

ROHIT KUMAR

Senior Application Security Engineer

Kolkata, West Bengal, India | 6290342545 | er.rohitkumar1410@gmail.com

[linkedin.com/in/rohitkumar384](https://www.linkedin.com/in/rohitkumar384) | github.com/r04i7

PROFESSIONAL SUMMARY

Senior Application Security Engineer with 5+ years of experience across web application security, mobile penetration testing (iOS/Android), API security assessments, source code analysis (SCA), and CVE research in banking, e-commerce, and enterprise environments. Skilled at building internal security automation tools, leading assessment teams, and translating technical findings into executive-level remediation roadmaps. Currently a Senior Associate at PwC, with prior experience at Black Duck (Synopsys) and Synopsys Inc., where 3 CVEs were discovered and published in MITRE/NVD.

PROFESSIONAL EXPERIENCE

PwC | Senior Associate

Mar 2026 – Present

- Conduct web application, Android, iOS, and API penetration testing and source code analysis (SCA) for enterprise clients across multiple industries.
- Built an internal Burp Suite extender tool to help the assessment team manage and track flagged/hidden issues more efficiently, streamlining the vulnerability triage workflow.
- Developed a session cookie analysis tool to identify session management weaknesses during web application assessments.
- Contribute to building internal security automation tooling to support penetration testing and reporting workflows.

Note: Synopsys Software Integrity Group (SIG) was divested and became Black Duck Software in 2024 — the roles below reflect one continuous tenure through that transition.

Black Duck (Synopsys) | Senior Security Consultant

Mar 2025 – Mar 2026

- Directed end-to-end security assessments for enterprise clients, covering penetration testing, threat modeling, and remediation validation across web, mobile, and API platforms.
- Executed advanced iOS and Android security testing, identifying critical authentication bypass and data leakage vulnerabilities in 40+ mobile applications.
- Delivered executive-level security reports and remediation roadmaps to C-suite stakeholders, improving client security posture by 45%.
- Mentored a team of 5 junior security consultants on OWASP methodologies, secure coding practices, and vulnerability exploitation.
- Designed scalable security testing frameworks using Python and Bash, reducing manual testing time by 30%.

Black Duck (Synopsys) | Security Consultant

Sep 2024 – Mar 2025

- Executed 80+ comprehensive web application assessments for banking and fintech clients, identifying high-severity vulnerabilities including IDOR, XXE, and SQL injection.
- Completed 50+ RESTful and GraphQL API penetration tests, uncovering business logic flaws and broken authentication mechanisms.
- Reduced false positive rates by 35% through validation workflows and script-based vulnerability verification.
- Collaborated with 10+ development teams to integrate security best practices into CI/CD pipelines, ensuring SOC2 and GDPR compliance.
- Facilitated security awareness training for 200+ developers on secure coding and the OWASP Top 10.

Synopsys Inc. | Security Service Associate

Mar 2022 – Sep 2024

- Discovered and reported 3 CVEs (CVE-2024-35581, CVE-2024-35582, CVE-2024-35583), published in the MITRE and NVD databases.

- Orchestrated 160+ web application penetration tests and 70+ mobile security audits across e-commerce and healthcare sectors.
- Directed threat modeling and architecture reviews for 30+ cloud-native applications, reducing attack surface by 40%.
- Engineered custom Python security automation tools for reconnaissance and reporting, improving efficiency by 25%.
- Triageed and validated 500+ security findings from commercial scanners to ensure accurate risk assessment.

CSCC Labs | Cyber Security Analyst

Jul 2021 – Mar 2022

- Managed engagements for 40+ web applications, identifying OWASP Top 10 vulnerabilities and business logic flaws.
- Assessed network security and configurations, identifying misconfigurations across 60+ systems.
- Spearheaded forensic analysis for security breaches, reducing mean time to resolution by 50%.

CSCC Labs | Cyber Security Intern

Feb 2021 – Jul 2021

- Supported vulnerability assessments for 20+ client applications and performed OSINT-based reconnaissance 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: Built a Burp Suite extender for managing flagged/hidden issues and a session cookie analysis tool, alongside open-source penetration testing automation, vulnerability scanning, and exploit development scripts (available on GitHub).

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

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