УДК 004.056.53:004.896:004.774

А.І. Білоус
О. В. Салієва

АВТОМАТИЗОВАНЕ ВИЯВЛЕННЯ ТА АНАЛІЗ ІН'ЄКЦІЙНИХ ВРАЗЛИВОСТЕЙ ВЕБЗАСТОСУНКІВ ІЗ ВИКОРИСТАННЯМ ВЕЛИКИХ МОВНИХ МОДЕЛЕЙ

Вінницький національний технічний університет

Анотація

У роботі представлено результати розробки вебплатформи «Red Defence» для автоматизованого виявлення ін'єкційних вразливостей вебзастосунків. Розроблено комплексну систему динамічного тестування безпеки (DAST), що реалізує гібридні алгоритми сканування для виявлення вразливостей класу SQL Injection, XSS та Command Injection. Як ключовий елемент наукової новизни запропоновано архітектуру підсистеми інтелектуального аналізу на основі великих мовних моделей (LLM), яка забезпечує автоматизовану оцінку критичності виявлених дефектів та генерацію рекомендацій з їх усунення. Тестування на спеціалізованому вразливому стенді підтвердило ефективність розроблених засобів із нульовим рівнем хибних спрацювань.

Ключові слова: кібербезпека, тестування на проникнення, DAST, SQL Injection, XSS, Command Injection, великі мовні моделі, LLM, сканер вразливостей, інформаційна безпека.

Abstract

This paper presents the results of the development of the "Red Defence" web platform for the automated detection of injection vulnerabilities in web applications. A comprehensive system for dynamic application security testing (DAST) has been developed, implementing hybrid scanning algorithms to detect vulnerabilities of the SQL Injection, XSS, and Command Injection classes. As a key element of scientific novelty, we propose an architecture for an intelligent analysis subsystem based on large language models (LLM), which provides automated assessment of the severity of detected defects and generates recommendations for their remediation. Testing on a specialized vulnerability testbed confirmed the effectiveness of the developed tools with zero false positives.

Keywords: cybersecurity, penetration testing, DAST, SQL Injection, XSS, Command Injection, large language models, LLM, vulnerability scanner, information security.

Вступ

Стрімкий розвиток вебтехнологій та перехід бізнес-процесів у цифровий простір зробили вебзастосунки критично важливою складовою сучасної інформаційної інфраструктури. Відповідно до звітів OWASP Top 10, ін'єкційні вразливості стабільно посідають провідні позиції серед найнебезпечніших загроз для вебсистем [1]. Успішна експлуатація таких вразливостей дозволяє зловмиснику отримати несанкціонований доступ до конфіденційних даних або виконати довільний код на сервері.

Традиційні засоби автоматизованого тестування на проникнення, зокрема комерційні платформи з високою вартістю ліцензій на прикладі Burp Suite [2] та безкоштовні рішення з відкритим кодом OWASP ZAP [3], sqlmap [4], мають певні архітектурні обмеження. До них належать переважно закрита модель аналізу, обмежена гнучкість при роботі з сучасними односторінковими застосунками (SPA) та відсутність вбудованих інструментів для глибокої інтерпретації результатів сканування [5]. Критичною прогалиною наявних рішень є відсутність штатної наскрізної інтеграції з технологіями великих мовних моделей (LLM) «з коробки». Наявні на ринку спроби використання ШІ мають ізольований або плагінний характер, що унеможливлює повністю автоматизований аналіз і комплексну оцінку складних аномалій у перехопленому трафіку без залучення сторонніх модулів.

Метою даної роботи є розробка та дослідження вебплатформи «Red Defence» для автоматизованого виявлення ін'єкційних вразливостей вебзастосунків із застосуванням гібридних алгоритмів сканування та конвеєрного інтелектуального аналізу результатів безпосередньо засобами великих мовних моделей.

Результати дослідження

Для досягнення поставленої мети було спроєктовано та розроблено вебплатформу «Red Defence», архітектура якого базується на асинхронному фреймворку FastAPI із застосуванням стандарту ASGI, що забезпечує паралельну обробку тисяч мережевих з'єднань в єдиному циклі подій . Для аналізу сучасних SPA-застосунків до архітектури інтегровано інструментарій Playwright, який забезпечує повноцінний динамічний рендеринг DOM-дерева та виявлення клієнтських вразливостей типу DOM-based XSS.

Ядро сканування реалізовано у вигляді трьох спеціалізованих модулів: SQLiScanner, XSSScanner та CMDScanner. Модуль SQLiScanner застосовує алгоритм статистичного аналізу часових затримок із подвійною верифікацією для виявлення вразливостей класу Blind SQL Injection. Алгоритм обчислює базову лінію часу відповіді сервера та порівнює її із затримкою після впровадження інструкцій SLEEP/pg_sleep ─ вразливість підтверджується лише за умови статистично значущої різниці, що мінімізує кількість хибних спрацювань. Модуль XSSScanner використовує метод маркерів-канарок: спочатку впроваджується унікальний маркер, визначається точний синтаксичний контекст його відображення (атрибут, JavaScript-блок, HTML-текст), після чого підбирається цільовий вектор для виходу з ізоляції. Модуль CMDScanner генерує різноманітні вектори з комбінацій префіксів (;, |, &&) та суфіксів (#, //) і верифікує виконання через обчислення математичного виразу (echo $((1337+7))).

Для підвищення ефективності в умовах активних засобів захисту реалізовано трирівневу ешелоновану модель сканування: експрес-аналіз базовими векторами, режим обфускації (Bypass Mode) із застосуванням URL/Hex-кодування та глибоке сканування (Deep Scan) з повним перебором розширених словникових баз. Наявність WAF автоматично визначається на етапі розвідки та активує відповідний рівень обфускації навантажень.

Ключовим елементом наукової новизни є підсистема інтелектуального аналізу на основі великих мовних моделей, що функціонує за принципом конвеєра Data-to-Insight. Модуль LoggedSession перехоплює повні сирі дампи HTTP-взаємодії для кожного вектора атаки. На основі зібраних даних система динамічно формує структурований запит до LLM із рольовою моделлю «Експерта з кібербезпеки», яка визначає суворий формат виводу: оцінка критичності за шкалою CVSS, опис виявленої аномалії та персоналізовані рекомендації з ремедіації вихідного коду. Архітектура підсистеми спроєктована за принципом Vendor-Agnostic ─ підтримується підключення API будь-яких провідних LLM-провайдерів, наприклад, OpenAI, Anthropic Claude, Google Gemini [6].

Для наочного порівняння розробленої платформи з існуючими засобами автоматизованого тестування характеристики систем узагальнено в таблиці 1.

Таблиця 1 – Порівняльна характеристика вебплатформи «Red Defence» з існуючими DAST засобами

Критерій порівняння	Burp Suite (Pro)	OWASP ZAP	Sqlmap	Платформа «Red Defence»
Тип архітектури	Десктоп	Десктоп	Консольна	Веборієнтована
Вартість ліцензії	Висока	Безкоштовно	Безкоштовно	Відкрите рішення
Глибина аналізу SPA	Висока	Середня	Відсутня	Висока
Прозорість логіки	Низька	Середня	Висока	Повна
Вбудоване використання ШІ	Обмежене	Відсутнє	Відсутнє	Глибока інтеграція (LLM)
Гнучкість HTTP-сесій	Висока	Середня	Складна	Висока

Аналіз порівняльної характеристики (табл. 1) підтверджує, що розроблена вебплатформа є єдиним серед розглянутих рішень інструментом, що поєднує веборієнтовану архітектуру, повну прозорість процесу сканування та вбудовану інтеграцію LLM для інтелектуального аналізу результатів тестування.

Тестування проводилось на спеціалізованому лабораторному стенді. За результатами тестування всі три модулі сканування продемонстрували стовідсоткову ефективність виявлення при нульовому рівні хибних спрацювань. LLM-агент коректно інтерпретував обфусковані вектори атак ─ зокрема, команди з подвійним екрануванням та SQL-конструкції з inline-коментарями ─ які не піддаються класичним сигнатурним методам аналізу.

Висновки

У результаті проведеного дослідження розроблено вебплатформу «Red Defence» для автоматизованого виявлення та аналізу ін'єкційних вразливостей вебзастосунків. Реалізовано гібридну модель сканування, що поєднує сигнатурні алгоритми, евристичний аналіз часових затримок та динамічний рендеринг DOM-дерева, що забезпечує повне охоплення поверхні атаки для вразливостей класу SQL Injection, XSS та Command Injection. Встановлено, що інтеграція підсистеми інтелектуального аналізу на основі LLM дозволяє усунути ключовий недолік існуючих DAST-інструментів – відсутність автоматизованої інтерпретації результатів сканування: система оцінює критичність виявлених дефектів та генерує рекомендації з виправлення вихідного коду. Тестування підтвердило стовідсоткову ефективність виявлення вразливостей при нульовому рівні хибних спрацювань, що доводить практичну цінність розробленого рішення для проведення комплексного аудиту інформаційної безпеки.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. OWASP Top 10. The Open Worldwide Application Security Project (OWASP). URL: https://owasp.org/Top10/ (дата звернення: 09.04.2026).

2. Burp Suite Professional Features. PortSwigger. URL: https://portswigger.net/burp/pro/features (дата звернення: 13.05.2026).

3. OWASP ZAP Getting Started. URL: https://www.zaproxy.org/getting-started/ (дата звернення: 13.05.2026).

4. Sqlmap: automatic SQL injection and database takeover tool. URL: https://sqlmap.org/ (дата звернення: 13.05.2026).

5. Білоус А. І., Салієва О. В. Порівняльний аналіз алгоритмів автоматизованого виявлення ін'єкційних вразливостей у сучасних вебзастосунках. Матеріали LV науково-технічної конференції підрозділів Вінницького національного технічного університету. URL: https://conferences.vntu.edu.ua/index.php/all-fm/all-fm-2026/paper/view/28700/23605 (дата звернення: 14.05.2026).

6. OWASP GenAI Security Project - Solutions Reference Guide Q2_Q3'25. *OWASP Gen AI Security Project*. URL: https://genai.owasp.org/resource/owasp-genai-security-project-solutions-reference-guide-q2_q325/ (дата звернення: 14.05.2026).

Білоус Артем Ігорович – студент групи 1КІТС-22Б, Факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, м. Вінниця, e-mail: artembilous7@gmail.com

Салієва Ольга Володимирівна – доктор філософії (PhD) за спеціальністю 125 «Кібербезпека», доцент кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, Вінниця, e-mail: salieva8257@vntu.edu.ua

Bilous Artem I. – student of group 1KITS-22B, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, e-mail: artembilous7@gmail.com

Saliieva Olha V. – Doctor of Philosophy (PhD) in specialty 125 "Cybersecurity", Associate Professor of the Department of Management and Security of Information Systems, Vinnytsia National Technical University, Vinnytsia, email: salieva8257@ vntu.edu.ua