Jyotishwar Raval

Cyber Security Analyst

Gandhinagar, Gujarat

+91 9998164676 • Jyotishwarraval@gmail.com • https://www.linkedin.com/in/jyotishwarraval/ • https://github.com/Jyotishwar-Raval/

Cybersecurity professional with hands-on experience in penetration testing, vulnerability assessment, and secure code analysis. Skilled in OWASP Top 10, network security, and cloud security assessments (AWS/Azure). Experienced in conducting SAST & DAST scans using GitHub workflows and tools like Semgrep & OWASP ZAP.

EXPERIENCE

Microsoft **02/2024 -03/2024**

Microsoft Student Ambassador

- I actively engaged in hands-on exercises, collaborated with fellow participants on challenging projects, and absorbed knowledge from industry experts. I delved into various aspects of AI Finished more than 20 modules in Microsoft in AI.
- I have shared the link to my transcript -> https://learn.microsoft.com/en-us/users/jyotishwarraval-8520/

Edureka **12/2023-03/2024**

Cyber Security and Ethical Hacking Internship

- Identified needs of customers promptly and efficiently.
- Knowledge about Networking
- Expert in Scripting
- Good hands-on programming
- Experience with servers and search engines
- Well-versed with available tools in market

LDR International School **1/2023-12/2023**

IT Admin

- Provided technical guidance to staff members regarding best practices in IT operations.
- Logged and prioritized IT-related service requests, ensuring timely resolution to enhance internal operations.
- Installed, configured, and maintained hardware such as computers, and printer.
- Collaborated with teams to address technical issues, contributing to a seamless guest experience

EDUCATION

- **Professional Certificate in Cybersecurity by IITM-Pravartak**
- **Bsc Cyber Security**

SKILLS

Tools: Nessus, Wireshark, Metasploit, Nmap, fail2ban, Snort, Kali Linux, OWASP ZAP, Burp suite, Kali (Advanced), Intrusion Detection, VAPT, Networking, Google Header Analyzer, Splunk, SonarQube, Threat Dragon

Operating Systems: Windows Server, Unix/Linux, Android, iOS

Programming Languages: Python (Proficient), C++ (Intermediate), PowerShell (Intermediate), Bash (Proficient)

Security Practices: Network Security, Cryptography, Access Control Systems, Threat Modeling, Security Auditing, CTF Player (THM, Picoctf)

OTHER

Certifications: Linux Professional Certified (Edureka), Microsoft Student Ambassador (Micorsoft), AI Tools workshop, Security Analyst Job Sim (TCS), Cybersecurity Job Sim (Mastercard), Cyber Security and Ethical Hacking Internship Program (Edureka), C++, AI mastery, Python Mastery.

Projects:

Steganography Tool

- Developed a **Python-based steganography tool** that securely hides and retrieves messages in images, ensuring data confidentiality. Implemented metadata validation, double-encoding detection, and GUI-based interaction for ease of use.

IP Hardening & Attack Surface Reduction

- Implemented IP and network hardening techniques to secure servers against unauthorized access, DDoS attacks, and network intrusions. Configured firewalls, SSH security, service restrictions, and SIEM-based monitoring to enhance system resilience.

Windows Server Logging & Security Analysis

- Implemented **advanced logging, centralized monitoring, and event correlation techniques** to enhance Windows Server security. Configured **Sysmon, SIEM integration, and PowerShell auditing** to detect and respond to cyber threats efficiently.

Automated Secure Code Analysis with Semgrep & GitHub Workflows

- Executed SAST scans on a static web application using GitHub Actions and Semgrep, identifying and mitigating vulnerabilities. Integrated security best practices into the CI/CD pipeline, ensuring automated secure code reviews and compliance with OWASP Top 10 standards

Dynamic Application Security Testing (DAST) with OWASP ZAP

- Conducted DAST scans on a running web application using OWASP ZAP and GitHub Actions, identifying security vulnerabilities in real-time. Automated security testing in the CI/CD pipeline, improving application security and compliance with OWASP Top 10 standards.

Deploying a Honeypot in Linux to secure server for Threat Intelligence using Pentbox

- Implemented a network honeypot using Pentbox to detect and log unauthorized access attempts. Monitored and analyzed attacker behavior to enhance intrusion detection and incident response strategies. Strengthened network security by gathering threat intelligence and mitigating reconnaissance attacks.