Mohammad Sufiyan Mulla

Penetration Tester

+91-9353655818 sufiyanmulla771@gmail.com linkedin.com/in/mohammadsufiyanmulla My Portfolio: Click Here

Summary

I have 1+ year of experience in bug hunting, freelancing, and working as a Cyber Security Intern, where I applied practical skills to identify and exploit real-world vulnerabilities. Motivated to contribute to secure system development and perform impactful security assessments. Completed professional certification in advanced penetration testing covering areas such as Network Security, Web Application Testing, Vulnerability Management, Wireless Security, Active Directory (AD) Pentesting, Docker and Cloud Security, and Thick-Client Pentesting. Hands-on experience with VAPT methodologies, exploitation techniques, and security reporting. Strong understanding of OWASP Top 10, reconnaissance, privilege escalation, and post-exploitation processes. Motivated to apply technical skills in real-world security assessments and contribute to secure system development.

Experience

Cybersecurity Intern **15 Nov 2025 – Present**

Unified Mentor Private Limited *Internship*

- I am currently working as a Cybersecurity Intern at Unified Mentor, where I am actively involved in real-time security operations, ethical hacking activities, and hands-on vulnerability assessment projects. Throughout my internship, I have been learning and practicing core cybersecurity concepts including ethical hacking fundamentals, virtual lab setup, Linux basics, networking, Wireshark analysis, OSINT techniques, information gathering, and an introduction to malware. In addition to structured modules and assignments, I am working on real-time projects that involve scanning systems, testing applications, and performing practical exploitation techniques within a controlled lab environment.
- My role includes conducting vulnerability scanning, analyzing system logs, assisting in incident response, and helping identify, evaluate, and mitigate potential security threats. I am developing a strong foundation in Web Application Penetration Testing (WAPT) and gaining practical experience with the OWASP Top 10 vulnerabilities. I regularly use professional security tools such as Burp Suite, Wireshark, SQLMap, Nmap, Kali Linux, and other penetration testing utilities to perform manual and automated testing. These tasks include traffic analysis, reconnaissance, enumeration, basic exploitation, and documentation of findings for internal security reports.
- This internship is helping me sharpen my technical expertise, analytical thinking, and problem-solving abilities while working in a structured professional environment. I am continuously learning and applying advanced security techniques, which is making me more confident and fully prepared for stronger, more challenging roles in penetration testing and cybersecurity.

Cloud Application Developer Intern **24 Feb 2025 – 20 May 2025**

Rooman Technologies Pvt. Ltd. *Internship*

- I have also successfully completed an internship at Rooman Technologies Pvt. Ltd., conducted under Skill India and NASSCOM, where I gained hands-on experience in cloud-based application design, deployment, and modern IT infrastructure workflows. During this training, I worked on real-time cloud concepts, learned how to design scalable architectures, and implemented application deployment strategies on cloud platforms. I developed practical skills in API integration, cloud resource management, and handling data efficiently across distributed environments. This internship enhanced my understanding of cloud technologies, application lifecycle management, and modern DevOps-aligned practices, adding strong versatility to my cybersecurity and technical skill set.

Security Researcher — Independent Bug Bounty Hunter **13 Dec 2024 - Present**

Bug Bounty Platforms - Bugcrowd,Hackenproof *Part-time*

- Experienced security researcher specializing in web application security, vulnerability discovery, and responsible disclosure. Independently identified and reported real-world SQL Injection (SQLi) vulnerabilities on production websites, including platforms without official bug bounty programs.
- Skilled in identifying and exploiting OWASP Top 10 vulnerabilities, including SQLi, XSS, IDOR, File Upload vulnerabilities, WordPress security weaknesses, and API Pentesting techniques. Proficient in manual testing using Burp Suite—payload manipulation, parameter tampering, request interception—and automated validation using SQLMap to confirm exploitability.
- Conducted in-depth backend response analysis, engineered precise proof-of-concept payloads, and delivered professional vulnerability reports with clear remediation steps. Demonstrates strong practical understanding of WAPT methodologies, ethical reporting standards, and applying professional penetration-testing techniques in real-world environments.

Projects

- **Final Year Project, SECAB INSTITUTE OF ENGINEERING & TECHNOLOGY College :** Developed Exomate Forearm, a wearable device for forearm support, as my final year project. Funded by The New Age Innovation Network (NAIN), Govt. of Karnataka with 1.25 Lakhs.
- **Freelancing (SQL Injection and DB Security Expert) :** I've completed the SQL injection testing on the dpboss website using both manual techniques (via Burp Suite) and automated tools like SQLMap.
  -Project Details : My Dp Boss website needs a thorough, end-to-end security hardening. I want a full cyber-security assessment that starts with an aggressive penetration test and finishes only when every critical vulnerability is patched and verified. The core focus areas are:
  • SQL injection prevention
  • Database security (configuration, access control, backup integrity)
  • Overall security testing, including logic flaws and server-side weaknesses
  -Please map out the entire attack surface, exploit anything you can in a controlled environment, document reproducible steps, and then close the holes. A concise report detailing findings, risk levels, recommended fixes, and evidence of successful remediation is the final deliverable. Retesting after fixes is mandatory; only a clean bill of health will mark the project complete.

Education

Bachelor of Engineering in Computer Science and Engineering **2021-2025**
Visvesvaraya Technological University

Certifications

• CPT (Certified Penetration Tester) from The Red Team Hacker Academy
• Cloud Application Developer by Rooman Technologies Pvt. Ltd

Skills

Skilled in identifying and exploiting SQL Injection (SQLi), Cross-Site Scripting (XSS), Insecure Direct Object References (IDOR), File Upload vulnerabilities, WordPress security weaknesses, and API Pentesting techniques. Experienced in manual vulnerability assessment, privilege escalation on both Linux and Windows, and understanding Denial of Service (DoS) attack concepts. Knowledgeable in network security scanning, including TCP/IP, DNS, VPN fundamentals, and hands-on practice across platforms such as TryHackMe, VulnHub, PortSwigger Web Security Academy, DVWA, and Metasploitable 2, covering the OWASP Top 10 and real-world web application testing scenarios.

Tools

Proficient with a wide range of cybersecurity tools, including Nmap for network scanning and enumeration, Burp Suite for web application testing, and Metasploit for exploitation. Experienced with Hydra for password attacks, John the Ripper and Hashcat for password cracking, and WPScan and Nikto for identifying WordPress and web server vulnerabilities. Familiar with directory brute-forcing tools like Dirb and Gobuster, as well as Netcat for networking and reverse shells. Able to set up and manage virtual labs using VirtualBox and VMware for safe testing and practice environments.

Hobbies

Traveling, practicing bug bounty hunting in free time and working on small freelancing projects to build my experience.

Language Skills

Mother tongue(s): Urdu
Other language(s): Marathi & English

All the above information are true and correct to the best of my knowledge and belief.
Yours sincerely : Mohammad Sufiyan Mulla