SULABH KUMAR JAIN

Penetration Tester

Thriving Red Team VAPT professional with a passion for exploiting vulnerabilities and crafting bulletproof remediation plans. I actively hone my skills through Open Bug Bounties and by conquering challenges on platforms like PortSwigger Labs, TryHackMe, and CTFs. I'm eager to leverage my real-world expertise and infectious enthusiasm to fortify your dynamic cybersecurity team.

Contact

+919942331008

kr.sulabhjain@gmail.com

linkedin.com/in/sulabhkumarjain

https://github.com/sulabhjain11

Thakurganj, Bihar

Education

- Bachelor of Technology in Computer Science and Engineering

  Vellore Institute of Technology,Tamil Nadu
  2019 - 2023

Language

- Python Scripting
- Powershell
- Bash scripting, Git

Certification

- Cyber Defense Engineering Using Python | Cybervidyapeeth Foundation.
- Cyber Security Hackathon and Value Added Program | VIT CHENNAI
- CEHV11 | EC-Council | Training Certificate.

Work Experience

RED TEAM INTERN TRAINEE

Cybersapiens United LLP, Bengaluru 12/2023 - 08/2024

- Secured clients with over 15 vulnerabilities, during red team vulnerability assessments. Vulnerabilities include blind SQL Injection, file upload leading to XSS, session fixation, violation of DPDP Act, BAC, amongst others.
- Research on various web application vulnerabilities, documentation, and spreading security awareness.
- Consistently stayed current with emerging threats, attack methodologies, and cybersecurity tools through continuous learning.
- Collaborated with the team to provide effective remediation strategies, enhancing client security posture.

KNOWLEDGE

- CIA, ISO27001:2013
- DPDP Act, NIST, GDPR
- Vulnerability Management
- Risk Management, Third Party Risk Management
- Data Privacy
- Cyber Attacks & Data Breaches
- Governance, Risk & Compliance GRC, IT/Security Audits
- VAPT, Ethical Hacking, Defensive & Offensive Testing
- Network Security, SAST, DAST
- TCP/IP, Kali Linux
- OWASP TOP 10
- Cryptography, Hashing
- Machine Learning

TOOLS

- Burpsuite pro
- OSINT Tools
- metasploit framework
- OWASP ZAP
- postman
- nessus, nikto
- Network Security Tools: Nmap, Wireshark, Cisco Packet Tracer, masscan, netcat.
- Specific framework scanners: wpscan, sqlmap, john the ripper.

Skills

- Manual Web Application VAPT
- Manual Network VAPT
- Bug Hunting
- Reporting & Documentation
- Presentation
- Verbal and Written Communication
- Research
- Team work
- Problem Solving
- Scripting
- System Hardening
- white-box testing, black-box testing
- API testing

Achievements

- Published paper on Credit Card Fraud Detection System using SMOTE-ENN and ADAPTIVE XGBOOST in IEEE.
- OS hardening index tool has been in use in a reputed company
- Included in Philips Hall of Honour for securing their website.
- Secured websites such as Philips, IISC Bangalore, DS Group, Evernote, Tonies, Cricket Australia

Projects

Research on Networking layer's using python's scapy

- Wrote python scripts to create scanners(arp scan, ICMP scan, TCP scan, UDP scan, traceroute using icmp, tcp and udp protocols) and some basic networking attacks(arp poisoning, MITM using arp poisoning, ICMP flood, ICMP redirect, ping-of-death attack, smurf attack, tunneling,).
- Used scapy to understand networking in-depth.

Optimizing Windows 10 Security through Automated CIS Hardening and Assessment Tool

- Automated Hardening: Hardens the Windows 10 OS automatically based on CIS compliance recommendations.
- The tool fully automates 492/492 policies as recommended by CIS framework for Windows 10.
- Reduces policy hardening time by 99%.
- Detailed Reporting: Generates report in command line and Excel format for easy analysis

Securing the Foundation: White-Box Pentesting & Feature Extension in v-Lab

- Responsible for white-box penetration testing of vlab portal of Vit Chennai.
- Developed the administration based features for administrators, and learning module for students.
- Found various vulnerabilities and patched them. Vulnerabilities included Information Disclosure, Broken Authentication, Password Hashing, Insufficient Access Control, XSS, DOS, SQL Injection, Insufficient Input validation.