Mohd Kaif Shaikh *Offensive Security Analyst & Penetration Tester*

✉ kaif80188@gmail.com ☎ +91 9867691586

Mumbai, Maharashtra in · Mohammad Kaif Ismail Shaikh

Kaifshaikh786

Summary

Offensive Security Analyst & 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

12/2025 – Present
Remote

Cybersecurity Intern
TechnoHacks Solutions Pvt. Ltd.

- Captured and analyzed network traffic using Wireshark; performed Nmap scans and vulnerability assessments.
- Built a secure virtual lab environment and conducted penetration testing, including OWASP web exploits.
- Developed Python scripts, analyzed logs, created phishing simulations, and documented incident response and risk mitigation.

12/2025 – Present
Remote

Cybersecurity Intern
Shadowfox

- 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

Education

2024 – 2027

Bachelor's in Computer Science
Rizvi Degree College, Bandra

Skills

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

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

Tools
Burp Suite Nmap Metasploit SQLmap Hydra Wireshark Shodan

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

Programming & Scripting
Python Bash PowerShell SQL JavaScript HTML/CSS

Achievements

Ranked Top #15nationally (TryHackMe, Oct 2025)
after completing 100+ labs and earning 30+ skill badges.

Authored 50+ cybersecurity writeups on CTFs, exploits, and bug bounty methodologies.

Projects

PhisProX - Phishing Email Detector
- Designed PhisProx threat detection system analyzing sender domains, URLs,
and social engineering tactics with 7-point risk assessment framework

Aspen-Framework - Automated Reconnaissance Tool

- Built an automated reconnaissance framework for subdomain enumeration, port scanning, and technology fingerprinting.
- Integrated DNS brute-forcing, CRT.sh lookups, passive DNS, and Google Dorks for comprehensive asset discovery.
- Reduced manual reconnaissance effort and improved asset coverage by identifying infrastructure often missed during manual enumeration.

Tr10d - API Key Leakage Detection Tool

- Developed a Python-based security tool to detect exposed API keys in JavaScript files and HTML source code.
- Implemented pattern matching and similarity analysis to identify hardcoded or leaked third-party API credentials.
- Enabled early detection of sensitive data exposure, helping improve application security posture and prevent credential misuse.

ParameterX - Parameter Discovcery & Analysis Tool

- Contributed to Python-based web security tool to discover HTTP parameters from URLs, forms, and common parameter lists.
- Automated parameter removal, response comparison, and behavior analysis to highlight potential IDOR and access control risks.
- Improved testing efficiency by prioritizing parameters with high behavioral impact using structured JSON risk reports.

Certifications

- CRTA: Certified Red Team Analyst
- CCEP - Certified Cybersecurity Educator Professional
- Certified Associate in Cybersecurity: By Fortinet CAPIE: Certified API Hacking Expert
- Google Cloud Cybersecurity Certificate