Achintya Singh Baghela

Security Analyst

Pune, MH   achintya_singh@outlook.com   +91 7405148140   achintyabaghela   achintya-esbee

Portfolio

About Me

Security-focused professional who thrives on hunting down vulnerabilities and understanding how attackers think. With CompTIA Security+ certification and hands-on experience testing APIs at HP, I've identified critical security flaws including HTML injection and broken access controls. I enjoy building security solutions—from Splunk dashboards that catch network anomalies to database clusters that stay resilient under pressure. Always learning through CTF challenges and eager to bring my problem-solving mindset to a dynamic cybersecurity team.

Certifications

CompTIA Security+ (SY0-701) Mar 2025

Credential ID: K7Z09GNSS2EQ1M5W

Technical Skills

Cybersecurity Tools: Burp Suite, Nessus, LimaCharlie, Tines, Splunk, Metasploit, Kali Linux

Linux Proficiency: Shell scripting, User/Permission Management, Network Configuration

Networking: TCP/IP, DNS, DHCP, Firewall Configuration (iptables, ufw), VPN (IPsec, OpenVPN)

Threat Intelligence: MITRE ATT&CK Framework, IOC Analysis, Threat Hunting, OSINT Collection, Threat Landscape Assessment

Experience

Software Security Tester Pune, MH
HP Inc. Jul 2023 – Apr 2024

- Conducted **25+ API security tests** per sprint, following OWASP guidelines, identifying and **mitigating 15+ critical vulnerabilities** per cycle including **HTML injection, Server Information Disclosure, and Broken Access Control**, **strengthening API security posture by 25%**. Compiled findings in Vulnerability Assessment Reports.
- Participated in DLP incident investigations by analyzing flagged email attachments and data transfer logs, contributing to policy violation assessments and remediation recommendations.
- Helped analyze API responses and log data for indicators of unintended data disclosure in compliance-sensitive environments.
- Delivered monthly presentations on high-severity vulnerabilities (HTML injection, Server Information Disclosure, Broken Access Control) with virtual lab demos and mitigation strategies to 50+ colleagues, from developers to senior managers.

Software Security Intern Pune, MH
HP Inc. Jan 2023 – Jun 2023

- Worked on API Interception and Vulnerability Testing using Burp Suite and Virtual Machines.
- Collaborated with 7 interns on backend development using Spring Boot. Performed Threat Modeling, identifying **10+ risk factors** and proposing mitigation techniques that **enhanced platform security by 40%**.
- Gained hands-on experience with Spring Boot security configurations, implementing input validation, authentication mechanisms, and secure API endpoint design during backend development collaboration.

Projects

EDR-SOAR Integration with Automated Incident Response

- Integrated LimaCharlie EDR with Tines SOAR platform for automated threat detection and response workflows.
- Created custom D&R rules to detect credential dumping (LaZagne.exe) and trigger automated security playbooks.
- Built Tines playbooks for Slack/email alerts with interactive prompts for endpoint isolation decisions.
- Tools: LimaCharlie EDR, Tines SOAR, Windows VM, LaZagne.exe

Splunk Firewall Traffic Analysis Dashboard

- Designed and implemented Splunk dashboard for real-time firewall log analysis and traffic monitoring.
- Created custom searches and alerts for anomalous network behavior detection and threat identification.
- Tools: Splunk Enterprise, pfSense/iptables logs, SPL (Search Processing Language)

Highly Available Database Cluster

- Deployed a 3-node MariaDB and Galera-4 cluster on Debian, ensuring redundancy and high availability.
- Tools: Python (Django), MariaDB, Galera-4, VirtualBox

GitHub-Asana Integration

- Developed a solution to synchronize GitHub issues with Asana tasks for real-time updates.
- Tools: Python (Django), GitHub API, Asana API
- GitHub Repository ↗

CTF Challenges and Labs - TryHackMe & HackTheBox

- Completed over 50 challenges on network enumeration, web exploitation, and privilege escalation.
- Tools: Nmap, Dirbuster, Burp Suite, Metasploit, Kali Linux

Education

Symbiosis Institute of Technology Jul 2019 – Jun 2023
BTech in Information Technology (Honors in Security and Privacy)