SHIVAM SARASWAT

+91-9084280701 ◇ Bengaluru, Karnataka

shivamsaraswat044@gmail.com ◇ linkedin.com/in/shivamsaraswat ◇ github.com/shivamsaraswat ◇ Portfolio ◇ Blog

OBJECTIVE

Experienced Cyber Engineer with a focus on Product Security, contributing two years of expertise in implementing cutting-edge cybersecurity solutions. Seeking a dynamic role as a Product Security Engineer to leverage my skills in securing and fortifying digital products against emerging threats. Having a Bachelor's Degree focused in Computer Science and Engineering with a Specialization in Cyber Security.

EXPERIENCE

Junior Cyber Engineer April 2023 - Present
IKEA

- Engineered and implemented Heimdall, an in-house Automated Web and API Security Monitoring Solution, encompassing Subdomain and API enumeration, vulnerability scanning, real-time Slack notifications, and data aggregation in Elasticsearch & MongoDB. This initiative also realized a 20% reduction in external engagement costs through its significant impact on our responsible disclosure programs.
- Deployed Heimdall in GCP Cloud Run using Docker Containerization, GitHub Actions and Artifact Registry.
- Implemented scorecard technique for DevSecOps instant assessment, providing on-demand valuable insights into the team's security posture. Established a centralized dashboard for the entire organization, enhancing visibility and trends into the overall DevSecOps state. This resulted in improved strategic decision-making, efficient policy management and heightened security awareness.
- Collaborated closely with Engineering teams (Chief Architects, Developers, and Senior Professionals) to pioneer R&D efforts to strengthen IKEA's product security infrastructure, integrating advanced tools into CI/CD pipelines. Collaborated cross-functionally to prototype and implement scalable solutions, driving a cloud-first architecture. Communicated security risks effectively and contributed to defining baseline security standards for products deployed across GCP and on-premise servers.
- Automated the extraction of critical issues from Google Security Command Centre (SCC) findings, enabling real-time notifications via Slack and visualization on the Looker Studio dashboard using BigQuery and Cloud Storage. This automation significantly optimized our response time to potential security threats in cloud projects, ensuring swift and effective risk management.
- Investigated and resolved multiple issues reported by external Security Researchers on the Bug Bounty program.
- Conducted regular penetration testing, threat modelling, and secure code review of internal products.
- Led the initiative in creating Access Control policies for Google Cloud Projects, resolved DNS Dangling issues, and formulated Best Practices policies, fostering a more secure environment for product teams.
- Led comprehensive security awareness initiatives, delivering over 10 engaging sessions to non-security co-workers, equipping them with practical insights and actionable strategies for enhancing cybersecurity within the organization.

Associate Security Automation Engineer March 2022 - April 2023
BreachLock

- Spearheaded research on the latest cybersecurity threats and devised automation code for Vulnerability Scanners and External Attack Surface Management (EASM) platform.
- Enhanced the effectiveness of the Automated Vulnerability Scanner by meticulously analyzing and incorporating insights from Pentester-discovered vulnerabilities, ensuring continuous improvement.
- Developed modular and efficient code for security automation plugins, optimizing functionality and scalability while ensuring comprehensive documentation.
- Engaged in a scrum-based environment, leveraging tools like Jira, Bitbucket, and Confluence to foster efficient collaboration and streamline project management processes.

- Created comprehensive test cases using Pytest, ensuring robust and reliable performance of the Scanner.
- 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. (Project Link)

- PYrevDNS is a simple tool for performing reverse DNS lookups on IP addresses.
- It can be used to perform lookup on a single IP address or on a list of IP addresses.
- It can also be used as Python module or run in a docker container.

Certify - SSL/TLS Certificate Security Analysis Tool. (Project Link)

- Certify is a powerful and easy-to-use tool designed to check the security of SSL/TLS certificates.
- It has comprehensive certificate analysis, covering subject alternative names, common names, organization details, and more.
- It identifies common misconfigurations like expired, self-signed, mismatched, revoked, and untrusted certificates.

PGrab. (Project Link)

- It is a banner grabber tool used to gather information about a remote server or device, specifically the banner or header information that is sent when a connection is made.
- It has options to give the hostname/IP, port, path and output file name as CLI input.

crt.sh Domain Finder. (Project Link)

- It can retrieve all the domains and the subdomains associated with a domain using crt.sh.
- It has options to give the domain name and output file name as CLI input.
- It can be used in conjunction with other tools to know the active domains.

Refinements In Zeek Intrusion Detection System. (Project Link)

- Designed and implemented custom scripts for improving the logging capability of the Zeek IDS.
- Utilized Bro (Zeek) Scripting language for making scripts.

SSH Bruteforcer and Bruteforce Detector. (Project Link)

- It has a tool for brute-forcing the SSH service, allowing for testing and analysis of SSH security measures.
- It also has a tool for detecting brute-force attacks on the SSH service.

ACCOMPLISHMENTS

- Published paper in the IEEE Conference on the topic – Refinements in Zeek Intrusion Detection System. (Paper Link)
- Accepted 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. (Link)
- Got the award of Best Security Product of the Year – Heimdall (Retail) in the 2nd Annual Cyber Security Excellence Awards 2023 for making Heimdall. (Link)
- Ranked in the top 1% (God Rank) on the industry-leading hacking platform TryHackMe. Complete 120+ rooms on topics like Web and Network Fundamentals, DevSecOps, Penetration Testing, OWASP Top 10, CTFs, Nmap, Wireshark, Metasploit, Nessus, OSINT, etc. (Profile Link)
- Ranked under 850 on the industry-leading pentesting platform Hack The Box. Solved 20+ machines and challenges related to Linux Pentesting using tools like Nmap, Wireshark, Metasploit, etc. (Profile Link)
- Ranked 103 out of 2513 participants in VirSecCon CTF and 131 out of nearly 1000 participants in DeepCTF.

SKILLS

Cyber Security Skills	Application Security, Product Security, Security Automation, Cloud Security, OWASP Top 10, Vulnerability Scanning, SAST, DAST, Automated Vulnerability Management, Policy-as-Code, Secure Code Review, Threat Modelling, Web Application Pentesting, Network Pentesting
Programming Languages	Proficient in Python, with intermediate knowledge in Shell Scripting with Bash and PowerShell, along with exposure to C
Cloud Platform	Google Cloud Platform (GCP)
CI/CD	GitHub Actions
Container	Docker
Database	MongoDB
SCM	Git, GitHub
SAST/SCA	CodeQL, Dependabot
Operating Systems	Ubuntu, Kali Linux, Windows
Tools	Burp Suite, Nmap, Wireshark, Nuclei, Git, Postman, Nessus, VS Code
Soft Skills	Team Work, Problem Thinking, Critical Thinking, Fast Learning, Active Listening

EDUCATION

B Tech CSE (Specialization in Cyber Security and Forensics), GLA University, Mathura 2018 - 2022
8.25 CPI
Relevant Coursework: Application Security, Physical Security, Network Security, Ethical Hacking and Penetration Testing, Python, Computer Networks, and Operating Systems.

Intermediate, Ingraham Institute Senior Secondary English School, Aligarh 2018
86%

High School, Ingraham Institute Senior Secondary English School, Aligarh 2016
9.6 CGPA

CERTIFICATIONS

- **EC-Council -** Certified Ethical Hacker (Practical) - ECC4270936185. (Certificate Link)
- **IBM -** Cyber Security & Forensics Graduate. (Certificate Link)
- **Internshala -** Ethical Hacking. (Certificate Link)
- **Fortinet -** NSE 1 Network Security Associate. (Certificate Link)
- **PentesterLab -** Unix Badge. (Certificate Link)
- **University of Michigan -** Programming for Everybody (Getting Started with Python). (Certificate Link)

EXTRA-CURRICULAR ACTIVITIES

- Dedicated volunteer for DEF CON Delhi Group | DC9111 for the past four years, playing a key role in organizing prominent Cyber Security Conference. Demonstrated expertise by creating Capture The Flag (CTF) challenges focused on OSINT, Steganography, and Python.
- Actively write blog posts related to Cyber Security.