Email: bharathsur97@gmail.com
Cell: +1 9172946243

Bharath Suresh

https://www.github.com/bharaths97
Linkedin: Bharath Suresh

Education

- **Rochester Institute of Technology** | ***MS Cybersecurity*** Aug 2021–May 2024 | Rochester, New York
- **SASTRA University** | ***B.Tech Electronics Engineering*** Jul 2015–Aug 2019 | Thanjavur, India

Skills

Domains: Penetration Testing, Offensive Security, Purple Teaming, Threat Modeling, Secure Coding, Memory Safety, Web Security, AI Security, Security Automation, Cloud Security, Cryptography

Programming/Scripting Languages: C/C++, Python, Java, Objective-C, PowerShell, Bash

Tooling: Burp Suite, ffuf, Hashcat, Metasploit, Nmap, Wireshark, Semgrep, Git, Ghidra

Platforms & Protocols: AWS, Windows, macOS, Linux, HTTP(S), TLS, TCP/IP, DNS

Professional Experience

- **Bureau Veritas Cybersecurity NA** | ***Security Engineer I*** **Jan 2025–Jan 2026 | Seattle, WA**
  - Delivered penetration testing engagements for AWS service teams, presenting exploit demonstrations and actionable remediation guidance to engineering stakeholders.
  - Identified and supported remediation of 100+ security vulnerabilities across 25+ production services, providing root-cause analysis and secure design recommendations.
  - Performed manual code reviews and dependency analysis across 120+ repositories, uncovering logic flaws, insecure authentication flows, and privilege-escalation paths not detectable via automated tooling.
  - Conducted adversarial testing on 5+ AWS internal AI-integrated services, identifying prompt injection vectors, data poisoning risks, and security weaknesses in agent and orchestration workflows.
  - Correlated findings across source code, API fuzzing, configurations, and service logs to construct multi-step attack chains, escalating low-severity weaknesses into high-impact vulnerabilities.
  - Reviewed threat model design documents to identify abuse cases, trust-boundary violations, and control gaps.
  - Developed 30+ automation scripts to simulate adversary behavior, validate security control effectiveness, and reduce manual effort across engagements.
- **WinWin Labs** | ***Security Engineer*** **Aug 2024–Jan 2025 | Remote, New York**
  - Conducted security testing of 20+ API endpoints, identifying flaws leading to sensitive data exposure vulnerabilities.
  - Discovered a critical authentication logic vulnerability with potential for large-scale account compromise.
- **Zoho Corporation** | ***Software Development Engineer*** **Jun 2019–Jul 2021 | Chennai, India**
  - Led native development of 3 enterprise-grade endpoint security monitoring products using Agile SDLC practices.
  - Performed security-focussed code reviews of native C++ codebases, identifying and developing POCs for 50+ vulnerabilities, including memory safety issues like buffer overflows and use-after-free issues.
  - Developed macOS application control features, implementing application allowlisting and blocklisting by monitoring process execution events and enforcing policy decisions at the OS level.
  - Designed and implemented detection logic for 100+ OS and service misconfigurations (Windows components, Firewalls, AV, Web and DB servers), aligned with OWASP Top 10 and CWE/SANS Top 25 classes.

Projects & Bug Bounties

- **AI & Agentic Security Research** GenAI | Agentic Systems | Security Automation
  - Evaluated agentic GenAI security tools against human-driven analysis, assessing attack-path reasoning, creativity, and depth of vulnerability discovery.
- **Covert Communication Channels** Data Encoding | Secure Communication | Conference Publication
  - Researched covert data-hiding techniques using cryptic crossword puzzles, designing 3 novel covert communication channels embedded in mass-media and presenting findings at the Annual Symposium on Information Assurance..
- **Linguistic Cryptography** C++ | Encryption Techniques | Algorithm Testing
  - Enhanced the A5/1 keystream randomness by integrating structured linguistic patterns, improving statistical randomness and exceeding baseline performance in 60%+ of NIST statistical tests.
- Disclosed a privilege escalation vulnerability via path hijacking in ManageEngine Vulnerability Manager Plus Agents.
- Disclosed a sensitive information logging issue in ManageEngine's VMP agents that disclosed command execution failures.