

# ROHITH GUJJURU

 9381376875

 rohithg987@gmail.com

 [Linkedin](#)

## EDUCATION

B.TECH

**AITAM (Aditya Institute of Technology and management)**

**IT (Information Technology)**

**CGPA 7.59**

**2020 – 2024**

**INTERMEDIATE**

**Sri Chaitanya jr college Palasa**

**MPC**

**CGPA 8.25**

**2018 – 2020**

**SSC**

**Sri Chaitanya Techno School**

**CGPA 9.7**

**2017 – 2018**

## TECHNICAL SKILLS

### **Security Monitoring & SOC:**

- SIEM basics (Splunk, Elastic Stack)
- IDS/IPS, Firewalls, Endpoint Protection
- Log Analysis, Security Event Monitoring

### **Vulnerability Assessment & Penetration Testing:**

- Ethical Hacking & VAPT
- Web Application Security, OWASP Top 10
- Kali Linux, Burp Suite, NMAP

### **Networking & Systems:**

- CCNA-level Networking Protocols
- Windows & Linux Operating Systems
- Wireshark

### **Scripting & Automation:**

- Python, Bash (basic scripting for automation)

### **Other Skills:**

- Threat Detection & Incident Response (intro level)
- Basic knowledge of security policies & ISO 27001
- Strong analytical thinking, attention to detail and Eager to learn.

## LANGUAGE

- English, Telugu

## PROFESSIONAL SUMMARY

Cybersecurity enthusiast with hands-on experience in VAPT, web application security, and SOC operations. Skilled in OSINT, threat detection, and penetration testing using tools like Kali Linux, Burp Suite, and Splunk. Certified in cybersecurity, penetration testing, and threat analysis, with a strong focus on identifying and mitigating vulnerabilities.

## WORK EXPERIENCE

**JUN 2023 – JUL 2023**

### **VAPT INTERN – SUPRAJA TECHNOLOGIES**

#### **ROLE : Web application Vulnerability Assessment and Penetration Tester**

- Conducted comprehensive vulnerability assessments on web applications using **OSINT**, identifying SQL Injection, XSS, and LFI vulnerabilities, **OWASP top 10**.
- Performed manual **penetration testing** and security auditing, ensuring applications complied with security standards.
- Assisted in documenting findings and remediation recommendations for development teams.
- Utilized security tools and frameworks (**Burp Suite, ffuf, SQLMap**) to **analyze, exploit, and report vulnerabilities efficiently**.

## CERTIFICATIONS

- **GOOGLE CYBER SECURITY PROFESSIONAL** (COURSERA 2025)
- **CYBER SECURITY ANALYST** (FORAGE 2024)
- **PENETRATION TESTING WITH KALI LINUX** (UDEMY 2022)
- **INTRODUCTION TO THREAT LANDSCAPE 3.0** (FORTNITE 2025)
- **OSINT COURSE** (MY OSINT 2025)

## PROJECTS

### **1. Web Application Vulnerability Scanner & OSINT Recon Tool (Python)**

- Developed a **Python-based** automated tool for **OSINT gathering** and **vulnerability scanning of web applications**.
- Detected common vulnerabilities including **SQL Injection and XSS using Amass and custom scripts**.
- Generated detailed reports summarizing findings for remediation prioritization.
- **Skills: OSINT Gathering, Web Application Vulnerability Scanning, Security Reporting, Python Programming**.

### **2. SOC Threat Detection Lab using Splunk & Simulated Attack Data**

- Configured a **Splunk SIEM** environment to analyze **simulated attack logs (Brute Force, Malware, Suspicious Activity)**.
- Detected, investigated, and documented **incidents** with correlation rules and incident tickets
- Mapped attack activity to **MITRE ATT&CK framework** to strengthen **SOC detection and response capabilities**.
- **Skills: SIEM Configuration, Log Analysis, Incident Triage, Threat Hunting, MITRE ATT&CK Mapping**

### **3. Log Analyzer with Real-Time Threat Detection**

- Developed a **Python tool** to parse **system logs** and detect anomalies in real time.
- Generated automated alerts to support **SOC monitoring** and incident response.
- Assisted in internal security awareness initiatives by demonstrating findings and alert handling to peers.
- Maintained dashboards for **tracking security events** and **documenting mitigation steps**.