MUHAMMAD SHADLY M

Malappuram, Kerala, India
📞 80753 25753
✉️ shadlymaliyekkalofficial80@gmail.com
🔗 linkedin.com/in/shadly-maliyekkal-653a38376

PROFESSIONAL SUMMARY

Cybersecurity professional with hands-on internship experience across **application security, network security, and SOC fundamentals**, including **Web, API, and Android penetration testing**. Experienced in identifying **OWASP Top 10 and OWASP Mobile Top 10** vulnerabilities through manual testing, static and dynamic analysis. Familiar with **log analysis, basic incident triage, Linux security, and core networking concepts**. Strong in technical documentation, vulnerability reporting, and continuous learning in offensive and defensive security domains.

TECHNICAL SKILLS

Application & API Security

- Web, API, and Android application penetration testing
- OWASP Top 10 & OWASP Mobile Top 10
- Authentication & authorization testing
- Insecure data storage, misconfigurations, access control issues

Network & Infrastructure Security

- Network reconnaissance and service enumeration
- TCP/IP, DNS, HTTP/HTTPS
- Firewalls, routing fundamentals
- Linux system hardening (basics)

SOC & Blue Team Fundamentals

- Log analysis (Linux and web server logs)
- Basic incident identification and alert triage
- Understanding of attack stages and common threat behavior

Security Tools

- Burp Suite, MobSF, OWASP ZAP
- Nmap, Nikto, Wireshark
- ADB, Frida

Scripting & Platforms

- Python (fundamentals), Bash (basics)
- Kali Linux, Ubuntu, Windows

PROFESSIONAL EXPERIENCE

Application Security Intern (Android, Web & API)

Xyvin Technologies | Sep 2025 – Nov 2025

- Performed **static and dynamic penetration testing** of Android applications using MobSF, Frida, ADB, and Burp Suite
- Identified vulnerabilities such as **insecure data storage, weak authentication, improper permissions, and insecure network communication**
- Conducted **API security testing** to identify authorization flaws and access control weaknesses
- Assisted in testing application workflows and validating exploitation scenarios
- Documented findings with **severity ratings, proof of concept, impact analysis, and remediation recommendations**
- Collaborated with senior testers to review results and improve testing accuracy
- Followed **OWASP MASVS** and **OWASP Mobile Top 10** during assessments

---

PROJECTS

Web Application Security Assessment

- Conducted structured web penetration testing using Burp Suite, OWASP ZAP, and Nikto
- Identified OWASP Top 10 vulnerabilities including XSS, SQL injection, and security misconfigurations
- Prepared a professional vulnerability assessment report with risk classification and remediation guidance

Android Application Security Audit

- Performed static and dynamic analysis using MobSF, Frida, and ADB
- Identified insecure components, weak storage mechanisms, and unsafe network traffic
- Documented findings aligned with OWASP Mobile Top 10 and MASVS controls

WordPress Incident Restoration

- Investigated and restored a compromised WordPress website
- Identified malicious files and vulnerable plugins responsible for compromise
- Implemented security hardening measures, configuration fixes, and patch updates

CERTIFICATIONS

- Certified Penetration Tester (CPT)
- Ethical Hacker — Cisco
- Cyber Threat Management — Cisco

EDUCATION

Certified Penetration Tester (CPT)
CC Cyber Campus, Calicut — 2025

Higher Secondary (Biology Science)
DUHSS Panakkad, Malappuram — 2024

Currently Pursuing

- CEH (Certified Ethical Hacker)
- Bachelor of Computer Applications (BCA)

CORE COMPETENCIES

Analytical Thinking · Technical Documentation · Accountability · Communication
Adaptability · Problem Solving · Continuous Learning in Cybersecurity