Yogendra Swaroop Srivastava

Security Engineer

+91 9980573720

yogendra.swaroop.srivastava@gmail.com

Website: https://www.yogendra-swaroop.blog
Github: https://github.com/yogi1426

ABOUT

- Security professional with over 4.5 years of experience in Product Security, Cloud Security (AWS/GCP), DevSecOps, and Secure SDLC. I specialise in integrating security into CI/CD pipelines using SAST/SCA, creating security automations, and managing WAFs for cloud environments.
- Skilled in penetration testing across mobile, web, and API platforms, I collaborate with stakeholders to resolve VAPT findings efficiently and enhance security posture. I have a passion for knowledge sharing, demonstrated through brown bag sessions and organizing a Capture The Flag (CTF) event for Cyber Security Month.
- Passionate about cybersecurity and its critical role in today's digital world, I remain committed to staying at the forefront of emerging trends and challenges. My goal is to contribute my expertise in securing assets and mitigating risks, thereby bolstering the resilience of organizations against evolving threats.

EXPERIENCE

Senior Security Engineer
Upstox(RKSV Securities Pvt. Ltd) (October 2023 – Present)

- Led VAPT Audit to identify and address security vulnerabilities for Upstox.
- Led the integration of security practices into the CI/CD pipeline, employing SAST/SCA to ensure only secure code is merged into the master branch.
- Implemented automated vulnerability scans for new domains to proactively identify security risks.
- Established security controls in public GitHub repositories for Upstox, preventing accidental exposure of sensitive information.
- Collaborated with stakeholders to address VAPT findings, developing an automated workflow for weekly updates, achieving timely closure of all reported findings a month ahead of schedule.
- Conducted Threat Modeling and security architecture reviews to ensure minimal security issues in feature deployments.
- Configured Cloudflare rules to enhance security posture.
- Delivered multiple brown bag sessions to engage the engineering team in addressing security vulnerabilities.
- Created and executed a Capture The Flag (CTF) event for Cyber Security Month, fostering organizational awareness.
- Identified and reported PII data within service logs, enhancing visibility for the engineering team.
- Automated the approval process via Slack to streamline security reviews, reducing delays for engineering teams.

Security Engineer

Mobile Premier League (MPL) (July 2021 – October 2023)

- Led End to End Product Security for one of the MPL's app.
- Managing AWS WAF and Cloud Armor (GCP WAF).
- Led and Managed Bug Bounty Program for MPL.
- Securing the Cloud Infrastructure (AWS/GCP).
- Worked to Setup Product Security Review process in the organization.
- Internal Red Teaming.

Security Research Engineer

VirSec Systems Pvt Ltd (March 2021-July 2021)
Location: **Bengaluru**

Cyber Security Instructor - Red Team

HackerU (February 2020 – March 2021)

- Trained students for Web Application Security, Python, Linux/Windows Privilege Escalation techniques, Penetration Testing.
- Created custom deliberately vulnerable machines for Pentest labs.
- Content Developer for the Red team textbooks.

Location: **Bengaluru**

.

LICENSES & CERTIFICATIONS

- Certified Network Security Specialist by ICSI(July, 2020)
- Certified by HackerRank for Python and Java(June, 2020)
- Offensive Security Certified Professional (OSCP, September 2019)
- Essential Badge, Android, Unix Badge from PentesterLab.
- CCNA, Redhat, MCSE – 3months training from Zoom Technologies, Hyderabad. (December 2016 – March 2017)

SKILLS

- **Core Competencies**: DevSecOps, Cloud Security (AWS/GCP), Security Automations, Web Application Firewalls (WAFs), Threat Modelling, Secure Code Review.
- **Security Expertise**: Proficient in Web Application Security, Mobile Application Security, Red Teaming, API Security, and industry standards/frameworks.
- **Network Security**: Strong understanding of networking concepts, network domains, communication protocols, and their impact on network and host system security.
- **Operating Systems**: Familiarity with Linux and Windows OS environments.
- **Development Knowledge**: Understanding of Web and Mobile Application Development processes.
- **Vulnerability Awareness**: Strong knowledge of OWASP Top 10 and SANS Top Attacks.
- **Tools & Technologies**: Experienced with Metasploit, Burp Suite, Nmap, Nikto, Sqlmap, Drozer, Frida, Volatility, Netcat, and various CSPM tools.
- **Scripting Languages**: Proficient in Python and Shell Scripting.
- **Programming Languages**: Knowledge of Java, PHP, HTML, CSS, and basic JavaScript.

PROJECTS

- **Shift-left Security**:
  - Set up SAST/SCA tools (Semgrep) and integrated them into the CI/CD pipeline, ensuring all Pull Requests undergo security reviews for code security vulnerabilities and open-source library issues.
  - Implemented pipeline controls to block insecure PRs and developed Slack-based automation for on-the-fly exception handling, minimizing delays.
  - Designed a custom automation solution to monitor public repositories (not managed by pipeline security) for accidental secret leakage using GitHub Workflows and Rulesets.

- **Product Security**
  - Conducted threat modelling for critical features, enabling engineers to focus on secure development and address low-hanging vulnerabilities.
  - Performing Penetration testing on critical features.
  - Fostered a "**Security-First**" culture by integrating security practices into the pre and post-development stages.
- **Cloud Security**
  - Deployed Service Control Policies (SCPs) to enhance the organization's cloud security posture.
  - Designed AWS Lambda functions to mitigate DDoS attacks using AWS WAF and Athena.
  - Developed AWS Lambda to identify IAM users without MFA and enforce MFA compliance.
  - Implemented an open-source CSPM tool with a custom wrapper to reduce false positives and ensure timely detection of critical cloud security issues, addressing the absence of commercial solutions.
- **Bug Bounty Program**
  - Launched an in-house Bug Bounty Program to attract global security researchers with minimal cost, eliminating reliance on commercial platforms.
  - Managed triaging of reported vulnerabilities and prioritized their resolution.
- **Knowledge Sharing**
  - Led brown bag sessions to educate and encourage engineers to address security issues proactively.
  - Organized a **Capture the Flag (CTF)** event for Cyber Security Month, creating **10+ vulnerable applications** with real-world scenarios, including: SQL Injection, LFI, RCE, JWT Attacks, Sensitive Data Exposure, Path Traversal.
  - Educated engineering teams on addressing **Open-Source vulnerabilities** through exploitation **POCs** and **brown bag sessions**.
- **Security Automations**
  - Developed a **File-Inspector tool** to ensure files are only downloaded and used from trusted sources, mitigating risks from malicious files.
  - **Attack Surface Monitoring**: Built an in-house setup to scan org public domains for Critical/High vulnerabilities using tools like Nuclei and DirBuster.
  - **PII Data Detection**: Developed a tool to identify and mask PII data in customer logs, ensuring compliance and data protection.
  - **Security Dashboard**: Created and shared dashboards with stakeholders to track security issues and prioritize VAPT findings.