**Gaurav C Sonawane**
songoroo77@gmail.com • (706) 461 8840 • linkedin.com/in/gaurav-sonawane-360867205/

## SUMMARY OF QUALIFICATIONS

Cybersecurity professional with 3 years of DevOps experience in cloud security, CI/CD automation, and AWS infrastructure management, combined with hands-on expertise in penetration testing, vulnerability assessment, and security reporting. Proven ability to identify and exploit vulnerabilities across application, network while delivering comprehensive remediation strategies and technical documentation.

## EDUCATION

**University of Georgia, School of Computing** Athens, GA
Master of Science in Cybersecurity & Privacy (GPA – 4) January 2024 – December 2025
**Savitribai Phule Pune University** India
Bachelor of Engineering, Information Technology (GPA – 8.6) August 2017 – May 2021

## TECHNICAL SKILLS

Programming Languages: Python, C, C++, Javascript
Operating Systems: Windows, Linux, Unix, Mac
Cybersecurity Tools: Netcat, Wireshark, Nessus, Ghidra, Burp Suite, Azure Cloud, AWS Cloud, Metasploit
DevopsTools: Jenkins, Kubernetes, Docker, Gitlab, Ansible, Terraform, Packer

## RESEARCH EXPERIENCE

**Offensive Security Research & Red Team Operations on Automotive Systems** Athens, GA (Jun 2024 – Present)

- Emulated adversarial threat actors against EV charging infrastructure by deploying EasyEVSE development platform and Azure IoT Central integration to identify attack surfaces across device-to-cloud communication protocols and charging station security controls.
- Developed custom fuzzer in C/C++ to discover network layer vulnerabilities in ISO15118 automotive charging protocol; leveraged AFL fuzzing techniques to validate protocol robustness and uncover security weaknesses in vehicle-to-infrastructure communications.
- Conducted end-to-end penetration testing of charging station architecture, identifying exploitable vulnerabilities across embedded systems, cloud integration points, and wireless communication channels used in electric vehicle charging operations.
- Designed real-world attack scenarios simulating both external adversaries and insider threats targeting automotive charging infrastructure, documenting exploitation paths and providing remediation guidance to strengthen overall security posture.

**Performing Penetration testing & Security Assessment of IOT devices** Athens, GA (Dec 2024 – Present)

- Conducted penetration testing across 5 core components (ESP32-S3 device, Mosquitto MQTT broker, Device backend system, InfluxDB, Grafana), identifying 11 vulnerabilities (4 high, 4 medium, 2 low, 1 negligible) with Syft/Grype SBOM scans and Nessus reports.
- Performed vulnerability scan using Nessus on backend services, achieving 100% remediation of identified CVEs across IoT server stack.
- Executed web and API testing with Burp Suite and sqlmap; validated authentication hardening against 1M+ automated login attempts with Hydra and documented brute-force resistance.
- Executed MQTT protocol fuzzing with Python across 10K+ payload mutations, achieving 0 crashes and confirming broker stability.
- Conducted firmware security analysis on ESP32 images using GHIDRA, confirming 100% encryption with no hardcoded credentials.
- Automated SBOM generation with Syft and performed CVE analysis across 200+ dependencies using Grype while monitoring IoT traffic with Wireshark to confirm TLS 1.3 enforcement and zero plaintext leaks.
- Delivered a comprehensive Penetration Test Report (30+ pages), fuzzing coverage documentation, and remediation roadmap aligned with HIPAA and FDA cybersecurity guidelines, strengthening system security posture and regulatory compliance readiness.

## RELEVANT EXPERIENCE

**Graduate Trainee (Cuelogic Technologies)** India (February 2021 - August 2021)

- Developed full-stack web applications with frontend and backend modules using Python Flask framework.
- Used Groovy scripts for CI/CD pipeline builds & actively got involved in entire Pipeline setups & Jenkins config.
- Created a continuous delivery process to include support for building of Docker images and publish into a private repository Nexus.
- Analyzed and fixed code errors resulting in 54% less system downtimes.

**Product Engineer (LTIMindtree)** India (August 2021 - July 2023)

- Configured Jenkins jobs, wrote shell scripts, provided administration and support in Jenkins for continuous integration and deployment to speed up software development process by 30%.
- Container management using Docker by writing Docker files and installed and configured Kubernetes.
- Used AWS platform to maintain, configure and support AWS services such as EC2, EKS, S3, Route 53, Active Directory.
- Managed disk space issues using cloudwatch reducing operational costs by 20%.
- Worked with 50+ developers, cloud platform engineers, security engineers, architects and stakeholders across the project

## CAMPUS AND COMMUNITY INVOLVEMENT

- Member of Blackhat Society, Atlanta Chapter
- Competed with University hacking team in PICO CTF, achieving top 9% global ranking and contributing 51% of team score