ALHAM RIZVI

Offensive Security Researcher & Penetration Tester

✉ its47h4m@gmail.com ☎ +91 8329478587

Mumbai, Maharashtra alham-rizvi

Summary

Offensive Security Researcher and Penetration Tester with hands-on experience in web, API, and network security assessments, vulnerability research, and bug bounty programs. Skilled in reconnaissance, exploitation, tool development, and delivering actionable remediation. Authored 200+ security writeups and reported verified vulnerabilities. Strong foundation in OWASP Top 10, MITRE ATT&CK, Active Directory security, and secure coding principles.

Experience

07/2025 – 11/2025

Cybersecurity Intern

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.

09/2025 – Present

Security Researcher - Bug Hunter (Intigriti, Hackerone, OpenBugBounty)

- Discovered and reported 5 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

2024 – 2027

Bachelor's in Computer Science

Rizvi Degree College, Bandra

Skills

Penetration Testing

Web & API Pentesting, Network Pentesting, Vulnerability Assessment, Reconnaissance & Enumeration, Exploitation, Active Directory Pentesting, Source Code Review

Operating Systems

Linux (Kali, Parrot), Windows, Windows Server/AD

Tools ●●●●○

Burp Suite, Nmap, Metasploit, Nessus, FFUF, SQLmap, Hydra, John the Ripper, Hashcat, Wireshark, Shodan, GitHub

Core Security Knowledge

OWASP Top 10, MITRE ATT&CK, HTTP/HTTPS, TCP/IP, Authentication & Authorization (JWT, OAuth), Cryptography (Hashing, Encryption, Keys),

Programming & Scripting ●●●○○

Python, JavaScript, Bash, SQL, C++, HTML/CSS

Certifications

CRTA: Certified Red Team Analyst • **eJPT:** eLearnSecurity Junior Penetration Tester (INE) •
FortiGate 7.6 Operator: By Fortinet • **Certified Associate in Cybersecurity:** By Fortinet •
Cisco Certifications: Jr Cybersecurity Analyst, Ethical Hacker, Cyber Threat Management, Endpoint Security •
CNSP: Certified Network Security Practitioner • **CAPIE:** Certified API Hacking Expert

Projects

11/2025 **403kill - HTTP 403 Bypass tool**

- Developed a Python-based CLI tool to automate 403 bypass attempts using path and header manipulation.

06/2025 – Present **Cybersecurity Writeups Archive - 200+ Writeups**

- Authored 200+ technical writeups on CTFs, exploit development, and bug bounty techniques.
- Documented step-by-step exploitation workflows, payloads, mitigations, and analysis.
- Built a searchable knowledge base to support ongoing learning and skill growth.

09/2025 – (10/2025) **Tr10d - API Finding Tool**

- Created a Python CLI tool to detect exposed API keys/tokens using automated regex scanning.

07/2025 – 11/2025 **Citizen-Connect: Government Services Platform (Academic Project)**

By University Of Mumbai

- Developed a unified portal integrating multiple Indian government services with responsive front-end and backend modules.
- Integrated an AI-powered chatbot to improve user assistance and overall platform usability.

06/2025 – 09/2025 **Cybersecurity Analyst Virtual Experience Project - Forage**

By Tata, Deloitte, Mastercard

- Identified phishing emails and analyzed indicators of compromise
- Reviewed and assigned appropriate IAM roles and access permissions
- Produced a professional security report summarizing findings and recommendations

Achievements

TryHackMe Ranking Top #6 (October 2025)
Ranked in the National top 6; completed 400+ labs and earned 30+ skill badges in offensive security.

Academic Project Showcase: 2K25 Expo Participant
Presented the Citizen-Connect platform integrating multi-service access and an AI chatbot; recognized for innovation and technical execution.

CTF Participation & Performance Recognition
Gained hands-on red-team experience through CTF competitions, improving teamwork, threat analysis, and exploitation skills.

Bug Bounty Recognition for Valid Vulnerability Reports
Received acknowledgments for responsible disclosure of vulnerabilities, including subdomain takeovers, misconfigurations, and authentication flaws.

Public Speaker - Tech & Cybersecurity Events
Delivered sessions on cybersecurity fundamentals, CTF methodologies, and secure coding practices; recognized for clear communication and audience engagement.