

ALHAM RIZVI

Offensive Security Researcher & Penetration Tester

 its47h4m@gmail.com  REDACTED  alham-rizvi  www.linkedin.com/in/alham-rizvi

SKILLS

Penetration Testing: Web, API & Network Pentesting, Vulnerability Assessment, Privilege Escalation, Reconnaissance

Security Research: JS Recon, Parameter Discovery, API Key Exposure, PoC Development, Automation Scripts

Application Security: Authentication & Access Control Testing, Business Logic Testing, API Security

Infrastructure Security: Linux/Windows Security, Network Protocol Analysis, System Hardening, Virtualization

People & Social: Social Engineering, Security Awareness Testing

Tools: Specialised in Burp Suite, Nmap, Metasploit, Nessus, FFUF, Dirsearch, Subfinder, Amass, SQLmap, | Hydra, John the Ripper, Hashcat, Wireshark, Shodan, Postman, Github

LANGUAGES

Python

Bash

Java Script

CSS

HTML

SQL

C++

EDUCATION

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

Maharashtra HSC XII Board,
Rizvi College of Arts, Science & Commerce
2024

OBJECTIVE

To advance my skills in cybersecurity by focusing on discovering and analyzing vulnerabilities across web applications, APIs, and low-level systems. I aim to apply automated testing, manual research, and practical exploitation techniques to improve security in modern platforms, including cloud environments, Artificial Intelligence, IoT devices, and decentralized applications.

EXPERIENCE

Security Researcher - Bug Bounty (Intigriti Hackerone)

09/2025 – Present

- Participated in bug bounty programs and reported 5 security findings, including one identified through exposed JavaScript files in an S3 bucket and Samba share.
- Hands-on web application testing: reconnaissance, vulnerability discovery, PoC development, and Report Writing.
- Successfully disclosed a subdomain takeover and JWT token Misconfiguration to a private bug bounty program and confirmed remediation.
- Strong practice in responsible disclosure and developer-friendly remediation guidance.

Offensive Cybersecurity Writeups Contributor - Independent/Freelance

06/2025 – Present

- Authored 150+ hands-on writeups covering CTF challenges, practical web exploitation, and real-world bug hunting.
- Documented methodology and tooling, with clear step-by-step solutions to accelerate learning and knowledge sharing.
- Provided practical exploitation analysis and PoCs, including mitigation guidance for XSS, SQLi, SSRF, RCE, LFI, file-upload flaws and subdomain takeover.
- Maintained a searchable knowledge base that highlights problem-solving ability, technical depth, and ongoing community contribution.

STRENGTHS

Efficient

Punctual

Quick Learner

Proactive

CERTIFICATIONS

eJPT: eJunior Penetration Tester(INE) | ID:
161978809

MCRTA (Ongoing): Multi-Cloud Red Team
Analyst

CRTA: Certified Red Team Analyst | ID:
68d5dacce01c42ea0885931d

Cisco: Endpoint Security, Junior Cybersecurity
Analyst , Cyber Threat Management, Ethical
Hacker Certifications

Cybersecurity Analyst Virtual Experience: By
Forage - Tata, Deloitte, and Mastercard

ACHIEVEMENTS

Ranked #6 on TryHackMe

01/09/2025

demonstrating strong problem-solving skills and
consistent offensive security capability.

Completed 400+ cybersecurity labs and earned 30+ skill badges

gaining hands-on experience in penetration testing,
vulnerability assessment, web exploitation, and
network security.

Earned multiple Cisco-issued badges on Credly

(Jr. Cybersecurity Analyst, Ethical Hacker, Endpoint
Security), validating industry-recognized technical
proficiency.

Participated in the 2K25 Expo at Rizvi College

presenting a field project and showcasing a website
developed as part of the initiative.

Participated in 2 offline Capture the Flag (CTF) events

improving teamwork, threat analysis, and practical red-
team decision-making.

Reported multiple valid vulnerabilities in private bug bounty programs

including misconfigurations and takeover scenarios
with confirmed remediation.

Developed custom automation tooling (e.g. Tr10d, XSS-Brute)

that improved reconnaissance efficiency and API
exposure detection in security workflows.

PROJECTS

XSSBrute - Payload & Automation Tool for Cross Site Scripting

11/2025

- Built custom XSS payload lists for bypassing filters
and WAFs.
- Added bruteforce & fuzzing payloads for parameters
and inputs.
- Designed for fast testing in bug bounty labs and CTF
environments.

Security Research Archive - 200 Writeups

06/2025 – Present

- Created 150+ detailed security writeups across web,
API, and CTF labs.
- Documented recon methods, exploitation steps, and
payload usage.
- Improved analysis, reporting, and vulnerability
explanation skills.
- Built a structured knowledge base for continuous
learning.

Tr10d - API Finding Tool, (10/2025)

- CLI tool for security researchers and bug bounty
hunters to detect exposed API keys and tokens from
web pages.
- Built with Python; integrates regex scanning and
automation.

Citizen-Connect Website Field Project

- University field project creating a unified platform
for Indian government services with AI chatbot
support.