Mohammed Assad

✉ asdtriada@gmail.com   in linkedin.com/in/asd-assad-632676308   github.com/Ro0tk1e

Cybersecurity practitioner and Capture The Flag (CTF) developer specializing in web exploitation, cryptography, steganography, and Android reverse engineering. Skilled in building secure environments, automating analysis pipelines, and developing reproducible labs for training, competitions, and community workshops. Passionate about vulnerability assessment, ethical hacking, and incident response.

Technical Skills

- **Security Domains:** Web application security, penetration testing, network security, cryptography, steganography, reverse engineering, digital forensics.
- **Security Tools:** Burp Suite, Wireshark, Metasploit, Apktool, Ghidra, Nmap, Netcat, Kali Linux, OWASP ZAP, TryHackMe, Hack The Box.
- **Core Competencies:** Vulnerability analysis, exploit development, malware analysis, incident response, OSINT research, secure coding practices.

Experience

CTF Lead & Security Researcher **2024–Present**
Yenepoya University, Bengaluru

- Organized and led an inter-college Capture The Flag competition with 70+ participants; designed 10+ challenges across cryptography, steganography, and web exploitation.
- Developed reusable security playbooks and walkthroughs for vulnerability exploitation, Android reverse engineering, and OSINT-based investigations.
- Reverse-engineered OWASP Uncrackable Apps (Lv 1–3) using Apktool, `smali` code modification, `zipalign`, and `jarsigner`; documented patching workflow and verification.
- Built isolated sandbox environments for vulnerability demonstration and exploit chain testing, improving lab stability and reducing setup time by 40%.
- Collaborated with Null Bangalore community on security workshops

Technical Projects

- **Multi-Stage CTF Challenge Pack:** Designed end-to-end puzzle integrating EXIF-based image steganography, audio LSB extraction, and OSINT location tracing; deployed for training and classroom events with automated SHA-256 verification.
- **Android Reverse Engineering Pipeline:** Automated Apktool → `smali` patching → `zipalign` → `jarsigner` to streamline APK analysis, reducing manual effort by 60%.
- **Vulnerability Lab Infrastructure:** Built virtualized testbed for common CVE exploitation and patch verification; supported web, Android, and IoT-based labs.

Education

Bachelor of Computer Applications (BCA) — Cybersecurity, Ethical Hacking & Digital Forensics **2023–2026**
Yenepoya (Deemed to be University), Bengaluru

Certifications

- Cisco — Introduction to Cybersecurity.
- Simplilearn — CEH v12 Practice Labs.
- Coursera — Google Cybersecurity Professional Certificate.
- Coursera — Introduction to Ethical Hacking.

Achievements

- Organized a 70+ participant university-level CTF event with zero flag leakage and on-time challenge deployment.
- Completed OWASP Uncrackable Apps (Lv 1–3) and documented reproducible reversing workflows.
- Recognized by peers for excellence in Android reverse engineering and CTF challenge design.

Interests

CTF challenge creation, Android reverse engineering, exploit development, OSINT investigations, cybersecurity research, and community-driven security workshops,martial arts,dance,basketball.