

Mufid Fata Rifki

Tangerang Selatan, Indonesia | mufidfata.rifki@gmail.com | +62 811-1673-370

[linkedin.com/in/mufid-fata-rifki](https://www.linkedin.com/in/mufid-fata-rifki) | pxilg.com | github.com/Pxilg

PROFESSIONAL SUMMARY

Information Technology student specializing in cybersecurity and purple teaming, combining offensive penetration testing with defensive network analysis and digital forensics. Strong foundation in Linux environments and security scripting, with a critical thinking approach to complex security problems. Active CTF competitor and bug bounty researcher with verified vulnerability disclosures against production web infrastructure.

EDUCATION

Bachelor of Information and Communication Technology (Hons)

Asia E University, Selangor, Malaysia | 2024-2028 | GPA 3.58

- Computing fundamentals, programming (Python, Java), operating systems, databases, computer networks, computer ethics and cyber law.
- Information System Audit project built on the .NET framework using C#, documenting and explaining the full audit workflow.

Diploma of Information Technology

CEP-CCIT Faculty of Engineering, Universitas Indonesia, Depok | 2024-present | GPA 3.69

- Professional cybersecurity program spanning network fundamentals, Linux, system penetration testing, server hardening, and SIEM simulation.

EXPERIENCE

Capture The Flag (CTF) Competitor

Independent | 2025-present

- Compete in local and international CTF events (player handle: pxilg) across reverse engineering, web exploitation, forensics, OSINT, cryptography, and steganography, all the way to the final
- Build custom Python automation and exploitation scripts using pwntools, Volatility, Impacket, BloodHound, and NetExec to solve challenges efficiently.
- Publish technical writeups and analysis on pxilg.com to document methodology and findings.

Bug Bounty / Vulnerability Disclosure Researcher

Independent | 2025-present

- Conduct authorized reconnaissance and web application testing against in-scope targets under public Vulnerability Disclosure Programs.
- Identify, validate, and responsibly report findings including access control flaws, information disclosure, and cross-site scripting.

HIGHLIGHTED PROJECTS

Real-Time Intrusion Alert and Active Response System (Wazuh + Telegram Bot)

- Built a SIEM lab on the open source Wazuh framework integrated with a Telegram bot for real-time alerting and interactive response.
- Simulated SSH brute force and suspicious traffic detection, with features for IP blocking, public IP and geo-IP lookup, alert summaries, and email reporting.

Exploiting MSSQL Misconfigurations for Active Directory Enumeration

- Conducted full-chain pentest practice in a virtual lab from recon to post-exploitation, leveraging leaked misconfigured MSSQL credentials with evil-winrm.

Python Log Forwarder with DoS Detection (Grafana + Loki)

- Simulated DoS traffic with hping3 and built a Python log forwarder, visualizing and analyzing traffic patterns through Grafana and Loki.

NOTABLE FINDINGS

- BMKG Vulnerability Disclosure Program: reported two exposed administrative panels on iklim.bmkg.go.id.
- BMKG Vulnerability Disclosure Program: reported cross-site scripting (XSS) vulnerabilities across three pages on iklim.bmkg.go.id.

CERTIFICATIONS

Professional: Certified Red Team Analyst (CRTA) - Cyberwarfare Labs; Certified Network Security Practitioner (CNSP) - The SecOps Group; Certified Social Engineering Defense Practitioner (CSEDP) - The SecOps Group; Pre Security (SEC0) and Cyber Security 101 (SEC1) - TryHackMe; SMT Program - INKOR.

Courses: Ethical Hacker, CyberOps Associate, Junior Cybersecurity Analyst Career Path, Introduction to Cybersecurity - Cisco; Web Fundamentals, Jr Penetration Tester, Pre Security, Advent of Cyber 2024 and 2025 - TryHackMe.

SKILLS

Hard Skills: Penetration Testing, OSINT, Digital Forensics, Network Analysis, Network Security, SIEM, Incident Response, Linux System Administration, Python and Bash scripting.

Soft Skills: Critical Thinking, Problem Solving, Adaptability, Teamwork and Collaboration.

Languages: Indonesian (native), English (intermediate).

HONORS & AWARDS

- Speaker, CCIT Induction Days 2025, representing the cybersecurity program to incoming students.