

# Prachi Oza

prachi-oza.github.io | prachi.oza92@gmail.com | +919106887920 | linkedin.com/in/prachi-oza/

## EDUCATION

### UNIVERSITY OF MARYLAND

#### MENG IN CYBERSECURITY

May 2023 | College Park, MD

GPA: 3.9 / 4.0

### NIRMA UNIVERSITY

#### BTECH IN COMPUTER ENGINEERING

June 2020 | Gujarat, India

## SKILLS

### PROGRAMMING & SCRIPTING

Python • Shell • C • C#

PowerShell • Bash

### SECURITY TOOLS

Wazuh • Splunk • Metasploit • Nessus

Burp Suite • Wireshark • Docker

### FRAMEWORKS & STANDARDS

ISO 27001 Series • NIST • PCI-DSS • AWS

## INTERNSHIPS

### BONUM TECHNOLOGIES LLC

Network Specialist Intern

Jul 2022 - Aug 2022 | Remote, TX

- Diagnosed network server performance and managed firewall rules using OPNsense and system diagnostic tools.
- Assisted in reviewing and analyzing Linux server configurations, resulting in significant increase in uptime.

### PROCLINK CONSULTING SERVICES LLP

Cybersecurity Intern

Jan 2020 - Jun 2020 | Gujarat, IN

- Developed custom vulnerability scanner using Python and Kali Linux, identifying critical vulnerabilities in ICSs.
- Conducted penetration tests to exploit vulnerabilities and assess system resilience, improving overall security posture.

## CERTIFICATIONS

- Splunk 7.x Fundamentals
- CompTIA Security+ (SY0701)
- AWS Certified Cloud Practitioner - In Progress

## EXPERIENCE

### FREELANCE | CLOUD SECURITY CONSULTANT

Nov 2025 - Present | Dar Es Salaam, TZ

- Provided freelance AWS cloud security consulting, designing and securing cloud infrastructure for a migration.
- Implemented secure VPC architectures, EC2 deployments, NACLs, security groups, and AWS WAF rules.
- Delivered detailed technical documentation and security recommendations to support a safe and scalable cloud transition.

### BONUM TECHNOLOGIES LLC | SECURITY ENGINEER

Aug 2023 - Mar 2025 | Remote, TX

- Implemented and monitored network security controls using Suricata IDS/IPS and Elastic SIEM, improving threat detection and response capabilities.
- Supported ISO 27001 certification by developing, reviewing, and enforcing information security policies, procedures, and documentation in compliance with international standards.
- Reviewed and maintained the company's SOC 2 report, ensuring alignment with compliance, audit, and risk management requirements.
- Collaborated with certified ISO auditors and cross-functional teams to strengthen the organization's Information Security Management System (ISMS).
- Conducted vulnerability assessments and penetration testing using tools such as OWASP ZAP, Burp Suite, and Nmap, identifying and mitigating security risks.

### FEYNMAN TECHNOLOGY PVT. LTD. | APPRENTICE SOFTWARE ENGINEER

Jun 2020 - May 2021 | Remote, IN

- Designed and enhanced the user authentication system with OAuth 2.0 and token-based authentication, improving login efficiency and reducing latency.
- Developed and maintained scalable web applications, ensuring high availability and seamless user experience.
- Integrated secure coding practices within the SDLC, proactively mitigating vulnerabilities such as misconfigurations and injection flaws.

## PROJECTS

### AUTOMATED BOT DETECTOR Present

- Designing an AI-driven bot detection system to distinguish automated traffic from human users using behavioral and request-level signals.
- Evaluating model strategies including logistic regression, tree-based models, and unsupervised anomaly detection for bot classification.

### SOAR AUTOMATION HOME LAB May 2025 - Jul 2025

- Developed an open-source SOAR lab integrating Shuffle, Wazuh, VirusTotal, AbuseIPDB, and Slack automating threat enrichment and triage.
- Built custom playbooks to extract IOCs, enrich alerts, and notify analysts, reducing manual triage effort by 80%.

### SECURE CODE REVIEW Oct 2022 - Dec 2022

- Conducted secure code reviews using Mitre CWE, SonarQube, Snyk, and Roslyn analyzer to identify 10+ OWASP Top Ten vulnerabilities.