Mohammadreza Hemmati

Tehran , Iran
mohammad.hmt99@gmail.com Linkdin Github

EDUCATION

B.Sc. of Computer Engineering **2017 – 2022**
Shahid Beheshti University *Tehran, Iran*

- **Supervisor:** Dr. Mojtaba Vahidi
- **Thesis:** Designing and Developing Advanced Websites for Business Introduction: A Comprehensive Approach to Digital Branding and User Engagement. Grade (A+)
- **GPA**: 3.15/4 (14.73/20)

RESEARCH INTERESTS

- Advanced Vulnerability Discovery and Exploitation Techniques in Web Applications
- Mitigation Strategies for Zero-Day Attacks in Critical Network Systems
- Machine Learning and AI-Driven Approaches for Automated Penetration Testing
- Security Assessment of IoT Devices and Protocols in Network Environments

WORK EXPERIENCE

Dotin (Core Banking) | Penetration Tester **December 2022 – January 2024**

- Experienced Cyber Security Professional specializing in penetration testing for web applications and network infrastructure, adept at conducting comprehensive analyses, identifying vulnerabilities aligned with OWASP Top 10 standards, and delivering actionable risk assessments and remediation strategies to enhance organizational security postures.

Novin Kish (Core Banking) | Penetration Tester **August 2024 – Present**

- Conducting in-depth investigation and analysis of security vulnerabilities and risk factors within web-based banking applications to identify systemic weaknesses and propose robust mitigation strategies.

Bankino (Middle East Neo Bank) | Penetration Tester **2023 - Present**

- As a freelance penetration tester, I specialize in identifying and mitigating security vulnerabilities in mobile applications and Progressive Web Apps (PWAs), ensuring robust protection for client systems and user data.

Bugdasht (Bug Bounty Platform) | Penetration Tester **2023 - Present**

- Through Bugdasht, I actively engaged in bug hunting and attack surface management (ASM), identifying vulnerabilities and securing digital assets across various bug bounty programs.

COURSES & CERTIFICATES

Zero-PointSecurity

- Certified Red Team Ops

TryHackMe

- Certified in RedTeaming Path.

Data Analysis BootCamp at University of Tehran July 2022 – August 2022

- Successfully completed an intensive Data Analysis Bootcamp, gaining hands-on experience with industry-standard tools and techniques while working on data analysis projects using datasets from Torob and Tapsell.

TECHNICAL SKILLS

Programming Languages

- **Python**: Proficient in Python, utilizing it extensively for automating penetration testing workflows, scripting security assessments, developing custom tools for vulnerability detection and exploitation, and analyzing web application and network vulnerabilities. Experienced in leveraging Python libraries like Scapy, Requests, and Paramiko for advanced network analysis, web scraping, and SSH-based operations, as well as crafting proof-of-concept exploits and integrating APIs into testing environments.
- **C#**: Skilled in C#, with a focus on developing and testing secure .NET applications, building custom security tools, and performing in-depth code analysis for identifying vulnerabilities. Adept at creating Windows-based exploitation tools, reverse engineering .NET binaries, and simulating realistic attack scenarios to assess the robustness of enterprise-level applications against cyber threats.
- Additional Experience: Java, Golang and ReacJS.

Frameworks, Tools, and Libraries

- Proficient in using Metasploit Framework for exploit development and vulnerability testing, Burp Suite for web application security assessments, and Nmap Scripting Engine (NSE) for advanced network scanning and automation. Experienced with OWASP ZAP for comprehensive web application scanning and Impacket for network protocol analysis and exploitation.
- Skilled in leveraging tools like Nessus for vulnerability scanning and compliance auditing across diverse environments, Wireshark for deep packet inspection, John the Ripper and Hashcat for password cracking, and Aircrack-ng for wireless security assessments. Familiar with Hydra for brute-forcing, Netcat for networking diagnostics and reverse shell crafting, SQLmap for database exploitation, and BloodHound for Active Directory environment mapping.
- Expertise in Python libraries such as Scapy for network packet crafting, Requests and BeautifulSoup for web scraping, Paramiko for SSH-based automation, and Pwntools for binary exploitation. Proficient in using C# libraries like SharpSploit for offensive security tasks, System.Net for network programming, and Newtonsoft.Json for JSON parsing in .NET environments.