Virupaksha Repalle

Atlanta, GA 30318 • viru.repalle@gmail.com • (509)-987-3340

EDUCATION

Georgia Institute of Technology — Atlanta, GA
Master of Science in Cybersecurity — *Expected May, 2027*

University of Washington — Seattle, WA
Bachelor of Science in Informatics — *June, 2024*
Software Development and Cybersecurity Specialization

EXPERIENCE

Pacific Northwest National Laboratories — Richland, WA
Cybersecurity Software Engineer — *June, 2023 - Current*

- Built assessment platform features using React, TypeScript, and JavaScript, shipping tools used by critical infrastructure operators to evaluate their cybersecurity posture
- Collaborated with cross-functional teams, writing tests, reviewing code, and communicating technical decisions to non-technical stakeholders across the energy, nuclear, and chemical sectors
- Conducted threat modeling and security assessments across IT and OT environments, identifying risks and recommending mitigations for national critical infrastructure
- Designed and implemented an AWS-native CI/CD pipeline (CodePipeline, CodeBuild, CodeDeploy) for the assessment platform, deploying to S3 and CloudFront with automated dependency vulnerability scanning and secret detection on every commit to prevent leaked credentials and vulnerable packages from reaching production

PROJECT EXPERIENCE

Authentication & Identity: OAuth 2.0 and OpenID Connect

- Implemented full OAuth 2.0 and OIDC authentication flows using Flask and Okta, covering authorization code flow, token validation, and redirect URI handling
- Examined common implementation pitfalls including token leakage, open redirect attacks, authorization code interception, and scoped access enforcement

API & Web Application Security Assessment

- Conducted OWASP Top 10 security assessments against simulated REST APIs and web applications, exploiting SSRF, XSS, CSRF, and SQL injection vulnerabilities
- Analyzed HTTP headers, cookies, session tokens, and authentication flows to identify insecure server configurations and broken access controls
- Produced structured vulnerability findings with remediation-focused reporting, and chained client-side attacks using Browser Exploitation Framework (BeEF)

Log4Shell (CVE-2021-44228) Vulnerability Analysis

- Reproduced remote code execution via malicious JNDI lookup payloads, tracing the exploit chain from user-controlled input through vulnerable logging to remote class loading
- Evaluated mitigation strategies including lookup functionality removal, dependency upgrades, and network restrictions, applying supply chain security principles

PUBLICATIONS

- Repalle, V. (2024). Cybersecurity Capability Maturity Model User Guide (Version 2). Pacific Northwest National Laboratories.
- Repalle, V. (2023). Web Development of Cybersecurity and Resiliency Maturity Models. Pacific Northwest National Laboratories.

SKILLS

Proficient Languages: Python, TypeScript, C, Swift, Bash, SQL
Cybersecurity: OWASP Top 10, Threat Modeling, Secure Code Review, Authentication & Identity (OAuth 2.0, OIDC), XSS, CSRF, SSRF, SQL Injection, Burp Suite, BeEF
Cloud & Infrastructure: AWS S3 + CI/CD, Linux, Git, Docker
Frameworks & Concepts: React, Node.js, Flask, MITRE ATT&CK, NIST CSF, REST APIs