Rohit Kumar

linkedin.com/in/rohitkumar384
github.com/r04i7

er.rohitkumar1410@gmail.com
Mobile: 6290342545
Bengaluru, Karnataka, India

PROFESSIONAL SUMMARY

Senior Application Security Engineer with 5+ years of experience specializing in web application security, mobile penetration testing, API security assessments, and CVE research across banking, e-commerce, and enterprise environments. Proven track record of identifying critical vulnerabilities and delivering executive-level remediation roadmaps.

EXPERIENCE

- **Black Duck (Synopsys)** — Bengaluru, Karnataka
  Senior Security Consultant — *Mar 2025 – Present*
  - **Assessment Leadership: Direct** end-to-end security assessments for enterprise clients, covering penetration testing, threat modeling, and remediation validation across web, mobile, and API platforms.
  - **Mobile Security:** Execute advanced iOS and Android security testing, identifying critical authentication bypass and data leakage vulnerabilities in **40+ mobile applications**.
  - **Strategic Impact:** Deliver executive-level security reports and remediation roadmaps to C-suite stakeholders, improving client security posture by **45%**.
  - **Mentorship:** Mentor a team of 5 junior security consultants on OWASP methodologies, secure coding practices, and vulnerability exploitation.
  - **Automation: Design** scalable security testing frameworks using **Python and Bash**, reducing manual testing time by **30%**.

- **Black Duck (Synopsys)** — Bengaluru, Karnataka
  Security Consultant — *Sep 2024 – Mar 2025*
  - **Web Security:** Executed **80+ comprehensive web application assessments** for banking and fintech clients, identifying high-severity vulnerabilities including IDOR, XXE, and SQL injection.
  - **API Testing:** Completed **50+ RESTful and GraphQL API penetration tests**, uncovering business logic flaws and broken authentication mechanisms.
  - **Efficiency:** Reduced false positive rates by **35%** through the implementation of validation workflows and script-based vulnerability verification scripts.
  - **DevSecOps:** Collaborated with **10+ development teams** to integrate security best practices into CI/CD pipelines, ensuring **SOC2 and GDPR compliance**.
  - **Training:** Facilitated security awareness training sessions for **200+ developers** on secure coding and OWASP Top 10 vulnerabilities.

- **Synopsys Inc** — Bengaluru, Karnataka
  Security Service Associate — *Mar 2022 – Sep 2024*
  - **Vulnerability Discovery: Uncovered** and reported **3 CVEs** (CVE-2024-35581, CVE-2024-35582, CVE-2024-35583) published in MITRE and NVD databases.
  - **Audit Volume:** Orchestrated **160+ web application penetration tests** and **70+ mobile security audits** across e-commerce and healthcare sectors.
  - **Threat Modeling:** Directed threat modeling and architecture reviews for 30+ cloud-native applications, reducing the attack surface by **40%**.
  - **Tool Development:** Engineered custom security automation tools in Python for reconnaissance and reporting, improving efficiency by **25%**.
  - **Triage:** Triaged and validated **500+ security findings** from commercial scanners to ensure accurate risk assessment.

- **CSCC LABS** — Hyderabad, Telangana
  Cyber Security Analyst — *Jul 2021 – Mar 2022*

- ○ **Penetration Testing:** Managed engagements for **40+ web applications**, identifying OWASP Top 10 vulnerabilities and business logic flaws.
- ○ **Infrastructure Security:** Assessed network security and configuration reviews, identifying misconfigurations in **60+ systems**.
- ○ **Incident Response:** Spearheaded forensic analysis for security breaches, reducing mean time to resolution by **50%**.

- **CSCC LABS** Hyderabad, Telangana
  Cyber Security Intern *Feb 2021 – Jul 2021*
  - ○ **Assessment Support:** Supported vulnerability assessments for 20+ client applications and performed reconnaissance using OSINT techniques for **15+ targets**.

PROJECTS & RESEARCH

- **CVE Research & Vulnerability Disclosure**: Discovered and responsibly disclosed **3 CVEs** (CVE-2024-35581, CVE-2024-35582, CVE-2024-35583). Conducted zero-day vulnerability research in web applications and open-source software.
- **Security Automation Tools**: Developed open-source security tools for penetration testing automation, vulnerability scanning, and exploit development (available on GitHub). Created custom scripts for reconnaissance and post-exploitation.

TECHNICAL SKILLS

- **Security Testing**: Web App Penetration Testing, Mobile Security (iOS/Android), API Security, VAPT, Source Code Analysis (SCA), Network Security

- **Tools & Frameworks**: Burp Suite Pro, OWASP ZAP, Postman, MobSF, JADX, Apktool, 3uTools, Objection, Frida, Genymotion, Metasploit

- **Standards**: OWASP Top 10, OWASP Mobile Top 10, CWE/SANS 25, SOC2, GDPR, Secure SDLC

- **Languages**: Python, Bash, Java, C++

CERTIFICATIONS

- Offensive Security Certified Professional (OSCP) [Pursuing]

- Certified Ethical Hacker (CEH)

- Licensed Penetration Tester (LPT)

EDUCATION

- **Punjab Technical University** Jalandhar, Punjab
  Bachelor of Technology in Computer Engineering *2016 – 2020*