SHIVAM SARASWAT

Product Security Engineer

@ shivamsaraswat044@gmail.com ☎ +91-9084280701 Bengaluru, Karnataka
shivamsaraswat.com blog.shivamsaraswat.com shivamsaraswat shivamsaraswat

EXPERIENCE

Product Security Engineer

IKEA

April 2023 – Ongoing Bengaluru, Karnataka

- **Architecting Security Solution & Deployment**: Engineered Heimdall, an in-house Automated Web and API Security Monitoring Solution, slashing external engagement costs by 20% through improved responsible disclosure programs. Orchestrated cloud deployment using GitHub Actions, Cloud Run, and Artifact Registry, ensuring seamless functionality.
- **SSDLC Automation & Integration**: Key architect for developing "Argos", an organization-wide proactive automated SSDLC maturity model. This includes one-click enablement via platform engineering, instant on-demand security assessment, security maturity score, actionable insights for better decision-making and automated secure template integration for developers.
- **Collaborative Innovation**: Worked with Engineering teams to pioneer R&D efforts aimed at significantly strengthening IKEA's product security infrastructure, integrating advanced tools into CI/CD pipelines.
- **Pioneering Exploration (PoC)**: Collaborated cross-functionally to prototype and implement scalable solutions, driving a cloud-first architecture.
- **Automated Vulnerability Management**: Streamlined the extraction of critical issues from Google Security Command Center (SCC) with real-time Slack notifications and centralized dashboard visualization, optimizing response time, triaging, follow-ups, and patching.
- **Operationalize Cloud Security**: Pioneered Google Cloud access control policies and best practices. Led cloud vulnerability management, prioritizing fixes, detecting false positives, and reporting to stakeholders. Visualized vulnerabilities on an internal dashboard to deduce trends and make informed decisions for mitigation.
- **Detailed Documentation**: Thoroughly documented Cloud Security findings investigations and research.
- **Shadow IT Asset Management**: Resolved numerous DNS dangling issues associated with shadow IT assets, which were critical in preventing potential subdomain takeovers.
- **Bug Bounty Program Management**: Investigated and resolved multiple issues reported by external Security Researchers on the Bug Bounty program.
- **Comprehensive Security Assessments**: Conducted regular Pentesting, Threat Modeling, and Secure Code Reviews for Internal Products.
- **Security Awareness**: Delivered 10+ engaging sessions with actionable cybersecurity strategies to non-security co-workers.

EDUCATION

B Tech CSE (Specialization in Cyber Security)

GLA University, Mathura

May 2022 8.25 CGPA

SKILLS

Cyber Security: Application Security, Security Automation, Cloud Security, OWASP Top 10, Secure Code Review, Vulnerability Management, Policy as Code, Pentesting (Web, Network), Threat Modelling

SAST/SCA: Semgrep, CodeQL, Dependabot, GHAS

Secret Scanning: Gitleaks, TruffleHog, GHAS, Talisman

DAST: Nuclei, Nuclei Templates

Scripting: Python, Golang, Bash, PowerShell

Cloud Platform: GCP, AWS

CI/CD: GitHub Actions

Containers & Orchestration: Docker, Kubernetes (K8S), Trivy, Hadolint

Database: MongoDB

Version Control: Git, GitHub, BitBucket

OS: Linux, MacOS, Windows

API Tools: Swagger, Postman

Security Tools: Burp Suite, Wireshark, Nmap, Nessus

Monitoring Tools: Elasticsearch (ELK)

ACCOMPLISHMENTS

Best Security Product of the Year 2023

Received recognition at the 2nd Annual Cyber Security Excellence Awards by Quantic India

InnerSource Hackathon Runner Up

Achieved 1st runner up in IKEA's InnerSource Hackathon 2024

Security Automation Engineer

BreachLock

March 2022 - April 2023 Noida, UP

- **Cyber Threat Research & Automation Code**: Researched on the latest cybersecurity threats and devised automation code for Vulnerability Scanners and External Attack Surface Management (EASM) platform.
- **Vulnerability Scanner Enhancement**: Enhanced the effectiveness of the Automated Vulnerability Scanner by meticulously analyzing and incorporating insights from Pentester-discovered vulnerabilities, ensuring continuous improvement.
- **Modular Security Automation Code**: Developed modular and efficient code for security automation plugins, optimizing functionality and scalability while ensuring comprehensive documentation.
- **Scrum-based Collaboration**: Engaged in a scrum-based environment, leveraging tools like Jira, Bitbucket, and Confluence to foster efficient collaboration and streamline project management processes.
- **Test Case Development**: Created comprehensive test cases using Pytest, ensuring robust and reliable performance of the Scanner.
- **Microservice API Development**: Designed and implemented Backend Microservice APIs using Swagger, Postman, Flask, and MongoDB, contributing to the creation of a resilient and responsive ecosystem for security tools.

PROJECTS

PYrevDNS
A tool for performing reverse DNS lookups on IP addresses

Certify - SSL/TLS Certificate Security Analysis Too
A powerful and easy-to-use tool designed to check the security of SSL/TLS certificates

crt.sh Domain Finder
A tool to find all the domains and the subdomains associated with a domain using crt.sh

Refinements In Zeek Intrusion Detection System
Designed and implemented custom scripts for improving the logging capability of the Zeek IDS

SSH Bruteforcer and Bruteforce Detector
A tool for brute-forcing the SSH service, allowing for testing and analysis of SSH security measures, and a tool for detecting brute-force attacks on the SSH service

PGrab
A tool for gathering information about a remote server or device, specifically the banner or header information that is sent when a connection is made

Speaker at Disobey 2024 Conference
Selected to present on – "Guarding Your Digital Realm: Heimdall – Your Shield in the World of Web and API Security" at the largest Nordic Security Event in Helsinki, Finland

Top 1% (God Rank) on TryHackMe
Completed 120+ rooms on topics like DevSecOps, Pentesting, CTFs, OWASP Top 10, Nmap, Wireshark, Nessus, etc.

PUBLICATIONS

Conference Proceedings

- A. Tiwari, S. Saraswat, U. Dixit, and S. Pandey, “Refinements in zeek intrusion detection system,” in *2022 8th International Conference on Advanced Computing and Communication Systems (ICACCS)*, vol. 1, 2022, pp. 974–979. DOI: 10.1109/ICACCS54159.2022.9785047.

CERTIFICATIONS

- **EC-Council -** Certified Ethical Hacker (Practical)
- **IBM -** Cyber Security Graduate
- **Internshala -** Ethical Hacking
- **PentesterLab -** Unix Badge
- **Fortinet -** NSE 1 Network Security Associate

LANGUAGES

English	●●●●●
Hindi	●●●●●