

# BHARAT GURBAXANI

bharatg@umd.edu | (240) 481-3472 | [Linkedin](#) | [Website](#)

## EDUCATION

### Master of Engineering, Cybersecurity

University of Maryland

Expected May 2025

GPA – 4.0

**Key Coursework:** Cloud Security, Cloud Computing, Penetration Testing, Linux System Administration, Digital Forensics and Incidence Responses

### Bachelor of Technology, Information Technology

SRM University

May 2019

GPA – 83%

## TECHNICAL SKILLS

**Cloud:** AWS EC2, AWS Lambda, AWS S3, AWS RDS, AWS IAM, AWS Route 53, AWS Cloudfront, AWS WAF

**Language & Tools:** Wireshark, Linux, Python, C, Windows, Microsoft Office Suite, Nmap, Autopsy

**Virtualization:** VMware Workstation, Oracle VirtualBox

**Penetesting Tools:** Nessus, Ghidra, Metasploit, OWASP ZAP, John the Ripper, Sqlmap

## WORK EXPERIENCE

### Graduate Teaching Assistant – Penetration Testing [[ENPM634](#)]

University of Maryland, College Park

Aug 2024 – Present

- Designed a lecture on pentesting AWS environments using CloudGoat and Pacu and led in-class exercise.
- Provided guidance to 140 students, fostering critical thinking and problem-solving while contributing to course content development.

### Security Consultant-I (Team Lead)

Highradius Technologies, Hyderabad India

Jan 2019 – Feb 2022

- Received the HighFlyer (Rewards and Recognition) award for Q3, 2021 for managing a team of 8 consultants, designing enterprise solutions, defining MVPs, and reducing the team's knowledge gap by 18% through the implementation of a comprehensive "PlayBook" guide.
- Managed the infrastructure vulnerability scanning program by leveraging Rapid7 Nexpose and Qualys scanners, automating the integration of proprietary network inventory sources with the Rapid7 Nexpose scanner and performing quality control checks on the scanning infrastructure.
- Conducted White-box/Black-box/Grey-box application assessments using manual techniques and automated reviews with dynamic application scanning (DAST) tools (like Burp suite), identifying root causes and recommending remediation. Additionally, performed static source code reviews using HP Fortify and IBM App Scan.
- Identified web application security weaknesses using OWASP Top 10 as a baseline, including identifying insecure development practices or application design. Leveraged industry tools like Acunetix and Burpsuite, open-source tools, and manual testing to identify various security issues and provide appropriate recommendations.

## PROJECTS

### Infrastructure Migration on AWS and Security Enhancement

- Succeeded in leading the migration of an on-premises infrastructure to AWS cloud, ensuring improved scalability, availability, and reliability.
- Implemented various AWS services and tools to enhance the security posture of the infrastructure, including AWS Patch Manager, AWS Backup, AWS IAM, AWS Shield, Web ACLs through WAF, and CloudFront, AWS RDS for secure storage of PII and credit card information.
- Configured application load balancer and auto scaler to ensure efficient resource utilization and high availability of critical resources.

### Scalable and Secure E-commerce Platform on AWS

- Architected resilient cloud infrastructure with Auto Scaling, Elastic Load Balancer, and multi-AZ VPC for high availability.
- Implemented layered security using AWS WAF, Shield Advanced for DDoS protection, and SSL/TLS encryption via ACM.
- Enhanced global content delivery with CloudFront edge caching and Route 53 geolocation routing to minimize latency.
- Set up proactive monitoring with CloudWatch and auditing via CloudTrail for performance insights and compliance.
- Conducted Jmeter stress tests; optimized costs using AWS Trusted Advisor and Cost Explorer.

### 2-Tier LAMP Stack Deployment with Security Enhancements

- Deployed a 2-tier LAMP architecture using VMs for web and database services, configured HAProxy for load balancing to ensure high availability.
- Implemented iptables and fail2ban for enhanced security, including rate-limiting SSH connections to prevent brute-force attacks and automatically blocking IPs after repeated failed login attempts.
- Enforced password policies using PAM (Pluggable Authentication Modules) for password expiration and complexity requirements, ensuring system-wide compliance with security standards.
- Configured ACLs to restrict webadmin access to only the /var/www/html directory, blocking modifications to WordPress and phpMyAdmin.

### Pentesting on a Vulnerable Virtual Server [CTF]

- Succeeded in capturing all the flags (6 flags) hidden on the server.
- Demonstrated the use of Weevely to obtain shell access, Zphisher to phish the CEO of the company, Sqlmap to leak the database, John the Ripper to crack the password, Python script to decrypt the base64 encoding.

## CERTIFICATIONS

INE Junior Penetration Tester [eJPT]

Dec 2023