SAHITH REDDY BURLA

Aspiring Cyber Security Analyst

sahithreddi143@gmail.com | +91 6301617318 | Korisapadu, A.P
linkedin.com/in/sahithreddy/ | github.com/sahith143

SUMMARY

Enthusiastic and skilled entry-level cybersecurity professional with hands-on experience in penetration testing, vulnerability assessment, and network security. Demonstrated expertise in identifying and exploiting OWASP Top 10 vulnerabilities through real-world projects and independent bug bounty programs. Adept in using industry-standard tools like Burp Suite, Metasploit, Nmap, OWASP ZAP, and Nessus. Eager to contribute to a dynamic security team and grow as a penetration tester with a strong foundation in offensive security, threat analysis, and scripting automation.

WORK EXPERIENCE

Digit Defence

Jan 2025 - Present

Cybersecurity Trainee

- Conducted **internal penetration testing** using Metasploit and Nmap to uncover misconfigurations and security loopholes.
- Executed **web application vulnerability assessments**, focusing on **OWASP Top 10** issues like SQL Injection and XSS.
- Utilized **Burp Suite** to intercept and analyze HTTP/S traffic, improving application security posture and reducing risk by **30%**.
- Automated vulnerability scanning tasks with **Python**, increasing audit speed and accuracy.
- Participated in **social engineering simulations** to identify organizational risk and strengthen employee security awareness.

PROJECTS

Web Application Security Assessment

Skillogic, Bangalore | Apr 2025 - Present

- Performed thorough vulnerability scanning and penetration testing using OWASP ZAP and Burp Suite, identifying critical security issues with a detection accuracy of 95%.
- Developed and tested exploits for identified vulnerabilities, using Metasploit and SQLmap, achieving a successful exploitation rate of 90%.
- Achieved 81% accuracy in identifying and documenting critical vulnerabilities during the web application security assessment using tools such as OWASP ZAP and Burp Suite.

Skills Applied: OWASP ZAP, Burp Suite, Nessus, Metasploit, SQLmap, Wireshark

Network Security Simulation

Skillogic, Bangalore | Mar 2025 – Present

- Designed and configured virtual networks to represent various topologies using GNS3 and Cisco Packet Tracer.
- Performed detailed network traffic analysis and vulnerability assessments using Wireshark, Nmap, and OpenVAS, achieving high accuracy in detecting potential security breaches.
- Achieved 82% accuracy in detecting simulated cyber threats and vulnerabilities using tools such as Nessus and Metasploit during the security testing phase of the Network Security Simulation Project.

Skills Applied: Cisco Packet Tracer, Nessus, Snort, Wireshark, Nmap, Metasploit, OpenVAS, OpenVPN

TECHNICAL SKILLS & TOOLS

- **Penetration Testing**: Web App, Network, API Security, OWASP Top 10, Bug Bounty
- **Vulnerability Assessment**: SQL Injection, XSS, CSRF, SSRF, File Inclusion
- **Security Tools**: Metasploit, Burp Suite, OWASP ZAP, Nessus, Nmap, Wireshark
- **Network Security**: GNS3, Cisco Packet Tracer, OpenVAS, Snort
- **Scripting & Automation:** Python (security scripting), Bash, SQL
- **Cloud Security**: Basic AWS Security, IAM Policy Understanding
- **Social Engineering & Red Team Simulations**
- **Threat Detection & Response:** Log Analysis, IDS/IPS, SIEM Basics

SOFT SKILLS

- Adaptability
- Problem-Solving
- Time Management
- Critical Thinking
- Attention to Detail
- Communication

EDUCATION

Bachelor of Technology in Electronics and Communication Engineering
Lovely Professional University, Punjab | Aug 2021 – Jul 2024
CGPA: 8.83
Relevant Coursework: Java, Data Science, Communication Networks, Digital Electronics

CERTIFICATIONS

- **IBM** Cybersecurity Analyst Professional Certificate
- Certified Cyber Warrior (**Hackingflix**)
- **AI** Cyber Security Associate **(IIFIS)**
- Cyber Security Professional (**Future Skills Prime & Skillogic**)
- Communication Networks (**NPTEL**)

NOTABLE ACHIEVEMENTS

- Discovered and reported critical **vulnerabilities** in a real-world web application as part of an independent **bug bounty** program.
- Ranked in the Top 5% in cybersecurity **Capture The Flag (CTF)** competitions.
- Published security research on **OWASP** vulnerabilities on **GitHub**.