HARSH BHETARIA

Email: harsh@mail.hnbhetaria.com | **Phone:** (347) 668-7172 | **Location:** Indianapolis, IN
LinkedIn: https://www.linkedin.com/in/harsh-bhetaria/ | **Website:** https://hnbhetaria.com | **GitHub:** https://github.com/hbhetaria2611

PROFESSIONAL SUMMARY

Lead Product Security Engineer with 10+ years of experience in threat modeling, security design reviews, and vulnerability assessment. Proven track record in web application security, mobile security, and infrastructure security across enterprise environments. Specialized in incident response, penetration testing, and secure software development lifecycle (SDLC) implementation.

CORE COMPETENCIES

Security Technologies: Threat Modeling, Penetration Testing, Vulnerability Assessment, Static Application Security Testing (SAST), Dynamic Application Security Testing (DAST), Security Code Review
Programming Languages: Python, Go, Hack, JavaScript, SQL
Security Tools: Burp Suite Professional, OWASP ZAP, Nessus, Qualys, SonarQube, Checkmarx
AI/Automation Tools: Claude Code, Google Gemini, Cursor, Windsurf, GitHub Copilot, ChatGPT for security automation and code analysis
Platforms & Frameworks: AWS Security, Cloud Security, API Security, Mobile Security (iOS/Android)
Methodologies: Secure SDLC, DevSecOps, Agile Security, Risk Assessment, Compliance (SOX, PCI DSS)

PROFESSIONAL EXPERIENCE

Senior Product Security Engineer | Slack Technologies

May 2022 - Present

- Lead product security initiatives for 20+ million daily active users, ensuring data protection and privacy compliance across platform integrations
- Conduct comprehensive threat modeling and security design reviews for new features, reducing security vulnerabilities by 40% pre-deployment
- Serve as Subject Matter Expert (SME) for security incidents, providing technical leadership and remediation guidance for critical security events

- Leverage AI-powered tools including Claude Code and Google Gemini to automate security processes, code analysis, and vulnerability detection workflows
- Collaborate with cross-functional engineering teams to implement security controls and secure coding practices throughout SDLC
- Perform security code reviews and static analysis for critical applications using automated tools and manual assessment techniques
- Develop and maintain security standards, guidelines, and best practices for product development teams

Security Engineer II - Device Security | Amazon Lab126

June 2021 - May 2022

- Enhanced security posture of Amazon Fire TV devices serving 50+ million users through comprehensive security assessments and threat modeling
- Led incident response for Severity-1 security incidents, achieving 30% reduction in mean time to resolution (MTTR)
- Implemented security requirements during design phase of SDLC, improving baseline security controls and ensuring compliance with privacy regulations
- Conducted security design reviews and penetration testing for IoT devices and embedded systems
- Collaborated with hardware and firmware teams to identify and remediate security vulnerabilities in consumer electronics

Senior Security Consultant | Synopsys, Inc

August 2015 - June 2021

- Led team of 5-8 security consultants, providing mentorship and technical training that resulted in 90% team retention and career advancement
- Conducted 200+ penetration tests across web applications, mobile applications (iOS/Android), and thick client applications for Fortune 500 clients
- Identified and reported critical and high-severity vulnerabilities, helping clients reduce security risk by average of 60%
- Designed and implemented comprehensive technical training program for new hires, improving onboarding efficiency by 40%
- Performed application security assessments using OWASP methodology and industry-standard security testing frameworks

EDUCATION

Master of Science in Cybersecurity
New York University | July 2013 - May 2015

Bachelor of Technology in Information Technology
CHARUSAT University | July 2009 - May 2013

CERTIFICATIONS

Certified Information Systems Security Professional (CISSP)
ISC2 | Credential ID: e1f87739-2954-481d-bcc2-12ca7f2c290a | September 2024

ADDITIONAL QUALIFICATIONS

- Experience with cloud security (AWS, Azure, GCP) and container security (Docker, Kubernetes)
- Knowledge of regulatory compliance frameworks (SOC 2, PCI DSS, GDPR, CCPA)
- Proficient in AI-assisted development and security automation using Large Language Models (LLMs)
- Experience with prompt engineering for security use cases and automated threat detection
- Published security research and vulnerability disclosures
- Active participant in security community and bug bounty programs