Samkit H Shah

✉ samkitshah.in@gmail.com   📞 +1 2014231751   🔗 samkitshah.in

Education

New York University, Masters in Cybersecurity   *Aug. 2023 to May 2025*
- GPA: 3.8/4.0; Member at OSIRIS Cyber Security Lab; Graduate Assistant at CSE Department; TA for Appsec Course

NMIMS, B Tech in Computer Engineering   *July 2017 to May 2023*
- GPA: 3.58/4.0; Student Ambassador Award

Technical Skills

Languages & Frameworks: Python, JavaScript, PHP, C++, Java, SQL, Bash, Node.js, React.js, Flask, Laravel, Go

Security & Pentesting: VAPT, Threat Modeling, Secure Code Review, API & Network Security, OWASP Top 10, Static & Dynamic Analysis, LLM Security, AI Threat Modeling, Model Inversion Attacks, Prompt Injection Testing

Cloud, DevOps & Tools: AWS, GCP, Firebase, Docker, CI/CD, GitHub Actions, MySQL, MongoDB, PostgreSQL, Burp Suite, Nmap, Hashcat, Metasploit, Wireshark, OSINT, Splunk, WAF, Nessus, Semgrep

Experience

Security Developer, (CTFd LLC - NY ☑)   *Jan. 2024 to May 2025*
- Developed real-world CTF challenges covering **OWASP Top 10** and advanced exploits, improving security education for **5,000+ players** and **enhancing secure coding skills**, leading to reduction in security vulnerabilities within their code.
- Built cybersecurity challenges tailored for non-technical users, improving their understanding of **phishing, social engineering, and data protection**, increasing security awareness.

Cybersecurity Specialist & Software Security Engineer   *Nov. 2020 to present*
- Architected and secured enterprise-grade software solutions for **30+ clients** across IT, Finance, and Manufacturing, integrating **penetration testing, secure coding, and threat intelligence**, preventing **$500K+** in potential security breaches.
- **Co-founded** and led development at **The Breakout Hunt** ☑, India's first breakout scanner native app with real-time stock alerts, while applying secure coding, adhering to a security-first SDLC, and deploying robust CI/CD pipelines.
- **Collaborated with security teams and SDEs** to implement AI-driven security solutions, reducing threat exposure by 25% and cutting manual security costs by 40%, safeguarding businesses from financial and reputational risks.
- Enhanced application security by implementing **data encryption, API hardening, runtime integrity checks, and continuous threat monitoring**, reducing security flaws by **40%** and ensuring compliance with industry standards.

Software Security Analyst, (Ithaca Clean Energy - NY ☑)   *Sept. 2024 to Dec. 2024*
- **Conducted VAPT and source code analysis,** uncovering **10+ critical vulnerabilities** and ensuring compliance with NIST & OWASP standards, collaborating with developers to remediate security flaws.
- Designed security automation tools,enhancing **vulnerability detection and threat response**, reducing security risks, and improving remediation speed in coordination with security and engineering teams.

Cyber Security Analyst, (Mahen Technologies)   *Dec. 2021 to Mar. 2023*
- Led security assessments across **15+ applications and 10+ networks** using gray-box testing, uncovering high-risk vulnerabilities and strengthening cloud and network security.
- Directed security investigations for **MNCs and government agencies,** identifying critical threats and spreadheading a **4-member team** to mitigate risks and enhance infrastructure security.
- Delivered **100+ hours of security training,** upskilling corporate teams and students on **secure coding, threat modeling, incident response, and zero trust architecture**, improving security awareness across organizations.

Software Developer Intern, (Cart Geek ☑)   *Dec. 2020 to May 2021*
- **Optimized backend performance and enhanced security,** reducing processing time by **20%** and improving scalability, while leading cross-functional teams to achieve **60% speed optimization** and earning the **'Intern of the Year' award**.

Projects

CTFc - AI Security Analysis Agent
- Created an autonomous analysis framework for automated web reconnaissance, source code vulnerability analysis, and step-by-step solution guidance, providing users with an initial attack pathway and structured insights for exploitation.

CTF Developer, BSides NYC & CSAW:
- Authored CTF challenges for cybersecurity competitions, applying real-world attack and defense techniques to improve hands-on security training.

Prompt Injection Testing on Lakera AI's Gandalf
- Explored prompt injection vulnerabilities by progressing to level 7 (top 8% of players) on the AI security challenge at Gandalf by Lakera AI, gaining hands-on experience with adversarial inputs and AI security.

Certifications And Awards

- **Security Researcher at BugCrowd:** For ethically reporting security bugs and received bounties and appreciations.
- **Winner, LLM CTF Attack Challenge, CSAW :** Solving CTF challenges with generative autonomous AI framework.