ALHAM RIZVI *Offensive Security Researcher & Penetration Tester*

its47h4m@gmail.com +91 8329478587 Mumbai, Maharashtra alham-rizvi alhamrizvi-cloud

Summary

Offensive Security Researcher & Pentester skilled in Web, API, and Network security, scripting, cryptography, exploitation, and vulnerability research. Verified bug bounty hunter and ranked Top 6 nationally on TryHackMe.

Experience

Cybersecurity Intern 12/2025 – Present
Redynox
- Configured firewall rules, secure authentication, and encrypted network access.
- Analyzed network traffic via Wireshark to detect suspicious HTTP/DNS patterns and unauthorized access.
- Performed vulnerability scanning using OWASP ZAP and manually exploited SQLi, XSS, and CSRF with mitigation documentation

Cybersecurity Intern 07/2025 – 11/2025
TheWebsiteMakers Pvt.Ltd Remote
- Worked hands-on with core security tools including Nmap, Metasploit, Wireshark, Burp Suite, and OWASP ZAP.
- Performed supervised vulnerability scanning and security testing on web applications.
- Gained practical experience in network scanning, packet analysis, and exploitation fundamentals.
- Assisted in preparing security documentation and concise vulnerability reports for tested applications.

Security Researcher 05/2025 – Present
Bug Hunter (Intigriti, Hackerone, OpenBugBounty)
- Discovered and reported 7 verified vulnerabilities, including exposed JavaScript files, misconfigured S3 buckets, Samba shares, subdomain takeover, and JWT misconfigurations.
- Performed reconnaissance, vulnerability identification, proof-of-concept (PoC) creation, and report writing for web applications.
- Verified fixes and followed up to ensure successful remediation of reported vulnerabilities.

Education

Bachelor's in Computer Science 2024 – 2027
Rizvi Degree College, Bandra

Skills

Penetration Testing: Web, API & Network Pentesting VAPT Reconnaissance & Enumeration Exploitation Active Directory Pentesting. Basic Source Code Review

Core Security Knowledge: OWASP Top 10 MITRE ATT&CK JWT & OAuth TCP/IP HTTP/HTTPS Cryptography (Hashing, Keys, Encryption)

Operating Systems: Linux (Kali, Parrot) Windows Server / Active Directory

Programming & Scripting: Python Bash PowerShell SQL JavaScript HTML/CSS

Tools: Burp Suite Nmap Metasploit SQLmap Hydra Wireshark Shodan

Certifications

CRTA: Certified Red Team Analyst | **eJPT:** eLearnSecurity Junior Penetration Tester (INE) | **CNSP:** Certified Network Security Practitioner | **Certified Associate in Cybersecurity:** By Fortinet | **CAPIE:** Certified API Hacking Expert | **Penetration Testing Engineer:** By Alison

Projects

Aspen-Framework - Automated Reconnaissance Tool 08/2025 – Present
- Automated subdomain enumeration, port scanning, and tech fingerprinting, cutting down a significant portion of repetitive recon work.
- Added DNS brute-force, CRT.sh lookups, passive DNS, and Google Dorks, allowing the tool to discover assets that were previously missed during manual enumeration.

403kill - HTTP 403 Bypass tool 11/2025
- Improved access-control testing by automatically identifying 403 responses across endpoints.
- Added header-based and path-based bypass techniques, enabling detection of misconfigurations that manual testing often overlooks.

Tr10d - API Finding Tool 08/2025
- Automated detection of API endpoints, keys, tokens, and cloud credentials, reducing the time spent searching through large codebases.
- Enhanced secret discovery accuracy using refined regex patterns and real-time scanning, providing more reliable findings than basic manual reviews.

Achievements

- Ranked **Top #6 nationally** (TryHackMe, Oct 2025) after completing 400+ labs and earning 30+ skill badges.
- Received acknowledgments for responsible disclosure of vulnerabilities, including subdomain takeovers, misconfigurations, and authentication flaws in Bug Hunting Platforms
- Authored **200+ cybersecurity writeups** on CTFs, exploits, and bug bounty methodologies.