KAIF TARASGAR

Penetration Tester | Offensive Security Analyst | Bug Bounty Researcher

Pune, Maharashtra, India | +91 9823453379 | kaiftarasgar2005@gmail.com

LinkedIn | GitHub | Portfolio | Medium

PROFESSIONAL SUMMARY

Penetration Tester and Offensive Security Analyst with hands-on web application vulnerability assessment, red team operations, and bug bounty research experience. CEH v12, CompTIA PenTest+, CompTIA Security+, CISSP Specialization, and CRTOM certified. **1st place winner at IU Hack2Xploit 3.0 CTF** (600+ participants, Defcon Pune Chapter). Awarded responsible disclosure certificates from Perfios and Sai Life Sciences for identifying authentication failures and security misconfigurations in live production systems. Technical Lead at CREST Cybersecurity Club. Experienced in SQL injection, XSS, authentication bypass, OWASP Top 10 exploitation, network forensics, incident containment, and security advisory report writing across 12+ internships.

BUG BOUNTY & RESPONSIBLE DISCLOSURE

Perfios — User Enumeration via Differential Error Messages (Authentication Bypass)
Certificate of Appreciation | Mar 2026

- **Vulnerability Class:** OWASP A07 — Identification & Authentication Failures. Discovered that `/api/login` and `/api/sendPasswo` returned distinct error responses for registered vs. unregistered emails, enabling unauthenticated account enumeration.
- **Impact:** Attacker could silently harvest valid employee accounts (confirmed: admin@, helpdesk@) for targeted phishing, credential stuffing, and email bombing attacks against the production helpdesk system.
- **Disclosure:** Submitted detailed PoC with curl-based reproduction steps, severity justification, and remediation advisory (unified generic response across both endpoints) through formal Bug Bounty Program.

Sai Life Sciences — DMARC Subdomain Policy Misconfiguration (sp=none)
Certificate of Appreciation — Certified by CISO Srikanth JS | Mar 2026

- **Vulnerability Class:** OWASP A05 — Security Misconfiguration. Identified that sailife.com enforced `p=quarantine` for the root domain but `sp=none` for all subdomains, leaving `*.sailife.com` with zero DMARC enforcement.
- **Impact:** Attacker could spoof `hr@connect.sailife.com` — email passes DMARC, delivers to inbox with no spam warning, enabling Business Email Compromise (BEC) targeting clinical and financial communications.
- **Disclosure:** Submitted via Com Olho Responsible Disclosure Program with live `dig +short TXT` PoC, full attack scenario walkthrough, and DNS remediation recommendation (`sp=quarantine` or `sp=reject`).

ELAN Limited — User Enumeration via Login & Password Reset Endpoints
200rs Bug Bounty Reward | Feb 2026

- **Vulnerability Class:** OWASP A07 — Identification & Authentication Failures. Differential error message pattern on internal IT helpdesk; independently discovered and reported with complete PoC and security advisory.
- Rewarded despite duplicate status — recognized for independent discovery, technical depth of report, and quality of remediation guidance.

EXPERIENCE

Cyber Security Intern — *Hacktify Cyber Security* Apr 2026 – Present

- Conducting web application penetration testing against real-world targets — identifying SQL injection, XSS, IDOR, authentication bypass, and privilege escalation vulnerabilities using Burp Suite and manual exploitation techniques.
- Producing structured security advisory reports with vulnerability classification (CVSS scoring), exploitation PoC, risk impact analysis, and remediation guidance aligned with OWASP Top 10.

Cyber Security Intern — *CyberWarLab* Mar – Apr 2026

- Performed black-box and grey-box penetration tests; identified and documented web application vulnerabilities including authentication failures, insecure direct object references (IDOR), and sensitive data exposure.
- Applied red team TTPs aligned with MITRE ATT&CK — lateral movement, persistence mechanisms, and C2 communication using Sliver framework; produced formal findings reports with PoC exploit chains.

Cybersecurity Intern — *VOIS for Tech (Edunet / AICTE)* Mar – Apr 2026

- Completed structured 4-week program covering ethical hacking, network security, Kali Linux, cryptography, and packet analysis; practiced vulnerability assessment with Nmap, Wireshark, and Social Engineering Toolkit (SET).
- Built a Python-based port scanner for network reconnaissance; explored Gen-AI integration for automated packet analysis and threat detection workflows.

Web Exploit Hunting & Bug Bounty Intern — *EduSkills Academy (AICTE)* Oct – Dec 2025

- Ranked **Outstanding (O)** — highest grade — in 10-week offensive security internship; developed expertise in SQL injection, XSS, SSRF, XXE, and SSTI attack vectors covering OWASP Top 10.
- Produced professional bug reports with CVSS-rated severity, step-by-step reproduction, indicator of compromise (IOC) documentation, and remediation recommendations.

Cyber Security & Ethical Hacking Virtual Intern — *Cryptonic Area* Jan – Mar 2026

- Awarded Letter of Recommendation from CEO; executed vulnerability assessments covering authentication bypass, privilege escalation, and web application security testing.
- Delivered structured security advisory reports documenting attack vectors, severity ratings, exploitation scenarios, and incident containment recommendations.

Cyber Security Intern — Advanced Level — *ShadowFox* Sep – Oct 2025

- Completed MSME and ISO 9001-certified program; performed network penetration testing, password cracking, hash analysis, and network security analysis using Metasploit, Nmap, and Wireshark.
- Conducted threat actor profiling exercises and practiced lateral movement and persistence techniques in isolated lab environments.

Additional Internships (2025)

- **Palo Alto Cybersecurity Virtual Intern** — AICTE (Jul–Sep 2025): NGFW, SIEM, SOC operations, incident containment, and Palo Alto Networks tooling across 10 weeks.
- **Ethical Hacking Virtual Intern** — EduSkills Foundation (Apr–Jun 2025): SQL injection, XSS, web application security testing with real-world exploit labs.
- **Zero Trust Cloud Security Virtual Intern** — Zscaler (Jan–Mar 2025): Zscaler Zero Trust Exchange architecture and cloud security access control frameworks.
- **Python Developer / Programmer** — VaultofCodes & CodSoft (Aug–Sep 2025): Security automation scripting and offensive tooling development in Python.
- **Cyber Security Intern** — Prodigy InfoTech (Jul–Aug 2025): Cybersecurity fundamentals, network security analysis, and Python scripting for security automation.
- **AI & Machine Learning Intern** — Edunet Foundation / IBM SkillsBuild (Dec 2025–Jan 2026): Built AI-powered resume builder; applied GenAI to cybersecurity threat detection use cases.

EDUCATION

Bachelor of Science — Cyber Security and Forensics Aug 2024 – Apr 2027
Pimpri Chinchwad University, Maval, Pune | Focus: Network Security, Ethical Hacking, Digital Forensics, Incident Response

LEADERSHIP & COMMUNITY

Technical Lead — *CREST Cybersecurity Club, Pimpri Chinchwad University* Current

- Lead technical initiatives and offensive security awareness programs for 100+ club members; mentor junior members on penetration testing methodology and CTF techniques.
- Organized and hosted club CTF competition (Feb 2026, 2026 participants) — designed multi-category challenges spanning Web Exploitation, Cryptography, Password Cracking, Forensics, and OSINT.
- CTF challenges remained unsolved by first-ranked teams, demonstrating advanced offensive security depth in challenge design.

Volunteer — PCCOE Job Fair 2026
Allocated by Training & Placement Cell as Company Point of Contact for International Automotive Components — managed full-day operations at an event with 200+ companies and 15,000+ students (Apr 2026).

CTF COMPETITIONS

1st Place — IU Hack2Xploit 3.0 Indira University × Defcon Pune Chapter | Apr 2026

- 12-hour individual competition (600+ participants) — Web Exploitation, Forensics & Steganography, Reverse Engineering, Cryptography, AI/ML Security, OSINT. Ranked **1st place solo**, no team.

Other Competitions: ISEA ISAP CTF 2026 (IIT Madras) | SYNAPSE 2025 CTF (24-hour offline) | H7CTF 2025 (EC-Council sponsored) | Chaitanya CTF 2025 | ZERODAY CTF | Digital CyberHunt CTF | *and many more.*

PROJECTS

CipherX Pro

- AI-powered universal decoder and cipher analysis tool addressing CTF and incident response use cases for multi-layer encoded payloads (Base64, Hex, XOR, ROT variants). Supports 73+ decoding operations with recursive detection, 8 parallel decoders, LRU caching, and sub-10ms latency via FastAPI and asyncio.
- **Threat Model:** Attacker-encoded C2 communication and obfuscated payloads in network forensics and malware analysis scenarios. Stack: Python, FastAPI.

PCAP-StoryTeller

- Network forensics tool transforming raw PCAP files into interactive attack storyboards — automated threat detection, attack graph visualization, geolocation mapping of threat actors, and forensic report generation for incident response.
- **Security Use Case:** Rapid IOC extraction and lateral movement reconstruction from packet captures. Stack: Python.

Banking-Security-Platform

- Enterprise-grade banking security simulation implementing MFA, real-time fraud detection, transaction anomaly monitoring, and security event alerting — demonstrates threat modelling for credential stuffing and session hijacking attack surfaces. Stack: Python.

Packet-Scope

- Real-time network packet analyzer with deep payload inspection, protocol statistics, geolocation mapping of source IPs, and malicious IP alerting — supports network intrusion detection and IOC identification in live traffic. Stack: Python.

GitHub links available on request.

TECHNICAL SKILLS

Offensive Security: Penetration Testing, Web Application Vulnerability Assessment, SQL Injection, XSS, IDOR, SSRF, XXE, SSTI, Authentication Bypass, Privilege Escalation, Lateral Movement, Persistence Mechanisms, Red Teaming, OSINT, Bug Bounty Research
Defensive & Forensics: Network Forensics, Memory Forensics, IOC Analysis, Incident Containment, Threat Actor Profiling, SIEM, SOAR, SOC Operations, Security Advisory Report Writing, Digital Forensics
Security Tools: Metasploit, Burp Suite, Wireshark, Nmap, Kali Linux, Sliver C2, Packet Tracer, SET (Social Engineering Toolkit), Microsoft Defender
Cloud & Zero Trust: Microsoft Azure Security, AWS Security, Zscaler Zero Trust Exchange, Oracle Cloud Infrastructure
Programming: Python, JavaScript, Bash, SQL, HTML, CSS, React.js
Frameworks: OWASP Top 10, MITRE ATT&CK, NIST CSF, CVSSv3, CTF Challenge Design (Web, Crypto, PWN, Forensics, OSINT)

CERTIFICATIONS

Primary Certifications:

- Certified Ethical Hacker (CEH) v12 — Coursera/Packt (Jun 2025)
- CompTIA Security+ (SY0-701) — Coursera (Sep 2025)
- CompTIA PenTest+ (PT0-002) — Coursera (Sep 2025)
- CISSP Specialization — Infosec/Coursera (Feb 2026)
- Certified Red Team Operations Management (CRTOM) — Red Team Leaders (Dec 2025)

Additional Certifications: Google Cybersecurity Professional (Sep 2025) | Microsoft Cybersecurity Analyst (Sep 2025) | Microsoft Azure Security Tools Specialization (Oct 2025) | Certified Ransomware Protection Officer – CRPO, 98% (Dec 2025) | Palo Alto Networks Security Operations Fundamentals (Aug 2025) | *and many more on LinkedIn.*

ADVANCED TRAINING & WORKSHOPS

HackHunt 2025 Bug Bounty Bootcamp | IntelVan 2025 OSINT Masterclass | Weaponizing Sliver C2 Webinar | Threat Evasion & Offensive Tooling Masterclass | Foundations of Threat Hunting (Picus Security) | *and many more.*