SETYA RAMADAN

Bekasi, Indonesia | +62 812 8896 8383 | ramveil.dev@gmail.com | https://ramveil.com | www.linkedin.com/in/setyaramadan28

SUMMARY

Cybersecurity student specializing in offensive security and web penetration testing. Experienced in identifying and exploiting real-world vulnerabilities through bug bounty programs and hands-on labs. Strong understanding of web application logic, enabling effective discovery of vulnerabilities such as XSS, misconfigurations, and authentication flaws. I have experience participating in CTF competitions and also building a foundation in security operations through the Cyber Ops Associate learning path.

EDUCATION

CEP-CCIT FTUI, Depok, Indonesia — August 2024 - Present
Professional Program in Information Technology (Cybersecurity)
GPA: 3.3

Asia e University, Selangor, Malaysia — September 2024 - Present
Bachelor of Information and Communication Technology (Honours)
Parallel Degree Program (Fully Online)
GPA: 3.56

PROFESSIONAL EXPERIENCE

Independent Security Researcher, Bug Bounty — October 2025 - Present

- Identified vulnerabilities including Stored XSS and debug misconfiguration in production applications
- Demonstrated impact leading to session compromise and data exposure
- Earned $370 bounty through responsible disclosure **(https://ramveil.com/writeups/bbp-mbmgroup/)**
- Discovered a critical broken access control vulnerability in a university LMS API, enabling a Student role to enumerate and modify other classroom metadata through unauthorized object-level PUT requests **(https://ramveil.com/writeups/bugonmyuni_pixelpath/)**
- Validated impact using Burp Suite with controlled proof-of-concept testing, responsible restoration, and a detailed remediation report for administrators

PROJECTS

Web Exploitation Writeups (ramveil.com)

- Published technical writeups on real-world vulnerabilities and CTF challenges
- Demonstrated exploitation techniques including XSS, authentication bypass, and logic flaws
- Focused on root cause analysis, manual testing, and impact assessment

Active Directory Attack Lab: Privilege Escalation & Credential Abuse

- Simulated an enterprise Active Directory environment and performed common attack techniques
- Conducted credential abuse and privilege escalation through misconfigurations
- Mapped attack paths and demonstrated domain compromise scenarios
- Tools: BloodHound, Impacket, Kerberoast

AI-Augmented SOC: Wazuh + Discord + LLM Integration

- Built a real-time monitoring pipeline using Wazuh SIEM and Discord alerts
- Integrated LLM to summarize and enrich security alerts automatically
- Simulated attack scenarios and validated detection and response workflow

Student Organization Web Application Security Testing (Work Locally)

- Identified SQL Injection and Stored XSS vulnerabilities in a web application
- Demonstrated authentication bypass using SQLi and payload execution via stored XSS
- Analyzed root causes including unsafe query construction and improper output rendering

Student Organization Data Management System (CLI Application)

- Developed a CLI-based system for managing member, event, and financial data
- Implemented authentication, role-based access (admin/user), and CRUD operations
- Designed relational database schema and integrated MySQL for data persistence

Windows Server Infrastructure Simulation (AD, DHCP, DFS, FSRM)

- Configured a simulated enterprise network with Active Directory and domain services
- Implemented DHCP failover, DFS replication, and file server resource management
- Designed network topology with main and branch servers for high availability

CERTIFICATIONS

- Practical Penetration Testing — Linuxhacking.id
- Junior Penetration Tester — TryHackMe
- Ethical Hacker — Cisco Networking Academy
- CyberOps Associate — Cisco Networking Academy
- Web Red Team Analyst — CyberWarFare Labs

SKILLS

- *Relevant Skills:*
  - Web Security: XSS, SQL Injection, Authentication Bypass, Logic Flaws
  - Active Directory: Privilege Escalation, Credential Abuse, Lateral Movement
  - Tools: Burp Suite, Nmap, ffuf, Gobuster, Impacket, Metasploit, Wireshark, SQLmap
  - Systems: Linux (Kali), Windows
  - Programming: Python (basic scripting), JavaScript (basic)
  - Concepts: OWASP Top 10, HTTP Protocol, Web Application Architecture

- *Language Skills:*
  - Indonesian (Native)
  - English (Intermediate)