Mehdi Al Housseini
Software Engineer

Beirut, Lebanon
+961 78831726 – malhousseini966@gmail.com
linkedin.com/in/mahdialhousseini

Career Objective

Highly skilled cybersecurity software engineer, proficient in web development, containerization, machine learning and cybersecurity, dedicated to delivering innovative, secure, and data-driven solutions.

Professional Experience

Ethical Hacker and Penetration Tester - Cylock, full time
Feb 2023 – Jan 2025
Bolzano, Italy – Hybrid

- Translated and optimized multi-language code—primarily in Python and Perl—specifically for penetration testing across servers, networks, and operating systems. Maintained high standards of readability, resilience, and efficiency to ensure robust, maintainable software solutions.
- Gained practical experience with web application security through projects using Django and Vue.js, enhancing my expertise in managing databases like PostgreSQL and implementing secure SQL practices.
- Enhanced web application interactivity and user experience using JavaScript, applying best practices in secure web development to prevent XSS and CSRF vulnerabilities.
- Designed and implemented secure, scalable web infrastructures with Flask, leveraging Gunicorn and Nginx for optimized delivery and reliability. Advanced Docker configurations to create secure, isolated networking environments suitable for high-stakes penetration testing and secure API interactions. This platform was designed to simplify complex penetration testing processes, making them accessible and manageable for users with varying levels of technical expertise.
- Deployed and optimized large language models for security data analysis using Google Cloud services, leveraging high-performance GPUs to train and test data efficiently. This implementation was specifically tailored to enhance the initial summarization of vulnerability assessment reports, ensuring detailed and accurate reflections of security scans.
- Managed version control and collaborative software development processes using GitHub, ensuring robust code review practices and secure coding standards.
- Engineered sophisticated web scraping and data extraction tools using Scrapy, Beautiful Soup, and Selenium, with a focus on analyzing web archives and HTTP headers for security testing purposes.
- Performed advanced network reconnaissance and enumeration using tools such as Nmap for port and service scanning, OS and service fingerprinting, and employing advanced techniques like decoy IPs and source-port manipulation to bypass firewall protections.
- Developed, utilized, and refined security testing tools such as Metasploitable, Dirb, Dig, Droopescan, Joomscan, Nikto, SSLScan, and TestSSL, creating custom scripts in Python and Bash to enhance tool efficacy and adapt to specific penetration testing requirements.
- Expertly configured and utilized BurpSuite for sophisticated traffic capture, analysis, and manipulation to identify and exploit application vulnerabilities effectively.
- Utilized Nessus, OpenVAS, and various other vulnerability assessment tools to automatically identify and capture system vulnerabilities; generated security reports, incorporating safe checks, rate-limiting, and false-positive handling. Additionally, automated these tools using Python scripts to improve scanning efficiency.
- Conducted infrastructure analysis, domain discovery, SMB and NFS enumeration and exploitation, as well as DNS footprinting, zone transfers, SNMP (snmpwalk, onesixtyone), FTP, web server scanning (Gobuster, ffuf) and subdomain enumeration using various tools and techniques.
- Prepared and delivered detailed security reports by utilizing advanced Python libraries to parse and analyze inputs, transforming them into comprehensive reports that outline identified vulnerabilities, proposed remediation strategies, and demonstrated proof-of-concept attacks to inform stakeholders and guide security enhancement efforts.

Machine Learning Engineer Internship- Truckscreenia, Full-time
Nov 2022 – Dec 2022
Bolzano, Italy – Onsite

- Collected, cleaned, and analyzed data to ensure quality and reliability, and gained meaningful insights using various machine learning models in Python to support business decisions.
- Developed and optimized data processing pipelines using Pandas, Scikit-learn and others to streamline machine learning workflows.

Python Developer and Researcher Internship – Beirut Research & Innovation Center, Full-time
Nov 2019 – Feb 2020
Beirut – Onsite

- Participated in a CubeSat Link Encryption project developing advanced encryption solutions for CubeSat communication.

Technical Skills

- **Programming Languages //** Python, C#, JavaScript, PHP, bash, SQL
- **Database Management Systems //** MySQL, Oracle TNS, SQLAlchemy, Postgresql
- **Development Frameworks and Libraries //** React, Vue.js, Node.js
- **Tools //** Rest APIs, GitHub, Postman, Docker
- **Cloud Services //** google cloud Vertex AI, Amazon AWS SageMaker
- **Infrastructure as code //** Automate the provisioning and management of resources on AWS using Terraform with defining infrastructure through code to create reproducible and scalable environments, including EC2 instances, S3 buckets
- **Theory //** Complexity Analysis, Data Structures and Algorithms, Design Patterns, OOP
- **Data Analysis and Visualization Tools//** R, Pandas, NumPy, Matplotlib, Seaborn
- **Machine Learning //** Scikit-learn, TensorFlow, Keras, pytorch, openCV, nlp, support vector machine, neural networks, clustering
- **Statistics //** Descriptive and inferential statistics, hypothesis testing, ANOVA, regression analysis, etc.
- **Networking //** sockets, VLANs, Dynamic Routing Protocols, VPN
- **Testing //** unit testing, test driven development, mocks, fuzzing
- **Embedded systems //** esp32, Arduino
- **Cybersecurity //** Expertise in network enumeration, footprinting, and vulnerability assessment across Windows and Linux. Skilled in exploitation (shells & payloads), password attacks, and hash cracking using tools like Hashcat, Mimikatz, Invoke-SMBExec, CrackMapExec, Evil-WinRM, and Kerberos utilities (Pass the Hash, Pass the Ticket). Proficient in managing password storage (SAM, NTDS.dit) and extracting/forging credentials with Mimikatz and Rubeus in Active Directory. Experienced in cracking protected archives (ZIP/PDF/Office) and BitLocker volumes. Enforces secure password policies (complexity, rotation, blacklisting) and leverages both cloud and local password managers.
- **Windows & Linux File Transfer //** PowerShell (DownloadFile, DownloadString, IEX), Certutil, Bitsadmin, Base64 Encoding/Decoding, Python HTTP Servers, FTP, SMB (Impacket)
- **Enterprise business management //** Trello

Soft Skills

- Cooperation and a willingness to operate as a team
- Strong attention to detail.
- Readiness to adapt and solve issues.
- Highly enthusiastic about digital transformation.
- Strong mentality for analysis.

Education

Master in Software Engineering for Information Systems – Free University of Bolzano, Italy
Jul 2021 – Jul 2023

Bachelor of Management Information Systems - Lebanese University, Lebanon
Sep 2015 – Jul 2020 Concurrent studies

Professional Bachelor of Telecommunication - Lebanon
Sep 2016 – Jul 2019 Concurrent studies

Languages

Arabic (Native); English (Fluent); Italian (Intermediate); German (Beginner)