Shivasurya Sankarapandian

📧 shiva@shivasurya.me | 📞 +1-(226) 581-4631

🏢 1804-23 Barrel Yards Blvd,
Waterloo, Ontario,
Canada - N2L 0E3

Github: shivasurya
Linkedin: shivasurya
HackerOne: shivasurya
Google VRP: shivasurya
Website: shivasurya.me

Software Engineer with more than five years of specialized work experience in development, shift left and offensive security. Currently seeking a challenging software engineering role focusing on security in SaaS or enterprise products.

Work Experience

Security Engineer, Sourcegraph Inc
Jun 2023 - Current (Contributions are mostly public in GitHub)

- Designed and lead application security initiatives:
  - Revamped secure-by-design security review for engineering projects and initiatives
  - Semgrep SAST scanning (Implementing SOC2 compliant) integrating with GitHub advanced security
  - Secret scanning in Git commits and repositories (Trufflehog open source, GitGuardian)
- Security review for engineering projects such as Cody AI assistant plugins for Intellij Jetbrains, VSCode, Eclipse, Visual Studio IDE
- Pro-active penetration testing on Sourcegraph & Cody AI infrastructure to secure them from vulnerabilities that includes Inference service, Cody Gateway, guardrails
- Building Sherlock (Cody AI assistant) performing AI assisted security code reviews on pull requests helps to keep tabs on new code changes, extra eyes to reduce security blindspot and integrates with SAST scanning.

Software Security Engineer (Application Security), Dropbox Canada LTD
June 2022 - June 2023

- Implemented DAST (Dynamic Analysis) for customer facing APIs and web services within dropbox infrastructure.
- Improved secure development practices with shift-left security theme by giving faster feedback to developers with security tools - integrating Semgrep static analysis and dependency checkers.
- Proactively conducting threat modeling & security audit with established best coding practices in the product features & securing workloads that includes desktop, mobile and web platforms.
- Managing appsec related Bugbounty program by triaging & fixing security issues via Hackerone.

Software Engineer (Application Security), Yelp Inc
Jun 2021 - Jun 2022

- Improved secure development practices with shift-left security theme by giving faster feedback to developers with security tools - static analysis, supply chain attack detection & dependency checkers.
- Reviewed technical & product specifications for security audit and established best coding practices in the product feature.

- Designed and implemented security framework solutions to improve the resilience of Yelp login systems to large-scale attacks with captcha, bot signal, and login signal implementations to prevent account takeover attacks & intrusion detection by heading the Login protection project.
- Managing Bugbounty program by triaging & fixing security issues via Hackerone.

Software Engineer (Application Security), Zoho Corporation (zoho.com)

SaaS Products with 75+ Million customers including CRM, Mail, Books

Dec 2016 - Aug 2019

Zoho Security (Moved to Security Engineering):

- Contributed to Zoho internal security firewall framework to prevent vulnerability & attacks in real-time with reference to owasp top 10 standard.
- Lead Mobile security team and contributed to continuous mobile security static code analysis to mitigate issues in mobile apps and Zoho Android & iOS SDK frameworks.
- Adopted industry-wide AES Encryption practice for Zoho Invoice and Books Payment feature while integrating with payment terminals & banking integrations.
- Reported 80+ vulnerabilities across Zoho, and ManageEngine products, including Multi-factor authentication bypass, Remote code execution.
- Managed Bugbounty program by triaging, fixing security issues & rewarding security researchers with financial bounty.

Education

University of Waterloo, Canada

Computer Science, Master of Mathematics

Sep 2019 - May 2021

Thesis: DEVAA - Automated approach to detect vulnerabilities in Android platform application

Security Contributions

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

Programming Languages:

GoLang, Java, Kotlin, NodeJS, JavaScript

Technologies and Frameworks:

Docker, Kafka, Redis, OSCP Tools, Static Analysis, Tree-Sitter, CodeQL, Semgrep, AWS, GCP, GDB

Open source contribution

Building codepathfinder.dev, open source alternative to CodeQL

Awards

Security - Smart India Hackathon Winner @ISRO (Indian Space Research Organization) Govt. of India - Official Blog **Apr 2017**