



АВТОМАТИЗОВАНА СИСТЕМА АНАЛІЗУ ЗАХИЩЕНОСТІ ВЕБ-ЗАСТОСУНКІВ

ГАЛИЦЬ В. О КН-3

КЕРІВНИК: ВОЗНЮК Я. І

- Дослідити найпоширеніші вразливості веб-застосунків
- Продемонструвати способи взаємодії з веб-застосунками мовою Python
- Розробити автоматизовану систему аналізу захищеності
- Розробити інтерфейс , зрозумілий кожному

МЕТА

ПЛАН

Розробити веб-краулер використовуючи Selenium WebDriver



Розробити модулі тестування вразливостей

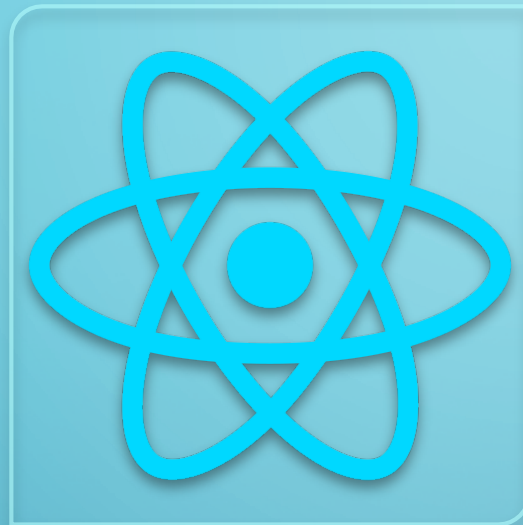
SQL-ін'єкції

XSS атаки

Cookie атрибути

HTTP заголовки

SSRF
вразливість



ІНСТРУМЕНТИ РОЗРОБКИ

ОГЛЯД ЗАСТОСУНКУ

Web-Analyst

Check Security



ОГЛЯД ВІДПОВІДІ ЗАСТОСУНКУ

Security Report for: [https:// www.cnn.com/](https://www.cnn.com/)

Misconfigurations

Missing Headers

X-Frame-Options: Protects against clickjacking.

Strict-Transport-Security: Enforces secure (HTTP over SSL/TLS) connections to the server.

Referrer-Policy: Controls information that is set in the Referer header.

Cookie Report

FastAB

Secure: false

HttpOnly: false

SameSite: Lax

Path: /

Domain: .cnn.com

Expires: 1747225864



ОГЛЯД ВІДПОВІДІ ЗАСТОСУНКУ

SSRF Report

No SSRF vulnerabilities found.

Sublinks Discovered

- <https://www.cnn.com/politics/congress>
- <https://www.cnn.com/privacy>
- <https://www.cnn.com/>
- <https://www.cnn.com/travel>
- <https://www.cnn.com/politics/supreme-court>
- <https://www.cnn.com/election/2024>
- <https://www.cnn.com/sport>
- <https://www.cnn.com/videos/fast/cnni-fast>
- <https://www.cnn.com/politics/fact-check>
- <https://www.cnn.com/>



ОГЛЯД ВІДПОВІДІ ЗАСТОСУНКУ

SQL Injection Results

<https://www.cnn.com/politics/congress>: Not vulnerable

<https://www.cnn.com/privacy>: Not vulnerable

<https://www.cnn.com/>: Not vulnerable

XSS Injection Results

`https://demo.testfire.net/index.jsp?content=personal_cards.htm:`

Vulnerable: `/search.jsp: <script>alert(123);</script>`

ОГЛЯД ВІДПОВІДІ ЗАСТОСУНКУ

ВИСНОВКИ

- Було досліджено поширені типи атак на веб-застосунки
- Розроблено систему аналізу вразливостей
- Покращено знання розробки застосунків для взаємодії з веб-браузерами



ДЯКУЮ ЗА
УВАГУ!

