# PRATEEK

7027028229 | 25167prateek.2020ece@gmail.com| LINKEDIN | GITHUB

## PROFILE(SOFTWARE ENGINEER)

Versatile and results-driven Software Engineer with 1.5 years of experience in full-stack development,secure coding, VAPT, and SIEM-based threat detection. I specialize in building scalable web systems using Python, Javascript, Django, MERN, and AI/ML, ensuring they are functional, secure, and resilient.
Hands-on with VAPT (Web, Cloud, Network, Serverless) and live log monitoring via self-deployed ELK Stack, Wazuh, and Security Onion. I bring the rare ability to build, secure, and monitor real-world software from development to defense.

## WORK EXPERIENCE

**Software Engineer (CCFIS Pvt. Ltd. / Amity University, Noida)** **May 2024 - Present**

### 🔐 Secure Coding & Development Projects

- **Keylogger** *(Python)* – Built an encrypted keylogger as a red-team simulation tool featuring stealth execution and secure log handling.
- **AI Person Detection System** (*Django, AI/ML, OpenCV, MySQL*) – Developed a real-time face recognition platform with integrated user detection and secure login access.
- **Smart Registration System** (*Django, AI/ML, OpenVision, SQLite*) – Built an AI-driven onboarding system with face & signature validation to prevent spoofing/duplication.
- **MERN Full-Stack Website** (*MongoDB, Express.js, React.js, Node.js*) – Built a production-grade site with JWT-based auth, RBAC, secure APIs, and full frontend/backend CRUD logic.
- **RhythmiX Music Platform** (*HTML5, CSS3, JavaScript*) – Designed a responsive streaming web app with secure playback and user-friendly UI.
- **Other Projects** – PyBankPro, PyCoinForge, VoiceGenius, VowelBlendQuest, CuriousBaby Quiz, TurboDash, Email Slicer, FPV Drone, Tic-Tac-Toe, ConvoGenius and much more **GITHUB**

### 🛡️ Vulnerability Assessment & Penetration Testing (VAPT)

- Performed **Web VAPT** using Burp Suite, OWASP ZAP, Acunetix—identified vulnerabilities like SQLi, XSS, CSRF, IDOR, and broken auth.
- Executed **Cloud VAPT** on AWS (IAM, S3, Lambda, CloudTrail) using ScoutSuite & Prowler—uncovered misconfigs, exposed services, and excessive roles.
- Conducted **Network VAPT** using Nmap, OpenVas, Wireshark—discovered open ports, insecure protocols, and lateral movement risks.
- Did **Serverless Penetration Testing** (Lambda/API Gateway) for vulnerable triggers, privilege misassignments, and unvalidated inputs.
- Created detailed reports with risk scores, exploitation steps, and tailored remediation strategies.

### 📊 SIEM & Log Monitoring

- **ELK Stack (Full Deployment)** – Deployed Elasticsearch, Logstash, Kibana from scratch for centralized log management and security dashboards.
- **Wazuh** – Configured and used for HIDS and log analysis—detected abnormal logins, escalations, and unauthorized activities.
- **Security Onion** – Used to inspect packets, detect anomalies, & generate actionable alerts from behavioral patterns. Investigated Indicators of Compromise(IoCs), supported post-breach analysis, & enforced mitigation workflows.

## SKILLS & TECHNICAL PROFICIENCIES

- **Languages & Tools:** Python, JavaScript (ES6+), Java, Bash, HTML5, CSS3, Bootstrap, Git, GitHub, Postman, VS Code, Pycharm
- **Frameworks & Libraries:** Django, React.js, Node.js, Express.js, MongoDB, MySQL, SQLite, AWS (IAM, EC2, Lambda, S3, CloudTrail)
- **Secure Development & Web Security:** OWASP Top 10, OWASP ASVS, JWT, OAuth2, HTTPS, CSRF, XSS, SQL Injection, Input Validation, RBAC, Secure SDLC, AES/RSA, Session Management.
- **VAPT & Penetration Testing:** Burp Suite, OWASP ZAP, Nmap, Nessus, OpenVAS, Shodan, Gobuster, DirBuster, Nikto, ScoutSuite, Prowler, Metasploit, Kali Linux.
- **SIEM & Threat Monitoring:** ELK Stack (Deployed), Wazuh, Security Onion, Suricata, QRadar, Splunk, Wireshark, tcpdump, Netcat
- **Cloud & Network Security:** Serverless Security, IAM Hardening, Firewall Rule Review, Cisco ASA, Fortinet,

pfSense, OPNsense, OpenVPN, SSL/TLS, IPSec, Active DIrectory

- **VMs and Machines :** VMware workstation pro, Virtual box, Hyper-v, Ubuntu, Kali Purple, Kali Linux, Windows
- **Strengths:** Secure Development • Full-Stack Engineering • VAPT • Log-Based Threat Detection • Code Ownership

## PROFESSIONAL SKILLS

- **Secure Development Mindset** – Embed security into code, not after it
- **Root-Cause & Threat Analysis** – Debug deep; trace vulnerabilities to the source
- **Log-Based Problem Solving** – Read logs like stories; detect issues before they escalate
- **Agile & Cross-Functional Collaboration** – Deliver fast with clarity in team-driven environments
- **Clear Technical Communication** – Explain security risks and code logic to devs, managers, and clients
- **Time & Priority Management** – Meet delivery timelines without compromising security
- **Ownership & Accountability** – Take complete charge from build to protection
- **Clean Code & Documentation Practices** – Deliver maintainable, well-commented, and scalable code

## EDUCATION

**B.Tech (Electronics and Communication Engineering)** **June 2020 - June 2024**

- UIET-MAHARSHI DAYANAND UNIVERSITY

**XIIClass (PCMB)** **April 2018 - April 2019**

- VIJAYA SR. SEC. SCHOOL