Sagar Palhade

Adarsh Nagar, Shegaon - 444203 | sagarrajendrapalhade@gmail.com | +91 9730607490

linkedin.com/in/sagarpalhade2442 | github.com/Saggy2442

Summary

CSE engineering student with expertise in Linux/Unix systems and Python programming. Strong analytical and logical skills demonstrated through SIEM incident detection, forensic analysis, and vulnerability assessment. Proven incident management and communication abilities through hands-on security projects and professional internships.

Skills

- Linux/Unix Systems : Kali Linux, Ubuntu, Linux administration, system log analysis, process monitoring
- Cyber Security : Wireshark, Nmap, Burp Suite, Frida, Jadx, Autopsy, Nessus, Metasploit, Hydra, Splunk SIEM
- Python & Programming : Security tool development, scripting, automation, malware analysis, Java
- Incident Management : Log analysis and correlation, threat detection, forensic analysis, incident investigation, alert handling
- Analytical Skills : Vulnerability assessment, threat analysis, root cause analysis, logical reasoning, data correlation
- Web Development : Node.js, React.js, MongoDB, Express.js
- Networking : Network analysis, packet capture, protocol analysis

Education

Shri Sant Gajanan Maharaj College Of Engineering, BE in Computer Science and Engineering

- CGPA: 7.84/10 | 2022 – Present

Experience

- **Cyber Security Intern - Threat Prism (Jul 2025 – Sept 2025)**: Conducted Android app penetration testing on Linux environment using Burp Suite, Frida, and Jadx to identify OWASP vulnerabilities. Performed digital forensic analysis with Autopsy to recover deleted files and document user activity for incident investigation.
- **Web Development Intern - ApexaiQ (Aug 2025 – Sept 2025)**: Built and deployed full-stack web applications using Node.js, Express, MongoDB, and JavaScript in professional Linux-based environment.
- **Central Railway Engineers Association Portal (Aug 2025 – Jan 2026)**: Developed secure MERN stack web portal with JWT and OTP-based authentication for membership and event management.

Projects

- **Home Lab: Attack Simulation & SIEM Incident Detection Project**: Simulated cyber kill chain with brute-force (Hydra) and RCE attacks on Metasploitable 2. Configured Splunk SIEM to ingest logs, detect authentication failures, and verify post-exploitation activities using custom SPL queries. Demonstrated incident detection and incident management capabilities.
- **Android App Penetration Testing**: Identified security weaknesses in Android banking app using Burp Suite and Frida, demonstrating analytical skills and logical vulnerability assessment.
- **Digital Forensic Analysis with Autopsy**: Performed forensic analysis on disk images using Autopsy to recover deleted files, extract browser history, and identify user activity for incident investigation on Linux systems.
- **Phishing Link Scanner (Python)**: Developed Python tool using domain extraction and Levenshtein distance analysis to detect phishing URLs, demonstrating Python proficiency and logical problem-solving.

Courses & Certifications

1. SAP Training (Ongoing)
2. Threat Prism - Cybersecurity Project Completion
3. IBM + Coursera - Introduction to Cybersecurity Tools & Cyber Attacks
4. NPTEL - Programming In Java
5. Udemy - Full Stack Web Development

Extra Curricular Activities

Pursuit 2024: In addition to supporting the technical team, I was also a part of other teams, including decoration, advertising, and event

ISTE Student Chapter: I served as the Technical Head, leading the team in successfully organizing and executing various technical events throughout the year.