

RIVALDO DOMINGGOS PARDEDE

Junior Penetration Tester | Red Team | Web, Mobile & Infrastructure Security

rivaldodominggos@gmail.com | +6282210460057 | linkedin.com/in/rivaldodominggos | github.com/rivaldodominggos | Bandung, Indonesia

PROFESSIONAL SUMMARY

Junior Penetration Tester on the Red Team at Temika Cyber, performing web, mobile, and infrastructure security assessments. Applies OWASP WSTG and MASTG methodology and retests findings to validate remediation. Discovered and responsibly disclosed a Critical (P1) Account Takeover vulnerability on a production university portal. 1st place winner in a national cybersecurity CTF. Hack The Box Academy Professional rank, Top 5% globally. Computer Science graduate (GPA 3.96/4.00), still active in CTFs and bug bounty outside work.

ACHIEVEMENTS & RECOGNITION

Critical (P1) Vulnerability Discovery: Account Takeover

Mar 2026

- Discovered and responsibly disclosed a Critical (P1) Account Takeover on *mahasiswa.usu.ac.id* via chained IDOR and Broken Access Control (OWASP A01:2021).
- Built a Burp Suite proof-of-concept showing full account takeover; reported with impact statement and remediation guidance.
- Received an official *Sertifikat Apresiasi* from Pusat Sistem Informasi Universitas Sumatera Utara (PSI USU).

1st Place: National Cybersecurity CTF "Siber Tangguh Bangsa Merdeka"

Aug 2025

- Team-based Capture The Flag competition focused on web security fundamentals and attack-surface exploration.

PROFESSIONAL EXPERIENCE

Junior Penetration Tester, Red Team

Aug 2026 - Present

Temika Cyber | Bandung, Indonesia (On-site)

- Perform mobile application penetration tests following the OWASP Mobile Application Security Testing Guide (MASTG).
- Perform web application penetration tests following the OWASP Web Security Testing Guide (WSTG).
- Retest web applications and infrastructure to validate remediation of previously reported findings.
- Document findings in reports with impact, reproduction steps, and remediation guidance.
- Preparing for upcoming wireless (Wi-Fi) penetration testing work.

Laboratory Coordinator, Computer Networking

Jan 2025 - Jun 2025

IKLC | Universitas Sumatera Utara | Medan, Indonesia

- Assisted and supervised hands-on networking labs covering TCP/IP, subnetting, and routing fundamentals for 20+ students per class.
- Guided students in analyzing network traffic with Wireshark and connecting theory with real-world network behavior.

Backend Development Trainee

Dec 2023 - Feb 2024

Indosat Ooredoo Hutchison (IDCamp) | Remote, Indonesia

- Built backend applications with Node.js: RESTful API design, authentication, and basic cloud services.
- Learned server-side fundamentals that inform secure client-server communication.

CYBERSECURITY TRAINING & HANDS-ON PRACTICE

Hack The Box Academy

Jan 2025 - Present

Self-driven training, Professional rank, Top 5% global

- Offensive web modules: SQL Injection, XSS, File Upload, Command Injection, Broken Authentication, Session Security, Web Attacks, GraphQL, and Ffuf-driven enumeration.
- Defensive modules: SIEM fundamentals, Windows Event Logs, digital forensics, and incident handling.
- Practiced pentesting methodology: reconnaissance, exploitation, post-exploitation, and reporting.

Hextree Android Security Path

Jan 2026 - Present

Self-driven training, in progress

- Static analysis of Android APKs with JADX and APKTool; runtime instrumentation with Frida.
- HTTP/HTTPS traffic interception with Burp Suite and mitmproxy.
- Intent attack surface analysis, Broadcast Receiver security, and Android bug bounty methodology.

TryHackMe

2024 - Present

Self-driven training, 47 rooms, Top 15%, 10 badges

- Covered pentesting fundamentals, OSINT, Windows and Linux privilege escalation, and forensics rooms.

LetsDefend

2025

Self-driven SOC and Blue Team training

- Completed SOC Fundamentals, Phishing Email Analysis, Detecting Web Attacks, and Linux for Blue Team.

Cisco Networking Academy

2024

Self-driven training via IDCamp

- Completed Introduction to Cybersecurity, Networking Basics, and Networking Devices and Initial Configuration.

TECHNICAL SKILLS

Web Application Security: OWASP Top 10, OWASP WSTG, IDOR, Broken Access Control (A01:2021), XSS, SQL Injection, Command Injection, File Upload, CSRF, Broken Authentication, Session Security, GraphQL attacks

Mobile Application Security: OWASP MASTG, Android reverse engineering (JADX, APKTool), Frida dynamic instrumentation, mobile network interception (Burp Suite, mitmproxy), Intent attack surface analysis, Broadcast Receiver security, Android bug bounty methodology (Hextree)

Infrastructure & Retesting: Network vulnerability assessment, remediation validation, vulnerability reporting, responsible disclosure, VAPT, pentesting lifecycle

Tools: Burp Suite (proxy, repeater, intruder), Nmap, Wireshark, Ffuf, SQLMap, Linux CLI, Git

Networking: TCP/IP, subnetting, routing fundamentals, DNS, HTTP/HTTPS, network traffic analysis

Blue Team / Defensive: SIEM fundamentals, incident handling, Windows Event Logs, digital forensics, phishing email analysis

Cryptography: Hybrid cryptosystems, RSA / XRSA, Salsa20, key management, authentication concepts (thesis work)

Secure Development Practices: Secure SDLC (CI version-gate, signed-release pipelines, base64 secret injection out of repo), source-code review (mentored 20+ students), dependency hygiene

Cloud-Adjacent Security: Production Firestore security rules (user-scoped, request.auth.uid bound), Firebase Auth error mapping, secret-injected CI/CD; Firebase = GCP family exposure

Compliance Awareness: OWASP ASVS, NIST CSF, MITRE ATT&CK, CVSS, POJK 11/2022, BI PADG 23/15/2021, PDP Law

Programming: Basic Python (automation), Bash, JavaScript (Node.js), PowerShell

Languages: English (professional), Bahasa Indonesia (native)

EDUCATION

Bachelor of Computer Science Aug 2022 - Jan 2026
Universitas Sumatera Utara

GPA: 3.96 / 4.00 · **Thesis:** Hybrid Cryptographic System Proof-of-Concept (XRSA + Modified Salsa20), focusing on key management, authentication concepts, and security-performance trade-offs.

SELECTED SECURITY WORK

Account Takeover via IDOR + Broken Access Control Mar 2026
OWASP A01:2021, Burp Suite, manual reconnaissance

- Identified an IDOR pattern in user-scoped requests of an authenticated portal through manual reconnaissance.
- Drafted the disclosure with reproduction steps, scope estimate, and remediation guidance for the system owner.

Hybrid Cryptographic System (XRSA + Modified Salsa20) 2025 - 2026
Bachelor's thesis, asymmetric and stream cipher hybrid

- Combined an extended RSA variant for key encapsulation with a modified Salsa20 stream cipher.

CERTIFICATIONS

Pre Security Path Certificate TryHackMe

PROFESSIONAL DEVELOPMENT (IN PROGRESS)

Preparing: Certified Penetration Testing Specialist (CPTS) and Certified Red Team Professional (CRTP). Not yet earned.

Ongoing: CTF competitions and bug bounty programs alongside professional work.