності різних методик захисту, включаючи динамічне і статичне тестування, а також застосування гібридних підходів. Такий підхід дозволяє отримати глибше розуміння потенційних ризиків і механізмів їх мінімізації, що є критично важливим для забезпечення стійкості сучасних систем електронної комерції.

Тому з кожного розділу ASVS було відібрано саме ті вимоги захищеності, які користувач може перевірити вручну на даному сайті. Кожна неуспішна перевірка показує про наявність вразливостей того чи іншого типу.

Згідно з визначеними критеріями та детальним описом, можливо провести практичний аналіз веб-сайту на наявність вразливостей, використовуючи його як звичайний користувач. Отримані результати дозволяють виконати кількісну оцінку виявлених вразливостей. Оскільки на сайті реалізовано процес аутентифікації, усі вимоги з цього розділу слід вважати обов'язковими.

Таблиця 2 містить кількісні оцінки вимог, оцінених за розробленими критеріями та загальний показник захисту для розділу " Автентифікація ", який містить три підрозділи та дванадцять безпекових вимог.

Продемонструємо оцінювання вимоги "Verify password credential recovery does not reveal the current password in any way" на сайті "OWASP Juice Shop". Нагадаємо, що кожен критерій має однакову вагу та оцінюється за шкалою від 0 до 1, де 0 означає відсутність реалізації, 0.5 — часткову реалізацію, а 1 — повну реалізацію відповідної функції або механізму безпеки. Виконання цієї вимоги виконувалось за наступними критеріями:

- Чи використовується безпечний метод для відновлення паролів, наприклад, генерація одноразового пароля або токена для скидання?

0 балів: Інтернет-магазин не використовує безпечний метод відновлення паролів, ідентифікуючи поточного користувача лише за відповіддю на секретне питання.

- Чи жодним чином не розкривається поточний пароль під час процесу відновлення?

1 бал: Поточний пароль не розкривається жодним чином під час процесу відновлення, що забезпечує максимальний рівень безпеки.

- Чи використовується двофакторна аутентифікація під час процесу відновлення паролів?

0 балів: 2FA не використовується під час процесу відновлення паролів, що збільшує ризик несанкціонованого доступу.

- Чи повідомлення під час процесу відновлення паролів не містять інформації, яка могла б розкрити поточний пароль?

1 бал: Повідомлення не містять жодної інформації, яка могла б розкрити або підказати поточний пароль, що забезпечує максимальний рівень безпеки.

- Чи існує документована політика, що забороняє розкриття поточного пароля під час відновлення?

0.5 бала: Політика існує, але вона не повністю охоплює всі аспекти процесу відновлення паролів або недостатньо детальна.

Таким чином, сумарно ця вимога отримує 3 бали з 5 можливих.

Цей приклад демонструє, як користувач, що володіє необхідними навичками, може оцінити критерії для кожної вимоги. Отримані оцінки можна підсумувати для визначення загального рівня захисту вебдодатка в межах підрозділів та розділу в цілому. Таким чином, перевіривши та оцінивши кожен критерій, можна провести розрахунок загальної кількості набраних балів по кожній з вимог.

Після отримання кількісної оцінки для кожної вимоги, можна обчислити кількісну оцінку та загальний показник захисту для кожного підрозділу і відповідно розділу. Оцінку захисту для всього розділу, можна отримати як відносний показник набраних за критеріями балів до їх максимально можливої кількості за формулою:

$$S_{розділ} = \frac{actual}{maximum},$$

де *actual* - це сума набраних балів із вимог в розділі, а*maximum* - максимально можлива кількість балів.

Оцінка безпеки автентифікації системи вказує на значні недоліки у забезпеченні належного захисту облікових записів. У підрозділі "Password Security" загальний показник складає лише 24%, що свідчить про низький рівень відповідності сучасним стандартам. Наприклад, вимоги до довжини паролів виконані частково, а функціональність перегляду введеного пароля відсутня. Однак позитивним моментом є середній рівень виконання вимог щодо відсутності

Таблиця 2 – Перелік оцінених вимог за критеріямидля розділу "Authentication"

Підрозділ/ Вимога	Результати оцінювання критеріїв для кожної вимоги			Сума набраних балів / максимальна кількість балів
	0 балів	0,5 бала	1 бал	
Безпека паролів				**14,5/60**
Переконайтеся, що встановлені користувачем паролі мають довжину не менше 12 символів.	5	1	0	0,5/6
Дозволені паролі довжиною щонайменше 64 символи, а паролі понад 128 символів відхиляються.	6	0	0	0/6
Переконайтеся, що обрізання пароля не виконується. Однак кілька підрядкових пробілів можуть бути замінені на один.	5	0	0	0/5
Переконайтеся, що в паролях дозволені будь-які друковані символи Unicode, включаючи нейтральні символи, такі як пробіли та емодзі.	4	2	1	2/7
Користувачі можуть змінювати свій пароль.	5	2	1	2/8
Переконайтеся, що функціонал зміни пароля вимагає введення поточного та нового пароля користувачем.	5	1	3	3,5/9
Переконайтеся, що немає правил складу пароля, які обмежують тип дозволених символів.*	4	1	6	6,5/11
Переконайтеся, що користувач може вибрати тимчасово переглянути весь прихований пароль або тимчасово побачити останній введений символ пароля на платформах, де ця функція не є вбудованою.	8	0	0	0/8
Загальна безпека автентифікатора				**3/15**
Засоби проти автоматизації ефективно знижують ризик тестування зламаних облікових даних, атак методом грубої сили та атак блокування облікового запису.**	9	0	0	0/9
Безпечні повідомлення надсилаються користувачам після оновлення даних автентифікації, таких як скидання облікових даних, зміни електронної пошти або адреси, входу з невідомих або ризикованих локацій.***	2	2	2	3/6
Відновлення облікових даних				**2,5/10**
Підказки до пароля або аутентифікація на основі знань (так звані "таємні питання") відсутні.	5	0	0	0/5
Переконайтеся, що відновлення облікових даних пароля жодним чином не розкриває поточний пароль.	2	1	2	2,5/5

*Не повинно бути вимог щодо використання великих чи малих літер, чисел або спеціальних символів.

**Такі заходи включають блокування найбільш поширених зламаних паролів, м'які блокування, обмеження швидкості, CAPTCHA, постійно зростаючі затримки між спробами, обмеження за IP-адресою або обмеження на основі ризику, такі як локація, перший вхід на пристрій, нещодавні спроби розблокувати акаунт чи подібне. Переконайтеся, що на одному акаунті неможливо зробити більше ніж 100 невдалих спроб за годину.

***Використання push-сповіщень - замість SMS або електронної пошти - є переважним, але в разі відсутності push-сповіщень, SMS чи електронна пошта є прийнятними, якщо в повідомленні не розкривається чутлива інформація.

ISSN 1993–9965 print
ISSN 2415–3524 online
Науковий вісник ІФНТУНГ
2024. № 2(57)

Таблиця 3 – Результати розрахунків оцінки захищеності для кожного з розділів

Розділ	Розподіл балів за критеріями для кожної вимоги			Сума набраних балів за розділом	Максимальна кількість балів за розділом	Відносний показник захисту за розділом
	0 балів	0,5 бала	1 бал			
Автентифікація	60	8	15	20	85	$0,24 = \frac{20}{85}$
Управління сесіями	46	4	4	6	54	$0,11 = \frac{6}{54}$
Контроль доступу	34	16	3	18,5	43	$0,43 = \frac{18,5}{43}$
Валідція, санітизація та кодування	39	17	1	9,5	57	$0,17 = \frac{9,5}{57}$
Захист даних	34	12	5	11	52	$0,21 = \frac{11}{52}$
Файли та ресурси	21	9	2	4,5	30	$0,15 = \frac{4,5}{30}$
Конфігурація	27	11	6	11,5	44	$0,26 = \frac{11,5}{44}$

обмежень на склад паролів (59%), що дозволяє використовувати символи Unicode, включаючи пробіли та емодзі. Підрозділи "General Authe?ticator Security" та "Credential Recovery" також демонструють невисокий рівень захисту з показниками 20% і 35% відповідно. Недостатня ефективність контролю автоматизованих атак, таких як brute force або використання викрадених облікових даних, становить значну загрозу. Водночас, певний прогрес спостерігається у вимогах щодо безпечного сповіщення користувачів після змін аутентифікаційних даних (50%) та захисту процесу відновлення облікових записів, наприклад, через заборону відображення поточного пароля (60%). Загалом, результати оцінювання свідчать про необхідність значних покращень у всіх аспектах автентифікації, особливо в частині забезпечення мінімальних стандартів захисту паролів і впровадження ефективних механізмів протидії атакам.

На основі розробленого алгоритму розрахунку оцінки захищеності і застосованого для розділу "Authentication", можна продовжувати розрахунок кожного наведеного розділу, згаданого вище в таблиці 2.

Таблиця 3 містить результати розрахунків оцінки захищеності для кожного з розділів, де відображено загальну кількість набраних балів та максимально допустиму кількість набраних балів, а також відносний показник захисту для розділу.

На основі цієї таблиці можна зробити оцінку веб-сайту за відібраними розділами та вимогами відповідно. Найнижчі показники виявлено в категоріях "Управління сесіями" (0,11), "Файли та ресурси" (0,15) та "Валідція, санітизація та кодування" (0,17). Це свідчить про серйозні ризики, пов'язані з можливим викраденням сесій, некоректною обробкою даних і завантажених файлів, що може стати джерелом атак типу SQL-ін'єкцій, XSS або зловмисного виконання коду. Категорія "Контроль доступу" показала відносно вищий результат (0,43), однак навіть тут існує значний простір для вдосконалення. Загалом, отримані результати свідчать про низький рівень впровадження безпекових практик. Веб-сайт потребує масштабних доопрацювань, включаючи покращення механізмів автентифікації, посилення захисту конфіденційних даних та усунення вразливостей у системах обробки даних і конфігурації. Це підкреслює важливість комплексного підходу до забезпечення кібербезпеки.

Запропонована методологія кількісної оцінки захищеності вебдодатків є певною альтернативою автоматизованим сканерам, які орієнтовані на ідентифікацію вразливостей на основі рекомендацій CWE та визначених сценаріїв. Сканери проводять аналіз у повністю автоматичному режимі, вимагаючи від користувача лише ініціювати процес сканування. Натомість розроблена методологія спрямована на ручне

тестування, що забезпечує детальніший аналіз. Автори дослідження [13] тестували ефективність різних сканерів з використанням середовища "OWASP Juice Shop". Слід зазначити, що кількість та зміст знайдених вразливостей можуть змінюватись в залежності від використаного інструменту. Автори дослідження дійшли висновку, що краще застосовувати кілька сканерів і не запропонували однозначних критеріїв їх порівняння. Адже сканер, який виявив максимальну кількість вразливостей, не знайшов багатьох критичних вразливостей, а більшість зі знайдених вразливостей виявилась інформаційного характеру. В той самий час, інструмент, що знайшов відносно невелику кількість вразливостей, мав вищий рівень виявлення критичних вразливостей. Запропонована методологія пропонує уніфікований підхід до оцінки захищеності вебдодатків, охоплює детальний перелік критеріїв та забезпечує глибокий аналіз. Методологія також надає точні рекомендації щодо захисту додатка за кожним критерієм, тоді як сканери здебільшого пропонують загальні рішення для усунення вразливостей. Таким чином, методологічний підхід дозволяє враховувати специфічні аспекти роботи додатка, які можуть залишитися поза увагою автоматизованих сканерів.

Висновки та перспективи подальшого дослідження

Запропонована методика кількісної оцінки рівня захищеності вебдодатків на основі стандарту OWASP ASVS демонструє об'єктивність та практичну корисність у реальних умовах. Цей підхід дозволяє отримати кількісну оцінку рівня захищеності вебдодатків електронної комерції на етапі експлуатації. Методологія ґрунтується на чітко структурованому наборі вимог, що охоплюють широкий спектр аспектів безпеки, починаючи від автентифікації користувачів і управління сесіями, до захисту від атак та належного зберігання конфіденційної інформації. Побудована авторами система критеріїв для перевірки кожної вимоги охоплює повною мірою тестування вимоги і дозволяє створити уніфіковану систему для тестування безпеки веб-сайту електронної комерції за умови відсутності технічної документації. Кількісні показники оцінки критеріїв не лише відображають поточний стан веб-сайту, а й є інструментом для систематичного аналізу впроваджених заходів безпеки.

Однак, слід зауважити, що дана методика може отримати подальший розвитокз врахуванням специфіки різних вебдодатків, особливо в контексті варіативності наборів вимог до безпеки. Різні вебдодатки мають різну архітектуру та функціональність, що визначає їх потреби у захисті. Наприклад, вебдодатки, які не використовують API-інтерфейси, не повинні отримувати знижені оцінки за відсутність впровадження вимог до API, адже ці вимоги для них є нерелевантними. Перед тим як розпочати процес оцінювання, необхідно здійснити попередній аналіз вебдодатка користувача з метою визначення його архітектурних особливостей і функціональних характеристик. Цей етап дозволить коректно сформувати набір вимог до безпеки, що відповідає специфіці конкретного вебдодатка. Очевидно, що в залежності від складності додатку для його тестування може бути застосована різна кількість вимог. Тому актуальним є питання розширення запропонованого підходу шляхом створення адаптивної системи оцінювання, яка передбачає індивідуалізацію вимог для кожного вебдодатка.

Проте, важливо враховувати не лише технічні характеристики вебдодатків, але й їхній бізнес-контекст, вимоги до конфіденційності та критичність захисту даних. Адаптивний підхід до оцінювання дозволить також краще враховувати специфіку різних галузей застосування вебдодатків. Наприклад, у фінансових або медичних системах окремі вимоги до безпеки можуть мати підвищену важливість, тоді як для стандартних комерційних вебдодатків такі вимоги можуть бути менш критичними. Індивідуалізація процесу оцінювання на ранньому етапі також дозволить отримати більш точні результати для подальшого вдосконалення безпеки, зокрема визначити конкретні зони ризику та сконцентрувати увагу на найбільш вразливих аспектах.

Отже, впровадження адаптивної моделі оцінювання, яка враховує специфіку вебдодатків, є важливим кроком у підвищенні точності та об'єктивності оцінювання захищеності вебдодатків. Такий підхід дозволить уникнути помилкових знижень загального коефіцієнта безпеки для додатків, які не використовують певні технології або функції, й, навпаки, забезпечить фокус на найбільш критичних аспектах для кожного конкретного вебдодатка.

Подальший розвиток запропонованої методики також можливий шляхом розширення сфери її застосування на різних етапах життєвого циклу вебдодатку: як на стадії розробки, так і під час його експлуатації. Вчасне виявлення та усунення вразливостей на ранніх етапах дозволяє значно знизити витрати на розробку та підтримку, а також мінімізувати ризики для бізнесу.

ISSN 1993–9965 print ISSN 2415–3524 online
Науковий вісник ІФНТУНГ 2024. № 2(57)

Література / References

1. Parishev A., Hristovski G., Jolakoski P., Stojkoski V. E. Commerce impact on economic growth. *1st International Scientific Conference "Economic and Business Trends Shaping the Future" (EBTSF-20)*, Skopje, 12-13 November 2020. P. 188-198. URL: https://repository.ukim.mk/bitstream/20.500.12188/9682/1/EBTSF-20_paper_16.pdf

2. Cao M. Competitive Advantages and Challenges of E-Commerce. *Advances in Economics, Management and Political Sciences*. 2023. 47. P.114-119. DOI: https://doi.org/10.54254/2754-1169/47/20230380

3. Saleh H., Rezk A., Barakat S. The impact of cyber crime on e-commerce. *International Journal of Intelligent Computing and Information Science*. 2017. Vol. 17, No. 3, P. 85-96. DOI: https://doi.org/10.21608/ijicis.2017.30055

4. Aldya A. P., Sutikno S., Rosmansyah Y. Measuring effectiveness of control of information security management system based on SNI ISO/IEC 27004:2013 standard. *IOP Conf. Series: Materials Science and Engineering*. 2019. 550 012020. DOI: https://doi.org/10.1088/1757-899X/550/1/012020

5. Lundholm K., Hallberg J., Granlund H. Design and use of information security metrics : application of the ISO/IEC 27004 standard. Scientific report FOI-R--3189—SE. FOI-Swedish Defence Research Agency, 2011. 57 p.

6. ISO/IEC. Information technology — Security techniques — Code of practice for information security controls. International Organization for Standardization, 2013. URL: https://webstore.iec.ch/en/publication/11288

7. Buccafurri F., Fotia L., Furfaro A., Garro A., Giacalone M., Tundis A. An analytical proce-?sing approach to supporting cyber security compliance assessment. *Proceedings of the 8th International Conference on Security of Information and Networks (SIN '15)*. Association for Computing Machinery, New York, NY, USA, 201546–53. DOI: https://doi.org/10.1145/2799979.2800007

8. Data Security Standard: Attestation of Compliance for Self-Assessment Questionnaire A. PCI Security Standards Council, 2013. URL: https://listings.pcisecuritystandards.org/documents/AOC-SAQ_A-v3_2-rev1_1.pdf

9. Disanayake C., Dilhara S., Dharmaratna N. S. Rationalized security frameworks for web applications. *Annual International Conference on Business Innovation (ICOBI)*. 2023. Volume 1, P.532-544. URL: https://nsbm.ac.lk/icobi/proceedings/icobi2023-proceedings-volume1.pdf#page=562

10. CWE – Common Weakness Enumeration. URL: https://cwe.mitre.org/ (accesed 06.02.2025)

11. OWASP Application Security Verification Standard (ASVS). 2021. URL: https://owasp.org/www-project-application-security-verification-standard

12. OWASP Juice Shop. URL: https://owasp.org/www-project-juice-shop/ (accesed 06.02.2025)

13. Tryhubets B., Tryhubets M., Zagorodna N. Analysis of the efficiency of open source and commercial vulnerability scanners for e-commerce web applications. *Scientific Journal of the Ternopil National Technical University*. 2024. Vol. 116. No. 4. P. 23–30. DOI: https://doi.org/10.33108/visnyk_tntu2024.04.023