Міністерство освіти і науки України

Державний вищий навчальний заклад
«Донецький національний технічний університет»

Кафедра автоматики і телекомунікацій

Донецький науковий центр НАН України і МОН України

«ТАК»

Телекомунікації, автоматизація, комп'ютерно-інтегровані та інформаційні технології

Збірка доповідей Всеукраїнської науково-практичної конференції молодих учених
(Дрогобич, 12 грудня 2024 р.)

Дрогобич
ДВНЗ «ДонНТУ»
2024

УДК 621.39+681+004
Т 15

Т 15 **«ТАК»**: телекомунікації, автоматика, комп'ютерно-інтегровані технології: зб. доповідей Всеукр. наук.-практ. конф. молодих вчених, 12 грудня 2024 р. / ДВНЗ «ДонНТУ; відп. ред. Г.В. Ступак. – Дрогобич: ДВНЗ «ДонНТУ», 2024. – 215 с.

До збірника увійшли матеріали доповідей, представлених на Всеукраїнській науково-практичній конференції молодих учених «ТАК»: телекомунікації, автоматика, комп'ютерно-інтегровані технології. Конференція проводилася кафедрой автоматики та телекомунікацій (АТ) ДВНЗ «Донецький національний технічний університет».

У збірнику представлені результати досліджень та розробок молодих вчених із технічних вузів та наукових закладів України.

Збірник призначений для викладачів, аспірантів і студентів вищих технічних навчальних закладів, а також фахівців з телекомунікацій, автоматизації, інформаційних та комп'ютерно-інтегрованих технологій, електротехніки та електромеханіки.

УДК 621.39+681+004

ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ МОДЕЛЮВАННЯ ЗАДАЧ ТЕСТУВАННЯ НА ПРОНИКНЕННЯ

Дорогий Я.Ю., доктор технічних наук, доцент, yaroslav.dorohyi@donntu.edu.ua;
Кравчук В.С., аспірант, vladkrava15@gmail.com
[1] Донецький національний технічний університет, Дрогобич, Україна

Вступ

Веб-застосунки є ключовим елементом цифрової інфраструктури, що забезпечують функціонування бізнесу, урядових структур і критичних галузей, включаючи енергетику, транспорт, фінанси та охорону здоров'я. Їхня зростаюча складність, а також інтеграція із системами третьої сторони значно розширюють поверхню потенційних атак. Зловмисники активно використовують вразливості веб-застосунків для компрометації даних, отримання несанкціонованого доступу чи здійснення деструктивних дій. У контексті критичної інфраструктури (КІ) такі атаки можуть мати катастрофічні наслідки для суспільства, включаючи порушення роботи життєво важливих послуг. Це зумовлює потребу у вдосконаленні процесів виявлення та усунення вразливостей.

Аналіз традиційних підходів

Тестування на проникнення (пентестінг) є основним методом оцінки безпеки веб-застосунків, який передбачає імітацію дій зловмисників для ідентифікації слабких місць у системі. Сучасні підходи до пентестінгу комбінують ручний аналіз із використанням автоматизованих інструментів, таких як Burp Suite. Хоча ці методи демонструють високу ефективність, вони є трудомісткими, залежать від кваліфікації фахівців, виділеного на тестування часу, і часто не забезпечують достатнього покриття складних сценаріїв атак. Особливо це актуально для КІ, де оперативність і точність виявлення вразливостей є критичними для уникнення значних ризиків.

Перспективи застосування штучного інтелекту

Штучний інтелект (ШІ) активно інтегрується в кібербезпекові процеси, відкриваючи нові можливості для автоматизації складних завдань. Його застосування у пентестінгу веб-застосунків дозволяє суттєво знизити часові витрати, покращити точність аналізу та забезпечити адаптацію до динамічних умов. У контексті КІ це може підвищити рівень захисту критичних систем від кіберзагроз. Проте наразі відсутні широко відомі ШІ-рішення, які б забезпечували ефективний пентестінг веб-застосунків. Розробка таких моделей є перспективним напрямом, що має значний науковий і практичний потенціал.

В якості напрямків дослідження можуть бути:

– аналіз традиційних методів тестування на проникнення веб-застосунків із врахуванням потреб КІ;

– огляд і оцінку існуючих ШІ-алгоритмів для виявлення вразливостей;

– розробку архітектури ШІ-моделі для інтеграції у процеси пентестінгу;

– проведення експериментального порівняння ефективності автоматизованих ШІ-методів із ручними підходами;

– оцінку ризиків і викликів, пов’язаних із використанням ШІ для пентестінгу КІ;

– інтеграцію прототипу моделі в сучасні інструменти, такі як Burp Suite.

Верхньорівневий опис ШІ-моделі для Burp Suite

Пропонована модель використовуватиме методи машинного навчання та обробки великих даних для ідентифікації вразливостей у веб-застосунках. Основою моделі є використання сучасних підходів до аналізу даних, включаючи тензорний аналіз, який дозволяє обробляти багатовимірні дані та будувати складні залежності між параметрами системи. Це особливо важливо для обробки великих обсягів логів, HTTP-запитів, конфігурацій та інших даних, які характеризують поведінку веб-застосунків. Модель складатиметься з кількох модулів:

1. *Модуль збору даних* – автоматизований збір і попередня обробка інформації про цільову веб-інфраструктуру, включаючи структуру, вхідні точки та API.

2. *Модуль аналізу вразливостей* – застосування тензорного аналізу для виявлення багатовимірних залежностей між характеристиками трафіку, поведінковими моделями користувачів і параметрами системи для ідентифікації аномалій, що можуть вказувати на вразливості.

3. *Модуль симуляції атак* – генерація сценаріїв атак з урахуванням результатів тензорного аналізу, що дозволяє виявляти навіть складні та приховані уразливості.

4. *Модуль оцінки ризиків* – автоматична класифікація виявлених вразливостей за рівнем ризику з використанням машинного навчання, оптимізованого для аналізу тензорних даних, а також надання рекомендацій щодо їх усунення.

5. *Інтерфейс інтеграції* – API для інтеграції з Burp Suite, що дозволить використовувати модель як частину інструментарію пентестера, забезпечуючи безперервний обмін даними та аналіз результатів.

На рисунку 1 представлено верхньорівневу архітектуру моделі та її взаємодію з Burp Suite.

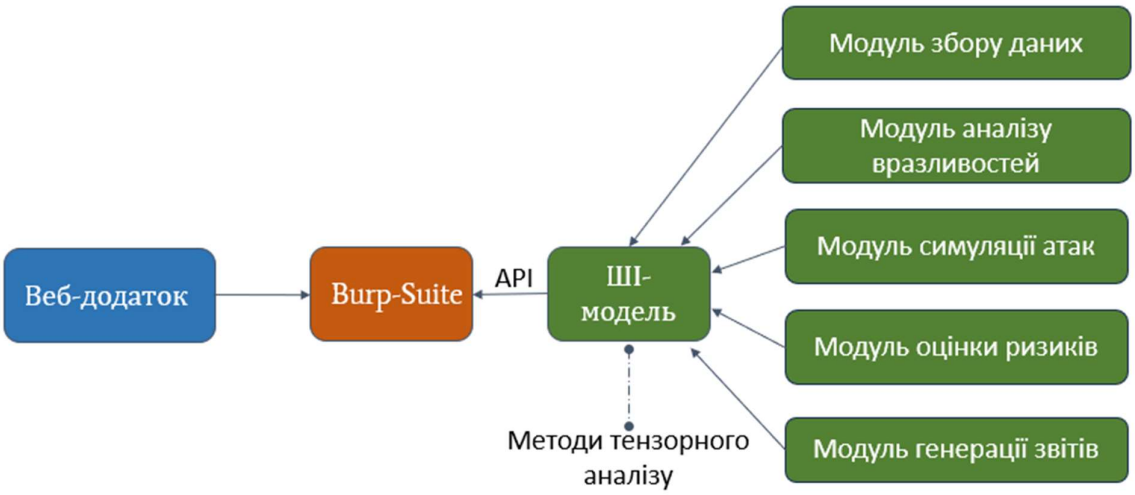

Рисунок 1. Архітектура моделі

Тензорний аналіз забезпечує ефективне виявлення прихованих закономірностей, які можуть залишитися непоміченими при застосуванні традиційних підходів. Він також дозволяє динамічно оновлювати моделі на основі нових даних, підвищуючи точність і адаптивність системи.

Використання тензорного аналізу як складової моделі значно розширює її функціональні можливості, дозволяючи враховувати складні взаємозв'язки у веб-інфраструктурі. Це забезпечить більш точне та оперативне виявлення вразливостей, що особливо важливо для захисту критичної інфраструктури. Інтеграція моделі в Burp Suite сприятиме вдосконаленню існуючих інструментів, роблячи їх доступними для ширшого кола фахівців.

Висновки

Розробка та застосування штучного інтелекту в процесі тестування на проникнення веб-застосунків відкривають нові перспективи для кібербезпеки, особливо в контексті захисту критичної інфраструктури. Використання тензорного аналізу в моделі дозволяє виявляти багатовимірні залежності між параметрами системи, підвищуючи точність і ефективність ідентифікації вразливостей. Інтеграція моделі у Burp Suite забезпечує автоматизацію тестування, скорочення часу на аналіз і мінімізацію залежності від людського фактора.

Отримані результати можуть бути використані для вдосконалення підходів до тестування безпеки, розробки комерційних рішень і зміцнення захисту критичних цифрових інфраструктур. Крім того, модель стане основою для подальших наукових досліджень у сфері кібербезпеки, сприяючи адаптації до нових викликів, пов'язаних із зростанням кіберзагроз.

Література

1. Бренд Л. Векторний і тензорний аналіз / Л. Бренд // Нью-Йорк: John Wiley & Sons. — 1947. — 276 с.

2. Дафти Д. Веб-додатки: Принципы безпеки та пентестування / Д. Дафти // Нью-Йорк. — 2020. — 320 с.

3. Гудфеллоу И., Бенджіо Й., Курвилл А. Глибоке навчання / І. Гудфеллоу, Й. Бенджио, А. Курвілл // Кембридж: MIT Press. — 2016. — 775 с.

Анотація

У статті розглянуто перспективи застосування штучного інтелекту для автоматизованого тестування на проникнення веб-застосунків із використанням тензорного аналізу. Запропоновано архітектуру ШІ-моделі, інтегрованої у Burp Suite, яка дозволяє ідентифікувати вразливості із врахуванням багатовимірних залежностей у даних. Основну увагу приділено ефективності таких методів для захисту критичної інфраструктури. Виконано аналіз традиційних підходів, оцінено потенціал сучасних алгоритмів ШІ та проведено порівняння автоматизованих і ручних методів тестування. Результати дослідження демонструють перспективність використання моделі для підвищення точності, оперативності та масштабованості процесів забезпечення кібербезпеки.

Ключові слова: кібербезпека, критична інфраструктура, штучний інтелект, тестування на проникнення, тензорний аналіз, веб-застосунки, Burp Suite.

Abstract

The article explores the prospects of applying artificial intelligence for automated penetration testing of web applications using tensor analysis. The architecture of an AI model integrated into Burp Suite is proposed, enabling the identification of vulnerabilities considering multidimensional data dependencies. The focus is placed on the effectiveness of these methods for protecting critical infrastructure. An analysis of traditional approaches has been conducted, the potential of modern AI algorithms evaluated, and a comparison of automated and manual testing methods performed. The study results demonstrate the feasibility of utilizing the model to enhance the accuracy, efficiency, and scalability of cybersecurity processes.

Keywords: cybersecurity, critical infrastructure, artificial intelligence, penetration testing, tensor analysis, web applications, Burp Suite.