Shivasurya (Shiva)

📧 s5sankar@uwaterloo.ca

📞 +1-226-581-4631

🏢 Waterloo, Ontario, Canada

Web: shivasurya
Github: shivasurya
Linkedin: shivasurya
Hackerone: shivasurya
Google VRP: shivasurya

Software engineer with more than three years of specialized work experience in saas development and application security (appsec). Currently seeking a challenging software engineering role.

Education

University of Waterloo, Canada   **Sept 2019 – Current**

Master's in Computer Science (GPA 3.85/4.0) - Expected Apr 2021

Work Experience

Security Software Engineer, Zoho (zoho.com)   **Apr 2017 – Aug 2019**

SaaS Products with 50+ Million customers including CRM, Mail, Books

- Contributed to Zoho internal security framework to prevent vulnerability & attacks in realtime including mitigation of SQL Injections, cross-site scripting, server request forgery using input validation framework.
- Deployed continuous mobile security static code analysis using HackSaw internal security to mitigate issues in mobile apps and zoho sdk frameworks.
- Handled **Secured Audit** for new features or major edition roll outs by defining threat model & auditing source code
- Found 120+ security issues through **code audit, blackbox and pentesting approach** in ***.zoho.com products**.
- Lead mobile, web security and managed bugbounty program for 70+ Zoho, ManageEngine cloud products.
- Managed security education program for developers to adopt best practices during the development lifecycle through CTF, Internal Hacking Challenge.
- **Tech Stack**: Java, JavaScript, Python, MySQL, PostgreSQL, Docker, Apache Kafka, Android, OSCP Tools, PMD, CodeQL, Lombok AST, OWASP Top 10, Mitre Attack Matrix for Benchmarking

Public Security Contributions

- **CVE-2018-16493 -** Found directory traversal leading to internal file access attack in a npm package
- APKTool Remote Code Execution via Zip Slip - reported to opensource and fixes are here
- Found security issues in Google, Dropbox, Twitter, Zendesk, Microsoft and more via Hackerone platform.

Projects

DEVAA - Automated approach to detect vulnerabilities in Android Apps (Thesis)

An automated approach to prove the application vulnerability with the help of exploitation techniques by assembling payloads, target and verifying them with the help of ADB instrumentation frameworks in Android.

Skills

Programming Languages: Java, NodeJS, Python, SQL, JavaScript, Kotlin, JavaScript

Technologies and Frameworks: Android, Reactjs, Apache Spark, Git, Docker, Kubernetes, Apache Kafka, OSCP Tools, Static Code analysis framework toolset, Lombok AST, CodeQL, OWASP Top 10, Mitre Attack Matrix

Awards

Smart India Hackathon Winner + Internship @ISRO (Indian Space Research   **Apr 2017**
Organization) Govt. of India