Hasan Krayem

Beirut, Lebanon, +961 76938271, itskrayem@gmail.com

PROFILE

A cybersecurity enthusiast who is passionate about protecting digital environments from attacks. Equipped with proficiency in web development, automation, networking, and Python programming. As someone who has completed the CCNA certification and is currently pursuing PenTest+, I have a thorough understanding of technology. My philosophy centres on lifelong learning and flexibility, guaranteeing the provision of creative, safe solutions adapted to changing market needs.

EDUCATION

2021 — 2024

Bachelor's degree, USAL

Beirut

Computer & Network Security

EXPERTIES

Programming and Scripting:

- Proficiency in scripting languages like Python, and Bash for automation and tool development.
- Knowledge of programming languages and frameworks as Java, Js, .Net(MVC), React, Node.js, and Flask for understanding vulnerabilities in software applications.

Network Security:

- Implementation and management of firewalls, VPNs, IPS, IDS, SIEM, DLP, Sandboxing.

Penetration Testing:

- Social engineering
- Operating systems
- Reporting & communication
- Cryptography
- Tools:Metasploit, Nessus, nmap, Hashcat, etc.
- OSINT framework
- WireShark
- DNS Recon
- Google Dorks

Vulnerability Assesment:

- Organizational, written communications and oral presentation skills
- Penetration testing skills including the use of relevant tools and technologies
- Detail oriented, organized, methodical, follow up skills with an analytical thought process
- Familiarity with validating vulnerability scanning results, mitigation and falsepositives
- Strong understanding of the Common Vulnerability Scoring System and itsapplication in a production vulnerability management environment

Web Application Security:

- Knowledge of common web vulnerabilities such as SQL injection, Cross-Site Scripting (XSS), and Cross-Site Request Forgery (CSRF).
- Proficiency with web application security testing tools like Burp Suite, OWASP ZAP.
- Experience gained through completing web security labs like WebGoat and Juice Shop

SKILLS

- A proactive approach to addressing security vulnerabilities and strong problem-solving skills.
- Fast self learner.
- Excellent communication skills and the ability to collaborate effectively with multidisciplinary teams.

PROJECTS:

Multi-Faceted Cybersecurity Assessment Tool

The "Multi-Faceted Cybersecurity Assessment Tool" is a Python-based project designed to provide comprehensive insights into the security posture of a given domain. This tool combines multiple cybersecurity assessment techniques, including network scanning, subdomain enumeration, link extraction, and data gathering from external sources.

The main functionalities of the tool include:

1. **Nmap Scanning:** Utilizes the Nmap library to perform version detection on the target domain, identifying open ports and services running on them.
2. **Subdomain Enumeration:** Uses asynchronous techniques with aiohttp to scan for potential subdomains associated with the target domain, leveraging a list of common subdomains.
3. **Link Extraction:** Parses the HTML content of the target domain to extract all hyperlinks, providing visibility into the web structure and potential attack vectors.
4. **Data Gathering with External APIs:** Utilizes external APIs such as Hunter.io and Shodan to gather additional information related to the domain, such as email addresses associated with the domain and known vulnerabilities (CVEs) associated with its IP addresses.

The project aggregates the results of these assessments into a structured JSON report, providing a comprehensive overview of the domain's security posture. This tool can be valuable for cybersecurity professionals, penetration testers, and system administrators seeking to identify and address potential security risks associated with a target domain.

Web Application Pentesting

This project presents a detailed security analysis of the website tjara.com, focusing on uncovering vulnerabilities and potential security threats. The analysis spans various stages, starting with information gathering and scanning, utilizing tools such as builtWith, Shodan, TheHarvester, Nmap, and Python scripts. These tools provide insights into the website's infrastructure, technologies used, open ports, and potential vulnerabilities.

The document then discusses findings from manual testing using tools like Burpsuite, identifying issues such as plaintext transmission of credentials, session token handling, and potential SQL injection vulnerabilities. Additionally, vulnerabilities associated with specific technologies used on the website, such as jQuery and WordPress, are highlighted.

The analysis further explores the website's infrastructure, including its underlying technologies and security policies. Recommendations are made for addressing identified vulnerabilities and enhancing the overall security posture of the website.

In conclusion, the document emphasizes the importance of addressing identified vulnerabilities promptly to ensure the security and integrity of tjara.com. It underscores the need for continuous monitoring and updates to mitigate potential security risks in the dynamic digital landscape.

LANGUAGES

English

Arabic