MOHAMMED FAHAD P

+91 7736535028 • mhdfahadp28@gmail.com • Kerala, India • LinkedIn • GitHub • Portfolio

PROFESSIONAL SUMMARY

Cybersecurity professional seeking a Penetration Tester or Security Analyst role with hands-on experience in web application and network penetration testing, API security analysis, and Active Directory attacks. Proven track record of identifying vulnerabilities through bug bounty and VDP programs, with expertise in VAPT, security automation, and custom offensive tool development using Go and Python.

TECHNICAL SKILLS

Offensive Security & VAPT: Web App Pentesting · Network Pentesting · VAPT · Exploitation · Post-Exploitation · Privilege Escalation

Penetration Testing Tools: Burp Suite Pro · Nmap · Netcat · Metasploit · SQLMap · Gobuster · Nikto · OWASP ZAP · Wireshark · Kali Linux

Web & API Security: OWASP Top 10 · XSS · CSRF · SSRF · IDOR · CORS · Authentication Bypass · API Security · Business Logic Flaws

Programming & Automation: Go · Python · Bash · C/C++ — offensive tool development, exploit scripting, security automation

EXPERIENCE

Cyber Security Intern | Future Interns *2026*

- Conducted vulnerability assessments on live websites using Nmap and OWASP ZAP, classifying risks (Low/Medium/High) and delivering detailed remediation reports
- Performed phishing email analysis identifying spoofed senders, fake domains, and malicious links, producing client-ready threat awareness documentation
- Executed API security testing via Postman and Browser DevTools, uncovering authentication flaws, insecure endpoints, and missing rate-limiting controls

Freelance VAPT Consultant & Security Researcher | Independent *2025 – Present*

- Discovered 10+ confirmed vulnerabilities through bug bounty and VDP programs, with full proof-of-concept and remediation documentation
- Performed web application VAPT across multiple targets, identifying OWASP Top 10 flaws including XSS, SSRF, IDOR, authentication bypass, and business logic vulnerabilities

PROJECTS

JSRecon — JavaScript Endpoint & Secret Extraction Tool *(Go)*

- Offensive recon tool extracting hidden API endpoints, parameters, and hardcoded secrets from JavaScript files using regex and AST parsing; outputs structured JSON for pentest engagements

PassGuard — Password Strength Analyzer *(Go)*

- Rule-based password analysis utility with weak pattern detection — built for offensive research use cases with ethical safeguards against plaintext credential exposure

PLATFORMS & LABS

- PortSwigger Web Security Academy — Completed 20+ PortSwigger Web Security Academy labs in advanced XSS, SSRF, authentication bypass, and business logic exploitation.

CERTIFICATIONS

- **Certified Penetration Tester v3 (CPTv3)** — Red Team Hacker Academy (2025)
- **Google Cybersecurity Professional Certificate** — Google (2026)

EDUCATION

Bachelor of Computer Applications (BCA) | University of Calicut, Kerala *2022 – 2025*