Avinash Jain

Infrastructure Security Engineer/Devsecops

Experienced full-stack Information Security Engineer with a demonstrated history of working in various security domain. Skilled in Cloud Security, Application Security, Penetration testing, Vulnerability Management, Container Security.

✉ avinashjain030193@gmail.com 📱 +91-9650754366 in linkedin.com/in/avinashjain619 Ⓜ medium.com/@logicbomb_1

WORK EXPERIENCE

Lead Infrastructure Security Engineer
Grofers

05/2018 – Present

Work

- Led strategic planning and technical implementation of Cloudflare WAF and FortiGate Network Firewall. Responsible for setting it up, hardening and meticulous tuning. At present, defending against 1M malicious web request on daily basis.
- GHSec bot - Developed an app to enforce security and quality of code for every pull request. App performs static code analysis, Dockerfile linter, secrets detection, unauthorised docker image detection along with coverage reports.
- Cloud Security - Led org wide efforts by hardening it as per CIS benchmark using config rules, trusted advisor, guardduty, lamda and inhouse scripts developed in Python. One of them was a s3 DLP tool to alert any unauthorised copy of s3 bucket.
- DNS HA(High Availability) - Automated DNS management using Terraform across AWS Route 53 and Cloudflare DNS. Integrated with Jenkins to manage any change raised in DNS to go through an approval process.
- Secrets Leakage - To reduce credentials leakage risk, integrated Vault with Postgres Database using Ansible to manage database and help developers generate dynamic temporary credentials.
- Created a python tool to find various security misconfigurations in web apps, set up Bug bounty program, Risk control matrix, Incident management program, User audit process, Security policies ,Security awareness program across the company.

Security Engineer - I
Expedia

10/2017 – 04/2018

Work

- Managed application security for multiple domains of Expedia. It includes DAST (using burp suite and web inspect) and SAST (using sonarqube), manual penetration testing, and reporting after reviewing for false positives and other cases.
- Authored and demonstrated proof-of-concept exploits for production web app vulnerabilities identified through static or dynamic analysis, working closely with developers and remediation team to get them fixed.

Senior Information Security Engineer
Makemytrip

01/2015 – 09/2017

Work

- WebGuard - Developed an Automated Vulnerability Scanning Tool - WebGuard to find potential security vulnerabilities by integration during QA cycle itself and provide an interactive interface to begin the scanning and generate report.
- DLP - Implemented and configured Data Leakage Prevention tools across various endpoints covering both data at rest and data at motion to prevent sensitive data leakage.
- VAPT - Carried out 250+ VAPT of web/mobile application with complete ownership of vulnerability assessment tools, responsible for their configuration maintenance, rules and triggers, etc.

SKILLS/TECHNOLOGY

Python   Bash   Terraform   Flask

MySQL/Postgres   VAPT   Cloud Security

Container Security   CI/CD Security

Vault   Ansible   DLP

VOLUNTEERING/TALKS

Hackerone Live Hacking Meetup
Hackerone

Threat Modelling in Container Security and Kickstart in Bug Bounties
null-OWASP Meetup

Hacking Docker, the Shodan Way
SARCON'20

Cloud Security
Secarmy

Security Awareness talks and training at various companies
Multiple

Left Shift Security change
OWASP Seasides

HONOR AWARDS

Bug Bounty - Rewarded and recognised by 50+ companies
Vmware, Mongodb, Zendesk, Gojek, CERN-EU, CERN-US, etc.

Reported Bugs to major companies
Google, NASA, Yahoo, 1password, etc.

Covered in various newspaper and editorials for my work in Infosec
BBC, Forbes, Techcrunch, Economic Times, etc.

EDUCATION

B.E. in Computer Science
Thapar University