# Bharath Suresh

✉ bharathsuresh.formal@gmail.com • 🌐 https://bharaths97.github.io
https://www.linkedin.com/in/bharathsuresh97/

## Education

- **Rochester Institute of Technology, Rochester, NY** **GPA: 3.97/4.0**
  *Master of Science in Cybersecurity* *Aug 2021 - May 2024*
- **SASTRA Deemed University, Thanjavur, India**
  *Bachelor of Technology in Electronics and Communication Engineering* *July 2015 - Aug 2019*

## Skills

- **Programming/Scripting Languages**: C, C++, Python, Java, Objective-C, Powershell, BASH
- **Tools, Technologies, and Platforms**: Nmap, Metasploit, BurpSuite, Wireshark, HTTP, TCP/IP, Git, OpenSSL, Visual Studio, OpenVAS, Cloudsploit, AWS, SIEM, EDR/XDRs, Windows, MacOS and Linux
- **Areas of Interest**: Endpoint Security, Penetration Testing, Cryptography, Security Monitoring and Tooling, Computer Forensics, Incident Response, Scripting, Vulnerability Management, Threat Modelling

## Professional Experience

- **iSECURE LLC** **Rochester, NY**
  **Information Security Engineer - Intern** June 2023 - August 2023
  - Developed MacOS packages and scripts, facilitating the collection of system, network activity, and security data.
  - Compiled technical documents summarizing the security posture and proposing improvements to the native and cloud infrastructures of customers based on industry best practices and frameworks such as NIST SP 800-53.
- **Chegg Inc.** **Santa Clara, CA**
  **Security Engineering Intern** June 2022 - August 2022
  - Implemented Web bugs in Microsoft Office documents by embedding API Hooks, leading to real-time network monitoring capabilities, identification of threats, and effective anomaly detection in network activity.
  - Developed an automated Slack notification system by ingesting the Web bug trigger outputs into Splunk, successfully reducing the time taken for incident response by the security operations team.
  - Performed web application penetration testing on Chegg's Math Solver to validate reported bug bounty exploits.
- **Zoho Corporation - ManageEngine** **Chennai, India**
  **Software Development Engineer (Security)** June 2019 - July 2021
  - Lead Windows native agent developer for multiple enterprise security monitoring tools.
  - Optimized the Windows native code by addressing memory-bound bottlenecks for reading XML data.
  - Initiated the foundation for developing a CIS compliance module, designed for Windows endpoints.
  - Engineered the Windows System Security Configuration Management module for OS Security Hardening.
  - Implemented detection and remediation of 50+ misconfigurations related to SSL/TLS, MS Office, and Windows OS.
  - Developed a module for vulnerability detection and remediation by correlating an endpoint's patching status to the CVE database.
  - Conducted research into the detection methodologies for OWASP top 10 and CWE top 25 vulnerabilities, laying the groundwork for further development in web application penetration testing.

## Research, Projects and CTFs

- Explored avenues for improvements in the security of cryptographic algorithms by integrating them with elements of Sanskrit grammar and literature for my final graduate project.
- Developed a forensic framework for Windows and Linux endpoints using honeytokens, rule-based alerting, and artifact collection to detect anomalous network behavior and reduce Incident Response times
- Presented a research paper on the implementation of Covert Channels in Cryptic Crossword Puzzles at the Annual Symposium on Information Assurance (ASIA)
- Analyzed similarities between Cryptic Crossword puzzle solving techniques and cryptanalysis techniques
- Uncovered a Business Logic Error vulnerability in Venmo arising due to phone-number recycling