МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Одеська юридична академія»

ЄВРОПЕЙСЬКІ ОРІЄНТИРИ РОЗВИТКУ УКРАЇНИ: НАУКОВО-ПРАКТИЧНИЙ ВИМІР В УМОВАХ ВОЄННИХ ВИКЛИКІВ

МАТЕРІАЛИ
Міжнародної науково-практичної конференції

Одеса, 26 квітня 2024 року

Одеса
«Фенікс»
2024

УДК 005.332.2(4):316.42(477)“364”“20”(062.552)
Є 24

Рекомендовано до друку вченою радою
Національного університету «Одеська юридична академія»
(протокол № 8 від 15.05.2024 р.)

За загальною редакцією ***С. В. Ківалова***

Відповідальний за випуск ***М. Р. Аракелян***

Є 24 **Європейські орієнтири розвитку України: науково-практичний вимір в умовах воєнних викликів** : матеріали Міжнар.наук.-практ. конф. (Одеса, 26 квітня 2024 р.) / за заг. ред. С. В. Ківалова. – Одеса : Фенікс, 2024. – 1000 с.
ISBN 978-617-8430-05-4

У збірнику відображено наукові напрацювання вчених, практиків, військовослужбовців у теоретичній та емпіричній площині у сферах філософських основ, загальної теорії та історичних досліджень держави і права, актуальних проблем світових соціально-політичних процесів, соціології та психології в умовах повномасштабного військового вторгнення. Висвітлено питання загроз національній безпеці в їх конституційному вимірі у рамках міжнародного та європейського права, трудового права та права соціального забезпечення, земельного, аграрного та екологічного права, пов’язані з функціонуванням економіки та підприємництва в умовах європейського вибору України. Розглянуто проблеми інформатизації та цифровізації суспільства, захисту інформації та кібербезпеки в умовах військового вторгнення, питання методики викладання іноземних мов, теорії та практики перекладу, проблеми лінгвістики та журналістики. Відображено наукові напрацювання у сферах адміністративного права та процесу, фінансового, морського та митного права, організації та вдосконалення судоустрою, прокуратури, інших правоохоронних органів, адвокатури. Висвітлено питання кримінального права, кримінально-процесуальних аспектів кримінального провадження та кримінологічних особливостей протидії злочинності в умовах воєнного стану, криміналістики, судової експертизи, психології та медицини у забезпеченні судочинства, цивільного та сімейного права, інтелектуальної власності та патентної юстиції, цивільного судочинства, господарського права та процесу. Розглянуто актуальні питання діяльності сучасних бібліотек у закладах вищої освіти, фізичної підготовки здобувачів вищої освіти.

Збірник розраховано на наукових і науково-педагогічних працівників, здобувачів вищої освіти, практичних працівників у сферах юридичної, економічної, соціологічної, політологічної, психологічної, філологічної наук, журналістики та кібербезпеки тощо.

УДК 005.332.2(4):316.42(477)»364»»20»(062.552)

Матеріали видано в авторській редакції

ISBN 978-617-8430-05-4

СЕКЦІЯ 24. КІБЕРБЕЗПЕКА ОСОБИ, СУСПІЛЬСТВА ТА ДЕРЖАВИ ЯК ФУНДАМЕНТАЛЬНИЙ ЕЛЕМЕНТ ЗАБЕЗПЕЧЕННЯ ОБОРОНОЗДАТНОСТІ УКРАЇНИ

СЕКЦІЯ 25. ПИТАННЯ МЕТОДИКИ ВИКЛАДАННЯ ІНОЗЕМНИХ МОВ, ТЕОРІЇ ТА ПРАКТИКИ ПЕРЕКЛАДУ ЯК ЗАСОБУ НАЛАГОДЖЕННЯ КОМУНІКАЦІЇ

злам або незаконне вторгнення, можуть мати серйозні правові наслідки. Будьте впевнені, що ваші дії відповідають вимогам закону та етики.

- Користування захисними заходами: Використовуйте захисні заходи, такі як файрволи, системи виявлення вторгнень та програмне забезпечення антивірусного захисту, для захисту системи від незаконної або шкідливої активності [5].

Фальсифікація системних журналів є серйозною проблемою, яка може мати значні наслідки для безпеки та цілісності системи. Недотримання правил безпеки системи на системних журналів може призвести до великих страт даних, та іншої важливої інформації. Дотримуючись рекомендацій системних адміністраторів та правил користування системою можна знизити ризики фальсифікації системних журналів зловмисниками, та захистити свою систему від атак.

Список використаних джерел

1. What is Log Tampering? URL: https://www.geeksforgeeks.org/what-is-log-tampering/
2. Chintan Gurjar. Computer forensics investigation: A case study. 2018. URL: https://www.infosecinstitute.com/resources/digital-forensics/computer-forensics-investigation-case-study/
3. Troubleshooting with Linux Logs. 2022. URL: https://www.loggly.com/ultimate-guide/troubleshooting-with-linux-logs/
4. How to Prevent Data Tampering In Your Business. 2020. URL: https://www.cypressdatadefense.com/blog/data-tampering-prevention/
5. Most Common Linux Logging Issues. 2023. URL: https://linuxstans.com/common-linux-logging-issues/

Ключові слова: Фальсифікація, системні журнали, лог файли, операційна система, програмне забезпечення, вразливості.

Keywords: Tampering, system logs, log files, operating system, software, vulnerabilities.

Дика Анастасія Іванівна
Національний університет «Одеська юридична академія»,
аспірантка кафедри інформаційних технологій
Трофименко Олена Григорівна
Національний університет «Одеська юридична академія»,
доцент кафедри інформаційних технологій, кандидат технічних наук, доцент

АНАЛІЗ ПОТЕНЦІЙНИХ ЗАГРОЗ ЗАСОБАМИ CHATGPT ДЛЯ ТЕСТУВАННЯ БЕЗПЕКИ ВЕБЗАСТОСУНКІВ

Вебзастосунки нині є невіддільною частиною сучасного цифрового світу. Зростання їх популярності не в останню чергу зумовило актуалізацію вимог до їх безпеки. Потенційно вебзастосунки можуть піддаватися різноманітним загрозам: атакам з використанням вразливостей, витокам конфіденційної інформації, атакам з метою отримання несанкціонованого доступу до системи тощо. Тестування безпеки вебзастосунків є важливою складовою процесу їх розробки, оскільки дозволяє виявити й усунути потенційні вразливості перед введенням програмного забезпечення в експлуатацію.

З появою штучного інтелекту стало можливим його використання й у сфері інформаційної безпеки, наприклад, для тестування безпеки вебзастосунків. Моделі глибокого навчання, зокрема GPT (Generative Pre-trained Transformer), дозволяють створювати системи, здатні аналізувати текстові дані, що відкриває широкі можливості їх застосування для тестування безпеки. Дослідники [1] звернули увагу на можливості застосування ChatGPT для автоматизації процесу тестування безпеки вебзастосунків, завдяки його здатності розуміти контекст

та в режимі реального часу аналізувати великі обсяги текстової інформації. ChatGPT добре інтегрується з різними інструментами автоматизації процесів, що дозволяє в режимі 24/7 ефективно виявляти потенційні загрози в сценаріях тестування безпеки.

ChatGPT може бути використаний для аналізу програмного коду, логів підключень під час тестування на вразливості вебзастосунків. Він може розпізнавати патерни, характерні для найпоширеніших видів атак – SQL-ін'єкцій, та перехресного скриптінгу (XSS). Ба-більше, крім аналізу даних, модель ChatGPT може генерувати такі типи атак та перевіряти реакцію системи на них. Це допомагає виявляти потенційні вразливості та перевіряти ефективність наявних у програмному забезпеченні захисних механізмів. Крім того, ChatGPT можна використовувати для моделювання взаємодії людини з програмними системами, що дозволяє виявляти вразливості, які традиційні методи тестування можуть пропустити. Це пояснюється тим, що ChatGPT базується на обробленні природної мови (NLP, Natural Language Processing), що дає йому змогу розуміти та обробляти людську мову. Це може допомогти тестувальникам безпеки у виявленні вразливостей, характерних для атак соціальної інженерії (байтінг, вішінг, претекстінг, приманка і підміна тощо).

Як приклад моделювання атаки соціальної інженерії засобами ChatGPT було створено сторінку для клікджекінгу. Клікджекінг-уразливість полягає в тому, щоб обманом змусити користувача натиснути на нешкідливу, на перший погляд, кнопку або посилання, яке насправді виконуватиме небажану дію, наприклад, завантажуватиме шкідливе програмне забезпечення або відправлятиме зібрану особисту інформацію на сторонні вебресурси. На рис. 1 наведено код мовою Python для виявлення вразливості вебсайту до клікджекінгу за допомогою ChatGPT.

python Copy code

```python
import requests

def check_clickjacking(url):
    try:
        response = requests.get(url)
        headers = response.headers

        if 'X-Frame-Options' in headers:
            x_frame_options = headers['X-Frame-Options']
            if x_frame_options.lower() != 'deny' and x_frame_options.lower() != 'sameorigin':
                print("Potential clickjacking vulnerability detected (X-Frame-Options header):", x_frame_options)
            else:
                print("No potential clickjacking vulnerability detected (X-Frame-Options header):", x_frame_options)
        else:
            print("X-Frame-Options header is not present")

        if 'Content-Security-Policy' in headers:
            csp = headers['Content-Security-Policy']
            if 'frame-ancestors' not in csp or "'none'" in csp or "'self'" in csp:
                print("Potential clickjacking vulnerability detected (Content-Security-Policy header):", csp)
            else:
                print("No potential clickjacking vulnerability detected (Content-Security-Policy header):", csp)
        else:
            print("Content-Security-Policy header is not present")

    except requests.exceptions.RequestException as e:
        print("Error occurred while checking the URL:", e)

# Example usage:
check_clickjacking("https://example.com")
```

Рис. 1. Скрипт для виявлення вразливості вебсайту до клікджекінгу

У проведеному експерименті ChatGPT успішно проаналізував код на наявні вразливості, реалізував скрипт для автоматизації процесу сканування вебзастосунків на вразливості. Однак, як показав цей експеримент та дослідження інших науковців [2], для ChatGPT характерна проблема щодо правильності поєднання різних фрагментів скрипту без людського втручання.

Попри значні переваги, варто зважати та враховувати певні обмеження використання ChatGPT у тестуванні безпеки. Зокрема, модель може виявляти лише ті загрози, які вона була навчена розпізнавати, тому її ефективність залежить від якості навчання та обсягу доступної інформації. Крім того, варто уникати повного автоматизованого тестування безпеки, оскільки це може призвести до пропуску певних видів атак або до виникнення помилкових позитивних спрацювань.

Використання штучного інтелекту, зокрема моделі ChatGPT, в тестуванні безпеки вебзастосунків відкриває широкі можливості для виявлення та запобігання різного роду загрозам. Проте важливо пам'ятати про обмеження використання моделі та враховувати їх при плануванні й виконанні тестування безпеки.

Список використаних джерел

1. Як використовувати ChatGPT для ефективного тестування безпеки : вичерп. посіб. 2023. URL: https://brainberry.ua/uk/newsroom/blog/how-to-use-chatgpt-for-effective-security-testing-a-comprehensive-guide

2. Al-Hawawreh M., Aljuhani A., Jararweh Y. ChatGPT for cybersecurity: practical applications, challenges, and future directions. *ClusterComputing*. 2023. Vol. 26. № 6. P. 3421–3436. DOI: 10.1007/s10586-023-04124-5.

Ключові слова: тестування програмного забезпечення, тестування безпеки, штучний інтелект, ChatGPT.
Keywords: software testing, security testing, artificial intelligence, ChatGPT.

Проданюк Назар Богданович
Чернівецький національний університет імені Юрія Федьковича,
аспірант кафедри теорії права та прав людини

ДЕЯКІ ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ ДОСТУПНОСТІ ЮРИДИЧНИХ ПОСЛУГ У ЦИФРОВУ ЕПОХУ

У процесі нашого дослідження, в контексті загального прискорення темпів технологічного прогресу в цифрову епоху, виявляється, що актуальність проблеми доступності юридичних послуг стає дедалі більш очевидною, а її вплив на доступ громадян до справедливості та правової допомоги набуває ще більшої важливості. Цифрова трансформація в сучасному суспільстві змінює уявлення про надання юридичних послуг. Сьогодні ми спостерігаємо перехід від традиційних методів надання правової допомоги до використання цифрових технологій. Мобільні додатки, онлайн-платформи, веб-сайти та штучний інтелект стають ключовими інструментами у забезпеченні доступу до інформації та послуг у сфері права. Одним із досліджень, що підтверджує це твердження, є робота М. Дубняк та В. Соловйової – «Цифрова трансформація юридичних послуг» , в якій зазначається: «Сьогодні існує тенденція до збільшення використання електронних форматів управління справами юридичного характеру, які дедалі частіше надходять у віртуальному вигляді, замість традиційного особистого звернення клієнта до офісу адвоката. З введенням нових систем, роль юриста трансформується: він перестає бути активним виконавцем завдань, а стає контролером кінцевого продукту системи. У довгостроковій перспективі можна прогнозувати створен-