УДК 004.056

Петровська М.Г., Кушніренко Н.І.

Національний університет «Одеська політехніка»

СИСТЕМА АВТОМАТИЗОВАНОГО МОНІТОРИНГУ КІБЕРЗАХИЩЕНОСТІ ВЕБ-ЗАСТОСУНКІВ

Вступ. У сучасному цифровому світі кількість веб-застосунків у бізнесі, державному управлінні, освіті та повсякденному житті стрімко зростає. Водночас збільшується й кількість кіберзагроз, що створює потребу у впровадженні ефективних методів контролю та моніторингу кіберзахищеності.Веб-застосунки є основною ціллю зловмисників, тому їхній захист - один із ключових напрямів кібербезпеки. Ручні методи перевірки вже не забезпечують потрібної оперативності та масштабованості, тож автоматизовані рішення стають основним інструментом для оцінювання рівня захищеності [1].

Мета: Підвищення рівня безпеки веб-застосунків шляхом створення системи автоматизованого моніторингу та оцінювання їх кіберзахищеності.

Основна частина

У ході дослідження проаналізовано основні існуючі рішення для перевірки безпеки веб-застосунків. Найпоширенішими інструментами є OWASP ZAP, Nikto, Burp Suite, Nmap, які дозволяють здійснювати як базове, так і розширене тестування на наявність вразливостей. Кожен із них має власну сферу застосування та особливості.

Результати порівняльного аналізу наведено у таблиці 1:

Таблиця 1 – Порівняння інструментів для аналізу безпеки веб-застосунків

Назва	OWASP ZAP	Nikto	Burp Suite	Nmap
1	2	3	4	5
Основне призначення	Розробка стандартів, рекомендацій, інструментів для веббезпеки	Перевірка вебсерверів на відомі вразливості	Перехоплення, аналіз та автоматизація тестування вебзапитів	Виявлення хостів, портів, служб у мережі
Основні функції	OWASP Top 10, ASVS, ZAP	Виявлення старих версій серверів, небезпечних скриптів	Перехоплення трафіку, автоматичне сканування, тестування XSS, SQLi	Порт-сканування, виявлення ОС, служб, топології мережі
Інтерфейс	Вебсайт, документи, іноді GUI в проєктах (наприклад, ZAP)	CLI (Командний рядок)	GUI	CLI, графічна версія Zenmap

1	2	3	4	5
Ліцензія / доступність	Відкрита (Open Source)	Відкрита (Open Source)	Відкрита (Open Source)	Безкоштовна і платні версії
Тип звітності	Стандарти, рекомендації, шаблони	Текстовий звіт (TXT, HTML)	Текстовий звіт (TXT, HTML)	Детальні інтерактивні звіти

Виходячи з аналізу, саме OWASP ZAP є оптимальним вибором для розробки системи автоматизованого моніторингу та оцінювання кіберзахищеності веб-застосунків, оскільки він дозволяє інтегрувати власні модулі, змінювати вихідний код, отримувати результати й обробляти їх у власній системі, зокрема із подальшою обробкою модулем AI, а також розширювати функціональність під конкретні потреби наукового дослідження.

Розроблений підхід передбачає використання інтегрованої системи, що поєднує автоматичне сканування вразливостей із контекстним аналізом ризиків. Система дозволяє виконувати періодичний моніторинг стану безпеки веб-застосунків, класифікувати виявлені загрози за рівнем критичності та формувати звіти у зручному форматі (дашборди, таблиці, графіки) [3].

Методологічною основою оцінювання рівня безпеки є стандарти OWASP Top 10 та CVSS [2], що дають змогу визначати критичність знайдених вразливостей і пріоритетність їх усунення. Автоматизований підхід забезпечує оперативність, об'єктивність та зменшує вплив людського фактора.

Система може бути інтегрована у процеси DevSecOps, що забезпечує безперервний моніторинг безпеки під час розробки та оновлення веб-застосунків.

Очікуваним результатом роботи є веб-застосунок, який забезпечує:

- автоматичне виявлення вразливостей веб-застосунків;
- оцінювання рівня кіберзахищеності за обраними критеріями;
- візуалізацію результатів у вигляді інтерактивних звітів;
- формування рекомендацій щодо усунення знайдених проблем.

Висновок. Розробка методів та засобів автоматизованого моніторингу кіберзахищеності веб-застосунків є актуальним напрямом у сфері інформаційної безпеки. Запропонований підхід дозволяє поєднати технічний аналіз із системним оцінюванням ризиків, що підвищує ефективність виявлення вразливостей і знижує ймовірність успішної реалізації кібератак на веб-застосунки. Отримані результати можуть бути використані для подальшої розробки інтегрованих рішень у межах корпоративних систем кіберзахисту та як основа для подальших наукових досліджень у галузі кібербезпеки.

Перелік використаних джерел.

1. OWASP Foundation. OWASP Top 10 – 2021: The Ten Most Critical Web Application Security Risks. – Режим доступу: https://owasp.org/www-project-top-ten/

2. FIRST Organization. Common Vulnerability Scoring System (CVSS) v3.1 Specification Document. – Режим доступу: https://www.first.org/cvss/

3. NIST Special Publication 800-115. Technical Guide to Information Security Testing and Assessment. – National Institute of Standards and Technology, 2008.