DIGITAL REALITY
SCIENTIFIC AND PRACTICAL FORUM
2025

ІНФОРМАЦІЙНА БЕЗПЕКА ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

ПРАЦІ

V МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

9-11 ЧЕРВНЯ 2025 РОКУ
ЛУЦЬК УКРАЇНА

MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE

NATIONAL TECHNICAL UNIVERSITY «KHARKIV POLYTECHNIC INSTITUTE»
ODESSA NATIONAL UNIVERSITY N.A. MECHNIKOV
LESYA UKRAINKA VOLYN NATIONAL UNIVERSITY

V INTERNATIONAL SCIENTIFIC AND PRACTICAL CONFERENCE "INFORMATION SECURITY AND INFORMATION TECHNOLOGIES"

9-11 June 2025
Kharkiv, Odesa, Lutsk – Ukraine

Conference Proceedings

Kharkiv, Odesa, Lutsk
National Technical University «Kharkiv Polytechnic Institute»

2025

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ «ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»
ОДЕСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ І.І. МЕЧНИКОВА
ВОЛИНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ЛЕСІ УКРАЇНКИ

V МІЖНАРОДНА НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ “ІНФОРМАЦІЙНА БЕЗПЕКА ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ”

9-11 червня 2025
Харків, Одеса, Луцьк – Україна

Матеріали конференції

Харків, Одеса, Луцьк
Національний технічний університет «Харківський політехнічний інститут»

2025

УДК 004:005.8(063)

Матеріали V Міжнародної науково-практичної конференції «Інформаційна безпека та інформаційні технології», Харків, Одеса, Луцьк, 9–11 червня 2025 року. – 66 с.

ISBN 978-966-418-541-4

Наведені тези пленарних та секційних доповідей за теоретичними та практичними результатами наукових досліджень і розробок. Представлені результати теоретичних досліджень в галузях кібербезпеки та захисту інформації, проєктування багатоконтурних систем безпеки, системи та засоби штучного інтелекту, електротехніка та телекомунікації, інформаційна безпека держави, суспільства та особистості, програмування та інформаційно-комунікаційні технології, математичне та комп'ютерне моделювання в інформаційних системах, геоінформаційні системи та технології, розпізнавання образів, цифрова обробка зображень і сигналів, програмна інженерія, комунікаційні, GRID та хмарні технології, IoT, інтелектуальний аналіз даних, DataMining і BigData-технології.

Матеріали публікуються в авторській редакції.

За достовірність викладених фактів, цитат та інших відомостей відповідальність несе автор.

УДК 004.8:004.451.9:004.415.2

Ткачук Р.Л.[1], Маслова Н.О.[1,2], Любименко О.М.[2], Івануса А.І.[1]

rlvtk@ukr.net, nataliia.maslova@donntu.edu.ua, olena.liubymenko@donntu.edu.ua, ivaaanusa@gmail.com

[1] Львівський державний університет безпеки життєдіяльності, Львів, Україна
[2] Донецький національний технічний університет, Дрогобич, Львівська область, Україна

СИСТЕМА ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ ЗАХИЩЕНИХ ВЕБ-ДОДАТКІВ З ЗАСТОСУВАННЯМ АГЕНТНИХ ТЕХНОЛОГІЙ

У роботі розглядається використання багатоагентних систем (MAS) для автоматизованого тестування на проникнення (пентестування). Запропоновано підхід, що базується на платформі JADE, де агенти працюють паралельно, адаптуються до змін у захисних механізмах (WAF, IDS/IPS) і генерують поліморфні атаки в реальному часі. Це підвищує ефективність виявлення вразливостей, зменшує потребу в людських ресурсах і дозволяє інтегрувати систему в реальні сценарії кібербезпеки.

Процес пентестування передбачає автоматизований збір інформації про цільову систему, включаючи виявлення відкритих портів, аналіз конфігурацій та пошук вразливостей. Однак сучасні захисні механізми, такі як WAF та IDS/IPS, ускладнюють цей процес, блокуючи підозрілі запити. Для подолання цих бар'єрів застосовуються методи обфускації запитів, динамічна зміна пейлоадів агентами та аналіз частоти відповідей сервера.

У попередніх дослідженнях розглядаються різні аспекти використання багатоагентних систем у кібербезпеці, зокрема для аналізу вторгнень та адаптації захисту [1-3]. Але розподілену MAS для пентестування, яка б поєднувала генерацію атак, зміну пейлоадів у реальному часі та паралельну взаємодію агентів раніше пропоновано не було. Запропоноване рішення на базі JADE заповнює цю прогалину, забезпечуючи інтелектуальний збір даних, адаптацію до захисту та підвищення ефективності тестування безпеки.

розміщуватись на різних фізичних або віртуальних машинах, у різних країнах, щоб уникнути блокування за IP або геолокацією.

Розподіленість підвищує ефективність пентестування, дозволяє обходити WAF і зменшує ризик виявлення.

Метою тестування було оцінити ефективність багатоагентної системи на базі JADE для обходу WAF у реальному часі за допомогою різних методів мутації пейлоадів. Було проведено три типи тестів:

1. XSS через кодування символів.
2. Поліморфний SQLi.
3. Розділений XSS-пейлоад.

Результати показали, що агенти ефективно обходять сигнатурні фільтри WAF, особливо для XSS. SQL-ін'єкції потребують складніших методів обходу. Графік тестування (100 запитів) показав середню успішність атак близько 60%.

У пентестуванні data mining використовується для автоматизованого збору інформації про цільову систему, але сучасні WAF та IDS/IPS ускладнюють цей процес, блокуючи підозрілі запити. Для обходу захисту застосовуються обфускація, динамічна зміна пейлоадів агентами та аналіз відповідей сервера. Багатоагентні системи (MAS) дозволяють розподіляти навантаження, адаптувати атаки в реальному часі та підвищувати ефективність тестування. Запропоноване рішення на базі JADE поєднує автоматичне сканування, генерацію атак і аналіз, забезпечуючи гнучкість, швидкість і здатність обходити захисні механізми.

Сучасні WAF-системи використовують сигнатурний аналіз, евристику та поведінкові моделі для блокування атак. Щоб ефективно тестувати безпеку, багатоагентна система на базі JADE повинна адаптувати пейлоади та змінювати стратегії атак для обходу захисту.

Архітектура системи включає чотири типи агентів:Recon-Agent, Mutation-Agen,t, Attack-Agent, Learning-Agent. Ці агенти працюють разом: Recon-Agent збирає дані, Mutation-Agent створює адаптивні запити, Attack-Agent тестує їх, а Learning-Agent оптимізує підхід. Така динамічна взаємодія дозволяє ефективно обходити WAF у реальному часі.

У розподіленій багатоагентній системі кожен агент працює автономно, але координується з іншими для досягнення спільної мети. Агенти можуть

Система демонструє високу ефективність завдяки динамічній зміні пейлоадів, паралельній роботі агентів і можливості адаптації. Подальші покращення включають інтеграцію машинного навчання для прогнозування фільтрів WAF і генерації складніших атак.

Список літератури

1. Kravari K. and Bassiliades N. A survey of agent platforms, J. Artif. Soc. Soc. Simul., vol. 18, 2015. DOI: 10.18564/jasss.26612.

2. Pal C.-V., Leon F., Paprzycki M., and Ganzha M. A review of platforms for the development of agent systems, Inf., vol. 14, p. 348, Jul. 2020. DOI: 10.3390/info14060348.

3. Kravchuk V., Maslova N., and Dorohyi I. Automated xss vulnerability detection in web applications based on a multi-agent approach, Scientific Papers of Donetsk National Technical University. Series: "Computer Engineering and Automation", vol. 3, № 4(36), pp. 19-30, 2025, https://doi.org/10.31474/2786-9024/v3i4(36).324435

ТЕЗИ ДОПОВІДЕЙ
V Міжнародної науково-практичної конференції
“Інформаційна безпека та інформаційні технології”

“Information Security and Information Technologies”

9–11 червня 2025 р.

Відповідальний за випуск: *С.П. Євсеєв*

Комп`ютерна верстка: *І.В. Аксьонова*
Технічна підтримка *С. В. Мілевський*

Підписано до друку 05.06.2025 р. Формат 60x84/16. Гарнітура Times New Roman. Папір офсетний. Ум.-друк. арк. 4,125.

Видавництво ПП “Новий Світ-2000”
e-mail: novsv2000@gmail.com
Свідоцтво про внесення суб’єкта видавничої справи до Державного реєстру видавців і розповсюджувачів видавничої продукції: серія ДК № 59 від 25.05.2000 р., видане Державним комітетом інформаційної політики, телебачення та радіомовлення України.

Видавець ФОП Піча С.В.
e-mail: novsv2016@ukr.net, https://ns2000.com.ua/
+38 068-978-94-42, +38 050-337-58-46
Свідоцтво про внесення суб’єкта видавничої справи до Державного реєстру видавців, виготівників і розповсюджувачів видавничої продукції: серія ДК № 5069 від 22.03.2016 року, видане Державним комітетом інформаційної політики, телебачення та радіомовлення України.