International Science Group

ISG-KONF.COM

IX

INTERNATIONAL SCIENTIFIC AND PRACTICAL CONFERENCE "SCIENTISTS AND EXISTING PROBLEMS OF HUMAN DEVELOPMENT"

Zagreb, Croatia

November 14-17, 2023

ISBN 979-8-89238-621-0

DOI 10.46299/ISG.2023.2.9

SCIENTISTS AND EXISTING PROBLEMS OF HUMAN DEVELOPMENT

Proceedings of the IX International Scientific and Practical Conference

Zagreb, Croatia
November 14-17, 2023

UDC 01.1

The 9th International scientific and practical conference “Scientists and existing problems of human development” (November 14-17, 2023) Zagreb, Croatia. International Science Group. 2023. 426 p.

ISBN – 979-8-89238-621-0
DOI – 10.46299/ISG.2023.2.9

РОЗРОБКА СКАНЕРА ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ ВЕБСАЙТУ НА ОСНОВІ МЕТОДІВ ЗАХИСТУ ВІД РІЗНИХ ТИПІВ АТАК

Лопатінський Андрій,
здобувач вищої освіти кафедри інформатики
Харківський національний університет радіоелектроніки

У сучасному цифровому віці, вебсайти відіграють ключову роль у функціонуванні бізнесу, урядових структур, освітніх установ та повсякденному житті людей. Вони є не тільки вітриною для бізнесу в Інтернеті, але й засобом комунікації, обміну інформацією та надання послуг. Важливість вебсайтів у сучасному світі не може бути переоцінена, але разом з їх зростаючою роллю зростає і ризик кіберзагроз.

Безпека вебсайтів стає все більш критичним аспектом у управлінні цифровими активами. Кіберзлочинці постійно розвивають нові методи атаки, використовуючи вразливості в коді, конфігурації серверів та інші слабкі місця для здійснення несанкціонованого доступу, крадіжки даних або навіть повного контролю над ресурсами. На додачу до прямих фінансових втрат, такі інциденти можуть призвести до втрати репутації, довіри клієнтів та правових наслідків.

З цієї причини, розуміння сучасних кіберзагроз та розробка ефективних стратегій захисту є необхідністю для будь-якої організації, що володіє вебресурсами. Це включає в себе не тільки технічні заходи, такі як застосування сканерів вразливостей, але й стратегічне планування, навчання персоналу та розробку комплексних планів реагування на інциденти.

Ключ до ефективного захисту вебсайтів полягає не тільки в технологіях, а й у глибокому розумінні потенційних загроз та методів їх нейтралізації. Це означає, що забезпечення безпеки вебсайтів вимагає постійного моніторингу, аналізу, оновлення систем безпеки та адаптації до постійно змінюваних умов кіберпростору. Освіченість та спеціальний підхід до кібербезпеки можуть значно знизити ризик та забезпечити надійний захист важливих цифрових активів.

Сканери вразливостей вебсайтів – це спеціалізовані інструменти, призначені для автоматичного виявлення потенційних слабких місць у вебзастосунках. Вони аналізують вебсайти, шукаючи відомі вразливості, такі як проблеми з конфігурацією, застаріле програмне забезпечення, вразливості у коді або неправильні налаштування безпеки. Цей процес дозволяє виявити і усунути потенційні загрози, перш ніж вони будуть використані зловмисниками [1-5].

Типи сканерів:

– активні сканери: відправляють активні запити до вебсайту для виявлення вразливостей;

– пасивні сканери: аналізують трафік, що проходить через вебсайт, для виявлення можливих вразливостей без відправлення власних запитів;

– гібридні сканери: поєднують в собі активні та пасивні методи сканування для більш глибокого аналізу.

Сканування зазвичай включає в себе кілька етапів:

– збір інформації. Визначення активних сервісів, відкритих портів, використовуваних технологій;

– аналіз вразливостей. Використання бази даних відомих вразливостей для порівняння з зібраною інформацією;

– випробування. Проведення тестів для перевірки підозрілих місць;

– генерація звітів. Створення детальних звітів з переліком знайдених вразливостей та рекомендаціями щодо їх усунення.

Сканери вразливостей часто інтегруються з іншими системами безпеки, такими як системи виявлення та запобігання вторгненням (IDS/IPS), системи управління безпекою інформації (SIEM) та іншими інструментами моніторингу для забезпечення комплексного підходу до захисту вебсайтів [6-10].

Оскільки нові вразливості та методи атак постійно розробляються, важливо регулярно оновлювати сканери вразливостей. Це включає оновлення бази даних вразливостей, а також покращення алгоритмів та методів сканування.

Сканери вразливостей є лише одним інструментом у широкому спектрі заходів безпеки. Вони повинні використовуватися разом з іншими стратегіями та практиками, такими як кодування з безпекою, регулярне оновлення та патчі, суворе управління доступом, резервне копіювання та відновлення, а також навчання персоналу з питань кібербезпеки.

До найбільш поширених вразливостей належать SQL Injection, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF) та інші. Ці вразливості можуть призвести до несанкціонованого доступу до даних, зміни контенту вебсайту, або навіть повного контролю над вебресурсом [11-15].

Крім вказаних вище загроз, існують інші не менш серйозні вразливості, такі як Server-Side Request Forgery (SSRF), XML External Entity (XXE) атаки та багато інших, які можуть спричинити серйозний ризик для безпеки вебсайту. Мій дослідницький проект спрямований на створення ефективного сканера для виявлення цих вразливостей та розробку рекомендацій зі зменшення їхнього потенційного впливу на вебресурси. Безпека вебсайту – це важливий аспект в сучасному інтернет-середовищі, робота спрямована на забезпечення надійного захисту від різних видів атак.

З огляду на збільшення кількості та складності кібератак, захист вебсайтів від потенційних загроз є критично важливим. Виявлення та усунення вразливостей є ключовим для запобігання втратам даних та збереження репутації компаній. В той же час, швидке розвиток кіберзагроз вимагає постійного оновлення та вдосконалення сканерів вразливостей.

Розробка дослідження розпочалася з визначення основних цілей, серед яких розробка ефективного сканера вразливостей та глибокий аналіз методів захисту. Проведено огляд наявних на ринку рішень, що дозволило зрозуміти, які інструменти та методики вже використовуються та які їхні переваги та недоліки.

На рисунку 1 представлено структуру вебсканера вразливостей.

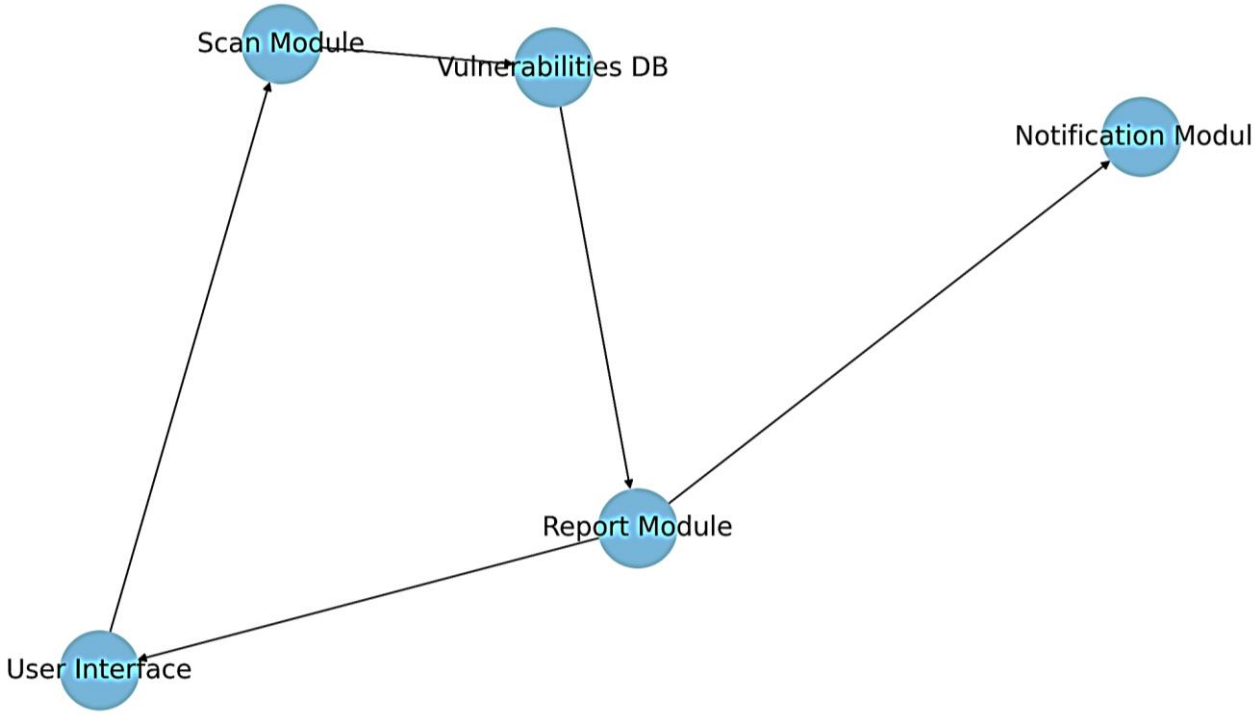

Рисунок 1 – Структура вебсканера вразливостей

Компоненти програми відображені як вузли, а їх взаємозв'язки – стрілками, що показують напрямок взаємодії між цими компонентами:

– User Interface (інтерфейс користувача). Точка входу для користувачів, де вони можуть вводити дані для сканування та переглядати звіти;

– Scan Module (модуль сканування). Відповідає за процес сканування вебсайтів на наявність вразливостей;

– Vulnerabilities DB (база даних вразливостей). Зберігає інформацію про відомі вразливості та способи їх виявлення;

– Report Module (модуль звітів). Генерує звіти про результати сканування;

– Notification Module (модуль повідомлень). Відправляє сповіщення користувачам про стан сканування або виявлені вразливості.

На основі зібраної інформації було розроблено прототип сканера вразливостей, використовуючи відкриті технології та інноваційні підходи. Прототип був протестований на низці вебсайтів з різними архітектурами та конфігураціями, що дозволило перевірити його ефективність у різних умовах.

Після розробки прототипу сканера вразливостей, провели його детальне тестування, включаючи внутрішні та зовнішні аудити, для перевірки його функціональності та надійності. Проведено тестування з використанням реальних атак, щоб оцінити його здатність виявляти та запобігати атакам в реальному часі.

Крім того, постійно вдосконалювали сканер, додаючи нові сигнатури та алгоритми виявлення вразливостей, оновлюючи його базу даних з відомими атаками та розробниками програмного забезпечення, щоб завжди бути на кроці перед новими загрозами. Наш підхід до розробки та тестування сканера дозволяє

забезпечити високий рівень захисту для вебсайтів у різних умовах та середовищах.

Після завершення тестування було проведено детальний аналіз отриманих результатів (рис. 2). Це допомогло виявити основні сильні та слабкі сторони розробленого прототипу, а також надало важливі напрямки для подальшого вдосконалення та оптимізації інструменту.

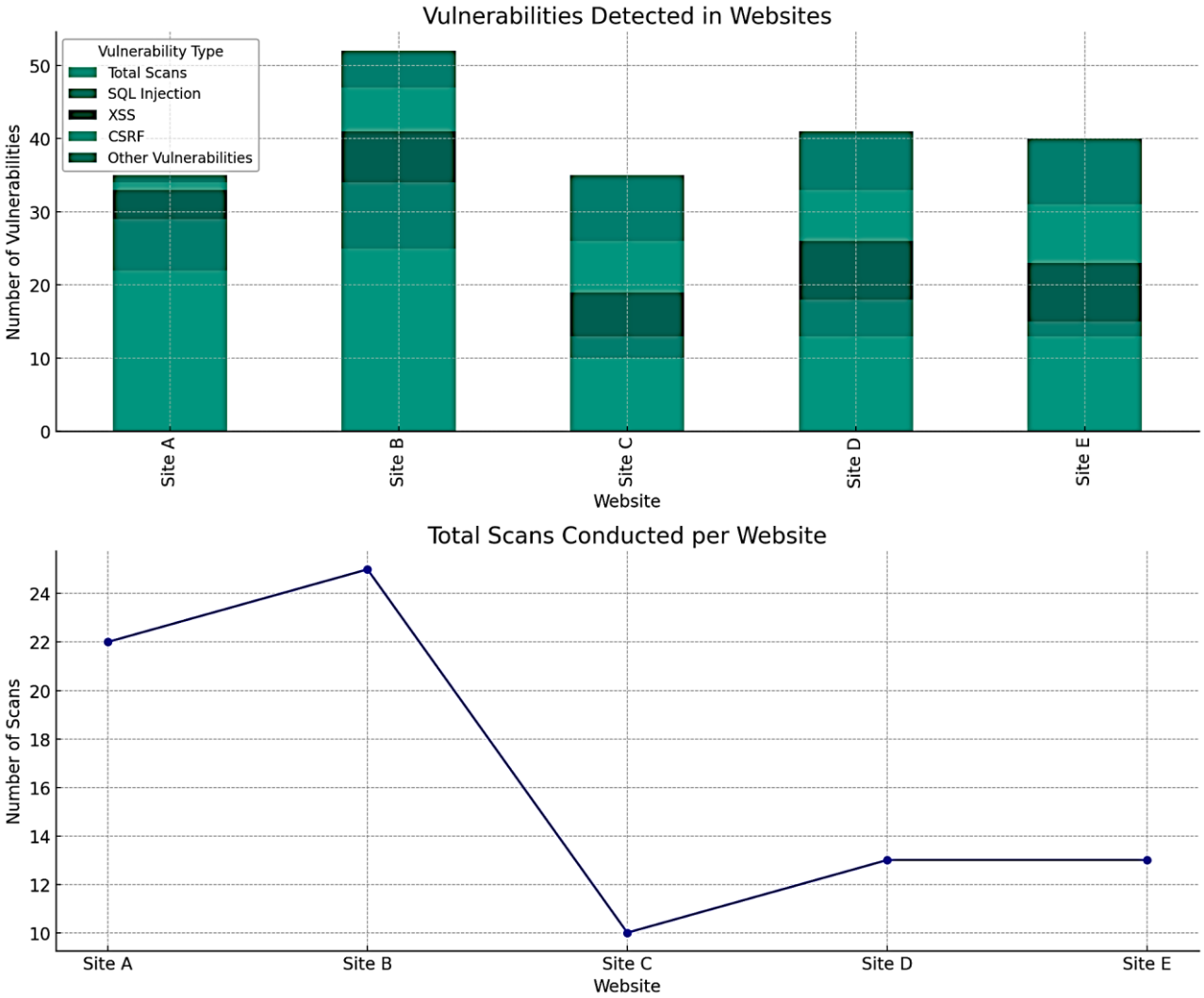

Рисунок 2 – Візуалізація результату тестування вебсайтів

Діаграма відображає кількість виявлених вразливостей різних типів на кожному вебсайті.

Типи вразливостей включають SQL Injection, XSS (Cross-Site Scripting), CSRF (Cross-Site Request Forgery), та інші вразливості. Це допомагає визначити, які вебсайти більш схильні до певних видів атак [16, 17].

Лінійна діаграма показує загальну кількість сканувань, проведених для кожного вебсайту. Ця інформація може бути використана для аналізу частоти сканувань та оцінки необхідності збільшення періодичності перевірок безпеки.

Після завершення тестування було проведено детальний аналіз отриманих результатів. Це допомогло виявити основні сильні та слабкі сторони

розробленого прототипу, а також надало важливі напрямки для подальшого вдосконалення та оптимізації інструменту.

Дослідження охопило широкий спектр методів захисту вебсайтів, системи виявлення та запобігання вторгненням, а також різноманітні техніки кодування та шифрування даних. Особливу увагу було приділено аналізу сучасних тенденцій та інновацій у цій сфері, включаючи застосування машинного навчання та штучного інтелекту [18-28].

У дослідженні розглядалися методи моніторингу вебсайту, такі як сканування вразливостей, відстеження змін в коді та виявлення незвичних патернів активності, що дозволяють вчасно реагувати на атаки та інциденти безпеки. Також розглядалися підходи до аудиту безпеки вебзастосунків та систем, включаючи пентестинг, що допомагає ідентифікувати слабкі місця та потенційні вразливості.

У дослідженні вивчалася важливість навчання та підвищення обізнаності персоналу щодо безпеки вебсайту, а також впровадження політик керування доступом та автентифікації користувачів, щоб попередити несанкціонований доступ до системи. Всі ці методи та техніки були враховані при розробці сканера вразливостей та рекомендаціях щодо підвищення безпеки вебсайтів у сучасному кібернетичному середовищі.

Ці методи були протестовані на вебсайтах з різними виявленими уразливостями. Це дозволило оцінити ефективність кожного методу у реальних умовах. Результати тестування можна побачити на рисунку 3.

Діаграма відображає кількість атак на вебсайти до та після впровадження методів захисту. Кольори показують порівняння між «загальною кількістю атак до» (світло-блакитний) та «загальною кількістю атак після» (салатовий) впровадження захисних методів. Це дає можливість оцінити загальну ефективність заходів безпеки, впроваджених на кожному вебсайті.

Лінійна діаграма показує відсоткову ефективність захисних методів для кожного вебсайту. Високий відсоток ефективності вказує на те, що впроваджені методи захисту значно знизили кількість успішних атак.

Ці візуалізації надають корисну інформацію про ефективність різних методів захисту вебсайтів, що дозволяє проводити аналіз безпеки та планувати подальші заходи для зміцнення захисту вебресурсів.

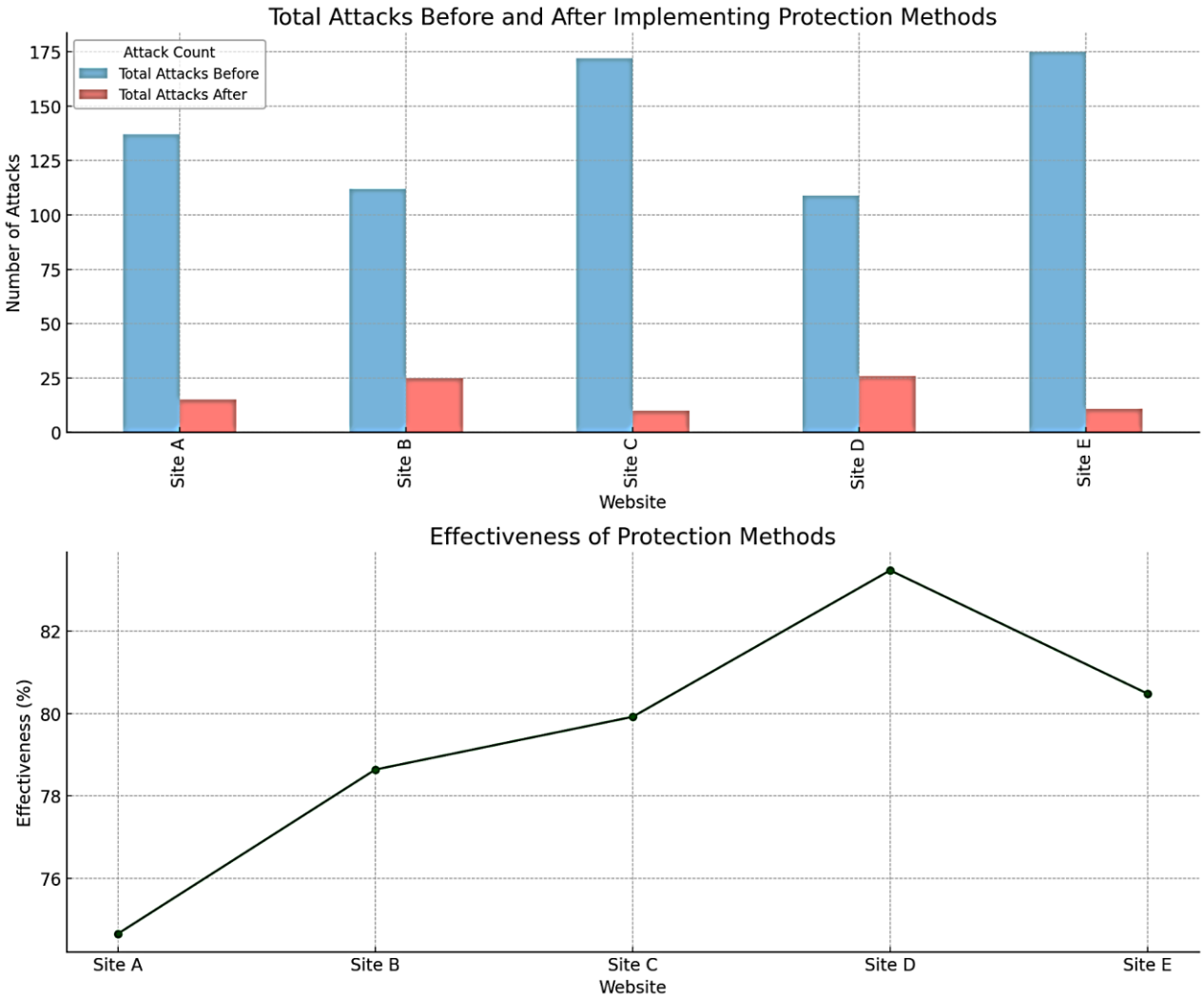

Рисунок 3 – Метрики та результати тестування ефективності методів захисту вебсайтів

На основі аналізу було розроблено комплексний набір рекомендацій для захисту вебсайтів. Ці рекомендації включають кращі практики, стратегії, а також конкретні технічні рішення, які можуть бути застосовані розробниками та адміністраторами для підвищення безпеки їхніх вебресурсів:

– регулярне оновлення та підтримка:

1) оновлення системи: регулярно оновлювати всі компоненти системи, включаючи серверне програмне забезпечення, CMS (системи управління контентом), плагіни та шаблони;

2) патчі безпеки: швидко застосовувати патчі безпеки, як тільки вони стають доступними;

– захист від SQL Injection:

1) параметризовані запити: використовувати параметризовані запити для запобігання вставці шкідливого коду в SQL запити;

2) ORMs (Object-Relational Mapping): розглянути використання ORMs, які забезпечують додатковий рівень абстракції та безпеки;

– захист від Cross-Site Scripting (XSS):

1) валідація вводу: строга валідація всіх вводів користувачів, особливо тих, що виводяться на сторінці;

2) сучасні бібліотеки: використовувати бібліотеки та фреймворки, які автоматично забезпечують захист від XSS;

– захист від Cross-Site Request Forgery (CSRF):

1) токени CSRF: використовувати токени CSRF для забезпечення, що запити до сервера відправляються з довіреної клієнтської сесії;

2) SameSite Cookies: налаштувати атрибути SameSite для куків для зменшення ризику CSRF;

– управління правами доступу:

1) обмеження доступу: надавати доступ до адміністративних функцій тільки необхідним користувачам;

2) сильні паролі та аутентифікація: використовувати сильні паролі та багаторівневу аутентифікацію;

– захист мережі:

1) Firewall (Міжмережевий Екран): налаштування міжмережевих екранів для блокування небажаного трафіку;

2) шифрування: використовувати HTTPS для шифрування даних, що передаються між користувачем і сервером;

– регулярне резервне копіювання:

1) автоматизоване резервне копіювання: налаштувати регулярні автоматизовані резервні копії всіх важливих даних;

2) перевірка резервних копій: періодично тестувати резервні копії на можливість відновлення;

– Моніторинг та відповідь на інциденти:

1) системи моніторингу: встановлення систем моніторингу для виявлення та оповіщення про підозрілу активність;

2) план відповіді на інциденти: розробка та імплементація чіткого плану відповіді на інциденти безпеки;

– Освіта та тренінги:

1) підвищення обізнаності: проведення регулярних тренінгів та семінарів з безпеки для персоналу;

2) оновлення знань: слідкувати за останніми тенденціями у кібербезпеці та адаптувати стратегії відповідно.

Ці рекомендації є фундаментом для забезпечення високого рівня безпеки вебсайтів та захисту від різноманітних кіберзагроз. Вони повинні регулярно переглядатися та оновлюватися, щоб відповідати змінам у технологіях та тактиках кіберзлочинців.

Список літератури:

1. Long, H. V., Tuan, T. A., Taniar, D., Can, N. V., Hue, H. M., & Son, N. T. K. (2020). An efficient algorithm and tool for detecting dangerous website vulnerabilities. International Journal of Web and Grid Services, 16(1), 81-104.

2. Muscat, I. (2016). Web vulnerabilities: identifying patterns and remedies. Network Security, 2016(2), 5-10.

3. Dua, M., & Singh, H. (2017, October). Detection & prevention of website vulnerabilities: Current scenario and future trends. In 2017 2nd International Conference on Communication and Electronics Systems (ICCES) (pp. 429-435). IEEE.

4. Appiah, V., Nti, I. K., & Nyarko-Boateng, O. (2017). Investigating websites and web application vulnerabilities: Webmaster's perspective. Int. J. Appl. Inf. Syst, 12(3), 1015.

5. Henri, S., García, G., Serrano, P., Banchs, A., & Thiran, P. (2020). Protecting against website fingerprinting with multihoming. Proceedings on Privacy Enhancing Technologies, 2020(2), 89-110.

6. Ponta, S. E., Plate, H., Sabetta, A., Bezzi, M., & Dangremont, C. (2019, May). A manually-curated dataset of fixes to vulnerabilities of open-source software. In 2019 IEEE/ACM 16th International Conference on Mining Software Repositories (MSR) (pp. 383-387). IEEE.

7. Alghawazi, M., Alghazzawi, D., & Alarifi, S. (2022). Detection of sql injection attack using machine learning techniques: a systematic literature review. Journal of Cybersecurity and Privacy, 2(4), 764-777.

8. Tang, P., Qiu, W., Huang, Z., Lian, H., & Liu, G. (2020). Detection of SQL injection based on artificial neural network. Knowledge-Based Systems, 190, 105528.

9. Chen, D., Yan, Q., Wu, C., & Zhao, J. (2021). Sql injection attack detection and prevention techniques using deep learning. In Journal of Physics: Conference Series (Vol. 1757, No. 1, p. 012055). IOP Publishing.

10. Likaj, X., Khodayari, S., & Pellegrino, G. (2021, October). Where we stand (or fall): An analysis of CSRF defenses in web frameworks. In Proceedings of the 24th International Symposium on Research in Attacks, Intrusions and Defenses (pp. 370-385).

11. Khodayari, S., & Pellegrino, G. (2021). {JAW}: Studying Client-side {CSRF} with Hybrid Property Graphs and Declarative Traversals. In 30th USENIX Security Symposium (USENIX Security 21) (pp. 2525-2542).

12. Calzavara, S., Conti, M., Focardi, R., Rabitti, A., & Tolomei, G. (2019, June). Mitch: A machine learning approach to the black-box detection of CSRF vulnerabilities. In 2019 IEEE European Symposium on Security and Privacy (EuroS&P) (pp. 528-543). IEEE.

13. Arshad, E., Benolli, M., & Crispo, B. (2022). Practical attacks on Login CSRF in OAuth. Computers & Security, 121, 102859.

14. Rodríguez, G. E., Torres, J. G., Flores, P., & Benavides, D. E. (2020). Cross-site scripting (XSS) attacks and mitigation: A survey. Computer Networks, 166, 106960.

15. Kumar, S., Pathak, S. K., & Singh, J. (2022). A Comprehensive Study of XSS Attack and the Digital Forensic Models to Gather the Evidence. ECS Transactions, 107(1), 7153.

16. Kumar, S., Pathak, S., & Singh, J. (2022). An enhanced digital forensic investigation framework for XSS attack. Journal of Discrete Mathematical Sciences and Cryptography, 25(4), 1009-1018.

17. Liu, M., Zhang, B., Chen, W., & Zhang, X. (2019). A survey of exploitation and detection methods of XSS vulnerabilities. IEEE access, 7, 182004-182016.

18. Гороховатский В.А., Передрий Е.О. (2009) Корреляционные методы распознавания изображений путем голосования систем фрагментов. *Радіоелектроніка, інформатика, управління*, №1 (20), с.74-81.

19. Gadetska S., Gorokhovatskyi V., Stiahlyk N., Vlasenko N. (2022) Aggregate Parametric Representation of Image Structural Description in Statistical Classification Methods. *In CEUR Workshop Proceedings: Computer Modeling and Intelligent Systems (CMIS-2022)*, 3137, pp. 68-77.

20. Гороховатський В., Творошенко І., Сидоренко Д. (2021) Класифікація зображень із використанням кластерного подання, *Міжн. наук. симпозіум Інтелектуальні рішення-С. Обчислювальний інтелект. Теорія прийняття рішень: праці міжн. наук. симп. (Вересень 29, 2021)*. Київ – Ужгород, С. 44-45.

21. Pomazan V., Tvoroshenko I., and Gorokhovatskyi V. (2023) Development of an application for recognizing emotions using convolutional neural networks, *International Journal of Academic Information Systems Research*, 7(7), pp. 25-36.

22. Pomazan V., Tvoroshenko I., and Gorokhovatskyi V. (2023) Handwritten character recognition models based on convolutional neural networks, *International Journal of Academic Engineering Research*, 7(9), 64-72.

23. Gorokhovatskyi V., Tvoroshenko I. (2023) Identification of visual objects by the search request. *International scientific symposium «INTELLIGENT SOLUTIONS-S». Computational intelligence (results, problems and perspectives). Decision making theory: proceedings of the international symposium*, September 28, 2023, Kyiv-Uzhorod, Ukraine, pp. 25-27.

24. Tvoroshenko I., Gorokhovatskyi V., Kobylin O., and Tvoroshenko A. (2023) Application of deep learning methods for recognizing and classifying culinary dishes in images, *International Journal of Academic and Applied Research*, 7(9), pp. 57-70.

25. Daradkeh Y.I., Gorokhovatskyi V., Tvoroshenko I., and Zeghid M. (2022) Tools for fast metric data search in structural methods for image classification, *IEEE Access*, 10, pp. 124738-124746.

26. Gorokhovatskyi V., Tvoroshenko I., Kobylin O., and Vlasenko N. (2023) Search for visual objects by request in the form of a cluster representation for the structural image description, *Advances in Electrical and Electronic Engineering*, 21(1), pp. 19-27.

27. Гороховатський В.О., Творошенко І.С., Чмутов Ю.В. (2022) Застосування систем ортогональних функцій для формування простору ознак у методах класифікації зображень, *Сучасні інформаційні системи*, 6(3), С. 5-12.

28. Гороховатський В., Передрій О., Творошенко І., Марков Т. (2023) Матриця відстаней для множини компонентів структурного опису як інструмент для створення класифікатора зображень, *Сучасні інформаційні системи*, 7(1), С. 5-13.