Srisai Charan Rayudu

Fairfax, VA | +15715853889

charan.rayudu1784@gmail.com | LinkedIn | Github | Portfolio

SUMMARY

Security engineer with hands-on experience in penetration testing, application security, and infrastructure hardening. Identified and remediated critical vulnerabilities across 40+ systems through coordinated disclosure efforts. Proficient in designing automated security tools using Python and Golang, and applying frameworks such as **OWASP**, **NIST**, and **CIS benchmarks**. **CompTIA Security+** certified, with practical exposure to cloud platforms (AWS), **DevSecOps** pipelines, and secure code review processes. Strong background in both offensive testing and implementation of defensive controls.

EXPERIENCE

Cyber Security Engineer, *DevFi Inc.,* Fairfax — Oct 2024 - Present

- Conducted IT audits across infrastructure, databases, and web applications, improving vulnerability management by 30% and aligning with NIST standards.
- Managed network security event detection and response, ensuring 100% compliance with legal requirements and optimizing firewall and IT operations.
- Delivered security training to 200+ IT staff, increasing policy adherence by 40% and reducing security incidents by 25%.

Graduate Teaching Assistant, *George Mason University*, Fairfax — Aug 2023 - May 2024

- Engineered Python scripts to automate extraction of sensitive data across Top 1M websites, enhancing detection of critical vulnerabilities such as email addresses, SSNs, IP addresses, and API keys.
- Mentored over 100 grad students in secure coding for Cybersecurity Capstone, reducing code vulnerabilities by 40%.
- Designed Capstone assignments on web/mobile application vulnerability mitigation, leading to 95% student success in Sage Conference.

Bug Bounty Hunter, *Freelance*, Remote — Mar 2020 - Aug 2022

- Secured over 40 companies via Vulnerability Disclosure Programs on platforms such as HackerOne and Bugcrowd, identifying critical bugs such as RCE, SSRF, and file upload vulnerabilities.
- Authored reconnaissance tools for vulnerability discovery and response, participating in CTF competitions to enhance red teaming skills.

Penetration Tester - Consultant, *US-Based Client (NDA-protected)*, Remote — Sep 2021 - Dec 2021

- Evaluated policies and served as a specialist on best practices, strengthening the organization's information security stance by 50%.
- Scrutinized systems for vulnerabilities (OWASP Top 10), leading to the mitigation of over 25 high-risk vulnerabilities.
- Employed industry-standard tools and methodologies, such as vulnerability scanners and manual testing techniques, to identify security weaknesses.

Red Team Penetration Tester - Consultant, *Fresh Digital*, India — Oct 2020 - May 2021

- Detected over 50 security vulnerabilities, including SQL injection, XSS, CSRF, LFI and Authentication Bypass, gained hands-on experience with DOS, network protocols such as TCP/IP and HTTP.
- Produced reports outlining vulnerabilities, impact, and recommended remediation strategies, interacted with development teams, resulting in a 30% reduction in time required to address security issues.

EDUCATION

Masters in Computer and Information Sciences, **George Mason University, Virginia** | May 2024

Bachelors in Computer Science and Engineering, **Vellore Institute of Technology, India** | May 2022

TECHNICAL SUMMARY

Programming Languages: C, Go, Java, Python, JavaScript, Bash, HTML/CSS.

Security Tools: Burp Suite Pro, Metasploit, OWASP ZAP, SQLmap, Acunetix, Nessus, Snort

DevOps: Git, Docker, AWS, Kubernetes, Jenkins, CI/CD, SAST/DAST, SonarQube, Snyk

Network Tools: Nmap, Wireshark, Cisco Packet Tracer

Operating Systems: Windows, Linux (Kali, ParrotOS, Ubuntu, FreeBSD), Unix, MacOS, Android, iOS.

Hardware: Raspberry Pi, Arduino, Network hardware installation.

Security Operations (SOC): SIEM, Log Analysis, Splunk

Additional Tools: Microsoft 365 Suite, Vulnerability Scanning scripts

PROJECTS

Prototype Pollution Vulnerability Scanner

- Engineered a Golang-based web vulnerability scanner to detect Prototype Pollution, utilizing the Chrome Developer Protocol for concurrent checks and improved scanning efficiency.
- Implemented logging of vulnerable URLs with optional export, ensuring ethical and responsible disclosure.

Automation using Nuclei Vulnerability Scanner

- Developed an automated Bash script in Linux utilizing tools like findomain, subfinder, assetfinder, knockpy, puredns, httpx, to enumerate over 1,000 unique subdomains per domain.
- Conducted vulnerability scans using nuclei templates on 500+ live subdomains, enhancing security measures and threat detection capabilities.

Tiny Recon

- Created a Bash script to automate reconnaissance, performing Nmap scans and discovering over 100 subdomains per domain using crt.sh, significantly enhancing domain visibility.
- Integrated Gobuster and WhatWeb to identify and analyse web directories and technologies on discovered HTTP services, streamlining the web vulnerability assessment process.

ACHIEVEMENTS

- **CompTIA Security+ CE (SY0-701)** – DoD 8570 Compliant IAT Level II
  Validates hands-on skills in network defense, risk management, and secure architecture
- **AWS Certified Cloud Practitioner**
  Foundational understanding of AWS cloud, security, and billing fundamentals
- Secured more than **40 companies** and received Hall of Fame recognitions
- Achieved **"Starstruck" with 118 stars** for a Github repository
- **20709** Rank at TryHackMe (Apr 2024)
- **4540** Rank at Bugcrowd (Aug 2022)