Vedang Lad

2409277745 | vedangslad31@gmail.com | College Park, MD | LinkedIn | Portfolio Website | GitHub

PROFESSIONAL EXPERIENCE

Cybertrust America **August 2024 – Present**
Cyber Security Analyst *San Jose, California*

- Performed vulnerability assessments on the organization's website using OWASP ZAP, identifying security weaknesses.
- Validated vulnerabilities using Burp Suite, ensuring accuracy by eliminating any false positives.
- Collaborated on generating detailed reports of findings and provided recommendations to mitigate identified vulnerabilities.
- Assisted in developing incident response plans and playbooks, and supported the implementation of IR recommendations.

Vodafone Intelligent Solutions **August 2020 - July 2022**
Senior Executive (ETL Developer) *Pune, India*

- Reduced data processing time by 50% for multiple ETL processes through enhancements to existing shell scripts.
- Achieved a 15% improvement in database performance by optimizing SQL queries and PL/SQL procedures.
- Successfully migrated legacy Oracle reports to Qlik Sense, enabling faster access to data insights for better decision-making.
- Conducted thorough code reviews and implemented best practices, leading to a 30% reduction in post-release bugs.

Orane Labs Private Limited **January 2019 - June 2019**
Web Backend Developer Intern *Pune, India*

- Developed multiple web features using Python and the Flask Framework, resulting in a 60% increase in user engagement.
- Successfully fixed bugs in the website source code, enhancing overall stability.
- Used Git for code management by handling branch creation, merging and conflict resolution for better team collaboration.

TECHNICAL SKILLS

Security Tools	: Burp Suite, Metasploit, Wireshark, Nmap, OWASP ZAP, Splunk, GDB
Programming Languages	: Bash Scripting, PowerShell, Python, C, MySQL, HTML, CSS, JavaScript
Other Skills/Knowledge of	: Cyber Kill Chain, MITRE ATT&CK, Scripting, Automation, Git
Interpersonal Skills	: Quick Learner, Attention to Detail, Troubleshooting, Problem-solving, Team Collaboration

CERTIFICATIONS

- CompTIA Security+, CompTIA
- Certified in Cybersecurity (CC), ISC2
- Practical Ethical Hacking, TCM Security
- Certified Penetration Testing Specialist (CPTS), HackTheBox (In-progress)

EXTRA-CURRICULAR

- Participated in jeopardy-style Capture The Flag (CTFs) events like NahamCon CTF 2025, UofTCTF 2025 and N0PSctf 2025.

EDUCATION

Master of Engineering in Cybersecurity, *University of Maryland College Park* Maryland, USA
Bachelor of Technology in Information Technology, *Symbiosis Institute of Technology* Pune, India

PROJECTS

HackTheBox (HTB) Penetration Testing Reports
Penetration Testing, Reporting, Kali Linux, Windows, Linux, Git | Project-Link

- Conducted black-box penetration testing on HTB machines (Linux/Windows), simulating real-world attack scenarios.
- Performed reconnaissance, enumeration, exploitation, pivoting, privilege escalation using various security tools.
- Identified and exploited various vulnerabilities, misconfigurations, and learned how to mitigate them.
- Summarized all findings in a professional penetration test report, including suggestions on remediating them.

Common Network Services Enumeration
Network Enumeration, Service Enumeration, Git | Project-Link

- Developed and maintained a GitHub repository containing enumeration commands for various network services.
- Curated a structured reference of enumeration techniques using different tools aiding in effective information gathering.
- Documented enumeration techniques for various network services such as FTP, SSH, SMB, DNS, SQL, RDP, etc.

Network Security Assessment
Penetration Testing, Vulnerability Assessment Report, Active Directory, Kali Linux | Academic Project

- Conducted a comprehensive penetration test on a dynamic Active Directory environment.
- Utilized a diverse range of penetration testing tools to pinpoint and exploit critical vulnerabilities.
- Crafted a thorough penetration testing report consolidating network enumeration and vulnerability exploitation findings.
- Recommended measures that bolstered security resilience and risk mitigation within the network infrastructure.

Digital Forensics: Investigating Anomalous Incidents
Autopsy, Wireshark, Python, Malware Analysis, Digital Forensics | Academic Project

- Conducted in-depth forensics assessment on a malware affected machine using Autopsy and Wireshark.
- Performed detailed log collection and analysis of encoded network communications and user activities.
- Prepared a concise, detailed forensic report summarizing findings, methodologies, and mitigation recommendations.