Ravindra Mahile

https://in.linkedin.com/in/ravindramahile

Email : ravimahile65@gmail.com
Mobile : +91-7067967717

Education

- **IET-DAVV Institute of Engineering Technology** — Indore, India
  M.Tech in Information Technology (Information Security); CGPA: 7.5 — *2024-2026*
- **BM College Of Technology** — Indore, India
  B.Tech in Computer Science and Engineering; CGPA: 7.3 — *2020-2024*

Experience

- **Bug Bounty Hunter**
  Hackerone and Bugcrowd — *Aug 2022 - Present*
  - **Links**: https://bugcrowd.com/h/ravimahile , https://hackerone.com/mrmahile
  - **Report Submissions**: Submitted 150+ valid security vulnerability reports across multiple private and public programs.
  - **Hall of Fame**: Achieved Hall of Fame status on Bugcrowd for reporting high-impact vulnerabilities. Industry Recognition: Acknowledged by major organizations including Shopify, Dell, BigCommerce, and the US Government for responsible disclosure.
  - **High-Impact Findings**: Reported critical issues such as IDOR, RCE, CSRF, and Broken Authentication affecting production systems.
  - **Tool Proficiency**: Leveraged tools like Burp Suite, Nuclei, and Garudrecon for reconnaissance and vulnerability validation.
- **Eggoz Nutrition**
  Data Security Intern — *Feb 2022 - May 2022*
  - **Collaboration**: Worked closely with cross-functional teams including developers and QA to address data security concerns.
  - **Web Application Security**: Tested and secured web applications by identifying weaknesses in authentication and data handling.
  - **Vulnerability Detection**: Discovered and reported critical issues such as Authentication Bypass and PII Leaks, contributing to overall system hardening.
  - **Security Best Practices**: Promoted and applied OWASP guidelines during code reviews and testing cycles.
  - **Reporting**: Documented vulnerabilities with risk analysis and recommended mitigations, supporting timely remediation by engineering teams.
- **Virtually Testing Foundation**
  Penetration Testing Intern — *Oct 2021 - Dec 2021*
  - **OWASP**: Completed OWASP Top 10 web application security fundamentals and best practices.
  - **Burpsuite**: Gained hands-on experience with Burp Suite, vulnerability scanning, and lab environment setup.
  - **Report Writing**: Learned penetration testing methodologies and professional report writing.
  - **Labs**: Practiced web application penetration testing in simulated lab environments.

Projects

- **InfosecPentest AI — AI-Powered Penetration Testing Platform**: Built an AI-powered penetration testing platform that automates 70 percent of security testing, including reconnaissance, vulnerability scanning, and exploit validation. Covers OWASP Top 10 vulnerabilities and provides proof-of-concept exploits along with remediation guidance for faster and more accurate security assessments.
- **Axion**: axion is a lightweight Go-based CLI tool for managing and executing SSH commands across multiple VPS instances defined in a YAML config.
- **hostname-extractor**: A high-performance Rust command-line tool for extracting hostnames from compressed JSONL files. This tool efficiently processes large .xz compressed files (40GB+) by streaming decompression in memory, never writing the decompressed file to disk.
- **Identifying API, Tokens, Credentials and Secrets Keys from Github Private and Public Repositories (Research in progress)**: Gitxpose scans public and private Git repositories to detect leaked API keys, tokens, and secrets. It helps you quickly identify and remediate credential exposure to prevent account compromise and data leaks.

Skills

- **Technologies**: Burpsuite, Nmap, Kali Linux, Subfinder, Shodan

Certifications and Achievements

- **TCS Hackquest Season 10 Top 25 Performance**
- **OCI Networking**