RAFLI PERMANA PUTRA

Penetration Tester | Security Analyst | Computer Science Student

Jogjakarta, Indonesia | https://www.imraflip.com | imraflip@gmail.com | +6285163636547

SUMMARY

Entry-level Penetration Tester and Computer Science student with hands-on experience through bug bounty, lab environments, cybersecurity bootcamp projects, and independent research. Familiar with common penetration testing tools, Linux-based security environments, and fundamental networking concepts. Experienced in documenting findings and producing structured technical reports.

EDUCATION

BINUS University | B.S. in Computer Science **2025 - Present**

Relevant interests: Cybersecurity, Network and Host Security, Web Application Security

Dibimbing | Cybersecurity Bootcamp **Sep 2025 – March 2026**

6-month intensive program focused on hands-on cybersecurity covering both Red Team and Blue Team domains, focusing on network security, vulnerability assessment and penetration testing, incident response, and digital forensics.

TECHNICAL SKILLS

- Operating Systems: Windows, Linux, Linux Command-line Interface
- Networking: OSI Model, TCP/IP, DNS, Virtualization
- Offensive Security: Reconnaissance & Enumeration, Vulnerability Assessment, Web Application Penetration Testing, OWASP Top 10, Network Security
- Pentesting Tools: Kali Linux, Burp Suite, Nmap, Metasploit
- Development & Tooling: HTML & CSS, JavaScript, C Programming, Python (Flask, FastAPI), Git, PostgreSQL

EXPERIENCE

Bug Bounty & VDP Participant **Jan 2024 - Present**

Independent

- Performed web application security tests that lead to vulnerability findings by focusing on OWASP Top 10 checks and Burp Suite pipelines.
- Identified multiple security issues such as misconfigurations and common web vulnerabilities during testing.
- Used tools like Burp Suite and browser-based testing techniques to analyze application behavior.
- Gained experience understanding duplicate reports, scope limitations, and responsible disclosure processes.

PROJECTS

Cybersecurity Bootcamp: Offensive Phase Final Project

- Conducted a full end-to-end web application penetration test, from reconnaissance and attack surface mapping to exploitation and professional reporting.
- Performed manual and automated reconnaissance to identify application endpoints, parameters, and hidden functionalities.
- Identified and exploited common OWASP Top 10 vulnerabilities (SQL Injection, XSS, IDOR, authentication/authorization weaknesses) using manual techniques and Burp Suite.
- Produced a structured penetration testing report including executive summary, technical findings, proof-of-concept exploitation, and remediation recommendations.

Personal Project: EternalBlue Exploitation

- Conducted a controlled network penetration testing in a lab environment.
- Achieved unauthenticated RCE via EternalBlue, demonstrating full system compromise.
- Documented findings and highlighted risks of legacy protocols and missing security patches in internal networks.