

Achintya Singh Baghela

📍 Pune, MH ✉ achintya_singh@outlook.com 📞 +91 7405148140 in [achintyabaghela](#) 🌐 [Portfolio](#)

About Me

- CompTIA Security+ certified with hands-on experience identifying critical vulnerabilities including HTML injection and broken access controls through API testing at HP
- Active CTF participant with proven ability to translate complex security concepts into practical solutions for dynamic environments
- Interested in Cybersecurity, Penetration Testing, Blue Teaming and OSINT

Certifications and Education

CompTIA Security+ (SY0-701) — Verify 	Mar 2025
Symbiosis Institute of Technology <i>BTech in Information Technology (Honors in Security and Privacy)</i>	Jul 2019 – Jun 2023

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 — HP Inc. Pune, Jan 2023 – Jun 2023

- Conducted **25+ API security tests** per sprint, identifying and **mitigating 15+ critical vulnerabilities** including **HTML injection, Server Information Disclosure, and Broken Access Control, strengthening API security posture by 25%**
- Participated in DLP incident investigations by analyzing flagged email attachments and data transfer logs, contributing to policy violation assessments and remediation recommendations
- Delivered monthly presentations on high-severity vulnerabilities with virtual lab demos and mitigation strategies to 50+ colleagues, from developers to senior managers

Software Security Intern — HP Inc. Pune, 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

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

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

Highly Available Database Cluster & GitHub-Asana Integration

- Deployed 3-node MariaDB and Galera-4 cluster on Debian ensuring high availability
- Developed GitHub-Asana synchronization solution for real-time issue tracking — [GitHub Repository](#) 

CTF Challenges - TryHackMe & HackTheBox

- Completed 50+ challenges on network enumeration, web exploitation, and privilege escalation using Nmap, Burp Suite, Metasploit, Kali Linux