# RESUME

**MADAPATHI SAINATH**
**Phone:** +91 9100185766
**Email :** sainath16414@gmail.com

## OBJECTIVE

To be a part of innovative team, with a challenging job profile that provides sample opportunity to contribute towards business goals and enables continuous learning.

## PROFESSIONAL SUMMARY

- Experience in Web Application Security Testing, Vulnerability Assessment Penetration Testing (VAPT), Network Penetration testing and generating reports using tools.
- Proficient in Linux operating system configuration and utilities.
- Performed Application Penetration Testing for various web applications and also Network Penetration Testing for various Networks.
- Hands on Practice for web application penetration tests such as Burp Suite, Partos, Acunetix Wire shark, Nmap, Nessus.
- Proficient in understanding application-level vulnerabilities like XSS, SQL Injection, authentication bypass, weak cryptography, Session Management, etc.
- Good understanding of OSI layers and fundamental Operating system concepts, security settings of Windows and Linux platforms.
- Skilled in executing OWASP top 10 test cases.
- Ability to work in large and small teams as well as independently.
- Reporting the identified issues in the industry standard framework.
- Excellent communication skills and abilities in resolving complex networking, hardware & software related issues.
- A Self-starter with a positive attitude, willingness to learn new concepts and accept challenges.
- Ability to build form good relationships with clients/operational managers and colleagues.
- Ongoing skill set development: Cyber security news, tools, vulns, exploits, remediation, blogs, courses. Always on the hunt for custom tools, and different methodology.

## PROFESSIONAL EXPERIENCE

### Job-Role: Security Analyst Trainee
### Duration: from January, 2022 to June, 2022
### Company: SecuArk InfoSec

- Performed Internal and external penetration testing (plan, discover, attack, report).
- Performed Web application testing and Network Penetration Testing.

(Manually and with tools such as Nmap, Burp Suite, Nessus, Wireshark, Metasploit).

- Identified threats, and developed test cases to target identified threats.
- Identified and exploited vulnerabilities of Network under test area.
- Carried out remote testing of a client's network and remote testing of their infrastructure to expose weakness in security.
- Also performed port scan of servers using NMAP and closed all unnecessary ports to reduce the attack surface.
- Performed penetration test on the company website and performed various attack on company website.
- Performed OWASP top 10 vulnerability cases.
- Conducted Vulnerability Assessment with Nessus; remediated vulnerabilities.
- Conducted vulnerability assessment and reviewing results.
- Created reports and recommendations from our findings and the level of risk.
- Presented our findings, risk and conclusions to management and other relevant parties.
- Created a report based upon penetration testing and presented it to the customer.

**Job-Role: Associate Security Analyst**
**Duration: July 2022 to August 2022**
**Company: Rooman Technologies**

## PROJECTS OUTLINE

**Project Category: E-Commerce Portal —Spectra**
**Tools Used:** Burp Suite, SQL map, OWASP, Nmap, Nessus, CSRF Tester, GitHub Scripts, etc
**Description:**
Spectra distant shopping e-commerce web application. It includes payment gateways, customer info, login pages, APIs, product info, and complex data.
**Project Responsibilities:**

- Check for regular security updates from standard bodies such as the Open Web Application Security Project (OWASP).
- Application Security Analysis (manual & automated) experience of web applications. Provide effort estimates for conducting security assessments.

- Experience in remediation review and recommendations to vulnerabilities identified during Security Assessments.

**Project Category: Health Care Application – Octra**
**Tools Used:** Burp Suite, OSINT Framework tools, SpiderFoot, Maltego, GitHub Scripts, Dig, Kali Linux, etc

**Description:**
Octra is an Indian multinational pharmaceutical company located in Hyderabad. They had vast data centers across the globe and enormous customers/clients.
**Project Responsibilities:**

- Practiced writing reports and information papers to support OSINT collection desired.
- Research, create, and maintain information repositories that uphold organizational and legal standards and allow for easy data migration.
- Distinguishing the critical high and medium low threats in the data collected based on the OSINT framework and prioritizing them based on the criticality to the report.

**Role: Representative | Operations**
**Concentrix Daksh Services India Pvt. Ltd. | 2022 – 2025**
**Responsibilities:**

- Worked in Continuously monitoring, detection and escalation environment.
- Applied analysis, monitoring, and escalation methodologies at initial triage.
- Escalated rare or complex violations to Tier-2 analysts for further investigation with documentation.
- Identifying recurring trends or patterns in content violations.
- Maintained accurate records of violations, tags applied and Escalations.
- Ensured actions were compliant with platform policies and guidelines.
- Promoted to Sr. Representative, Operations within one year for consistent performance and quality excellence.

## SKILLS

- Linux
- Burp Suite
- Nmap and Zenmap GUI
- Metasploit
- Aircrack-ng suite
- Maltego
- Wireshark
- OWASP
- Bwapp

---

## EDUCATIONAL BACKGROUND

Vivekananda Degree College (affiliated with Osmania University) [2018-2021]
**BSc [Computer Science] - 86%**
Hyderabad

---

I hereby declare that the above written particulars are true to the best of my knowledge.

Place: HYDERABAD **[M.SAINATH]**

Date: