Anagha Shyama Prakash

Los Angeles, CA | shyama.prakash.anagha@gmail.com
anagha.dev | linkedin.com/in/anagha-shyama-prakash | github.com/S-Anagha

EDUCATION

University of Southern California
Master of Science, Computer Science - Los Angeles, CA | Jan 2025 - Dec 2026
- **Relevant Coursework:** Security Systems, Software Engineering for Security, Adversarial Machine Learning, Information Retrieval

Visvesvaraya Technological University
B.E. (Hons.) in Computer Science and Engineering - Bangalore, India | Sep 2019 - Jun 2023
- **Relevant Coursework:** Computer Networks & Security, Cryptography, Distributed Systems, Unix Programming, Operating Systems

TECHNICAL SKILLS

- **Programming:** Python, Bash, JavaScript (Node.js), Go, SQL, PowerShell
- **Application Security:** Penetration testing, vulnerability research, API security, OWASP Top 10, threat modeling
- **Security Tools:** Burp Suite, OWASP ZAP, Nmap, Metasploit, Wireshark, Snort, Postman, Splunk, Caldera, Atomic Red Team
- **Frameworks:** MITRE ATT&CK, CVSS
- **Systems:** Linux, Docker, Kubernetes, AWS, Azure, Google Cloud
- **Networking:** HTTP, TCP/IP, DNS, REST APIs, authentication and authorization

EXPERIENCE

Security Software Engineer Intern
Lumina AI Health Institute - Marina del Rey, CA | Jun 2025 – Sep 2025
- Identified and exploited application logic flaws in REST APIs to uncover Insecure Direct Object Reference, Authentication Bypass, and injection vulnerabilities using Burp Suite
- Reproduced exploit paths end-to-end and worked with developers to fix access control and input validation weaknesses in a healthcare platform
- Added audit logging around sensitive endpoints to expose abnormal access patterns and support incident response

Cybersecurity Analyst
SISA Information Security - Bangalore, India | Jul 2023 - Aug 2024
- Investigated 500+ real-world attacks using Splunk, IDS, and WAF logs across web and cloud systems
- Analyzed attacker behavior including brute force, scanning, and lateral movement using HTTP and network telemetry
- Tuned 30+ detection rules in Snort and ModSecurity to better capture real attack patterns

Attack Simulation Intern
SISA Information Security - Bangalore, India | Sep 2022 - Apr 2023
- Conducted 200+ penetration tests on web applications and cloud systems using Nmap, Metasploit, and custom scripts
- Exploited SQL injection, cross-site scripting, and IAM misconfigurations to demonstrate real impact and support remediation
- Simulated adversary behavior by mapping techniques to MITRE ATT&CK and executing attack scenarios using Caldera and Atomic Red Team
- Developed Python and Bash scripts to automate payload execution and streamline security testing workflows

VULNERABILITY RESEARCH

USC Cyborg Club
Vulnerability Researcher | Jan 2025 – Present
- Actively test web applications and APIs using Burp Suite to identify flaws in authentication, authorization, and input handling
- Performed API fuzzing, JWT manipulation, and SSRF testing using Burp Suite and custom scripts to evaluate application behavior under adversarial inputs

PROJECTS

API Sentinel – Modular API Security Scanner
- Built a Python-based CLI tool to perform automated security testing of REST APIs, implementing four modules targeting injection flaws, authentication weaknesses, and access control vulnerabilities
- Designed and executed 100+ payload permutations per endpoint to simulate real-world API abuse scenarios, enabling efficient discovery of misconfigurations and reducing manual testing effort

CodeForesight – AI-Driven Vulnerability Analysis System | AI for Security
- Developed a multi-stage pipeline using CVE and OWASP datasets to analyze over 1,000 vulnerabilities, classifying them based on exploitability, attack surface, and potential impact
- Modeled attacker behavior by combining machine learning outputs with language model reasoning to identify vulnerable code patterns and generate context-aware remediation insights

CanaryRAG – Security Defense for Retrieval-Augmented Generation | Security for AI
- Designed an adversarial testing framework using 200+ synthetic canary documents to simulate data poisoning, prompt injection, and unauthorized data access in RAG systems
- Implemented multi-signal tracking across retrieval rankings, embedding similarity, and query patterns to detect persistent attack behavior and reduce false positives during adversarial testing

SECURITY ACHIEVEMENTS

- **Winner, Adventure of Triads Statewide Capture The Flag Competition (2× winner)**
- **Selected for WiCyS Security Training Scholarship; completed SANS BootUp CTF**