Ahmed Ramadan

Cyber Security Engineer | Penetration Tester | OSCP+ | CREST CRT | CREST CPSA

ahmedramadan.ar16148@gmail.com +201554554167 Cairo, Egypt

linkedin.com/in/ahmed-ramadan-9380a1383 medium.com/@ahmedramadan.ar16148

hackerone.com/rmdnnn

Summary

OSCP+, CREST CRT, and CREST CPSA certified Cyber Security Engineer with **4+ years of experience** conducting full-scope security assessments across **web applications, REST and GraphQL APIs, mobile applications, external networks, Infrastructure and Active Directory environments**. Skilled in manual penetration testing, secure source code review, OWASP Top 10 exploitation, API security testing, vulnerability assessment, authentication and access control testing, privilege escalation, lateral movement analysis, and proof-of-concept development.

Experienced with Burp Suite, Nmap, Nessus, Metasploit, Python, Bash, and security automation to identify, validate, and prioritize vulnerabilities. Active bug bounty hunter and vulnerability researcher credited with **CVE-2026-44977** and multiple Security Hall of Fame acknowledgements, including Mercury, ActBlue, and Groq. Strong ability to write clear technical reports and provide actionable remediation guidance to engineering teams.

Certifications

OffSec Certified Professional Plus (OSCP+) — OffSec
Credential ID: OS-57216833

CREST Registered Tester (CRT) — CREST
Credential ID: 7657380034

CREST Practitioner Security Analyst (CPSA) — CREST
Credential ID: 7657380034

EXPERIENCE

Offensive Security Engineer | Penetration Tester, *DeepStrike.io* 12/2023 – Present
Remote

- Deliver full-scope penetration tests across web applications, REST and GraphQL APIs, mobile, external networks, and Active Directory, surfacing critical IDOR/BOLA, injection, authentication bypass, and broken access control findings.
- Lead internal network and Active Directory assessments, mapping attack paths from initial foothold to domain compromise through privilege escalation, credential abuse, and lateral movement.
- Build custom tooling and automation for vulnerability discovery, exploit validation, and CVE monitoring, reducing manual effort across repeat engagement workflows.
- Produce client-facing reports translating technical findings into business impact, risk ratings, and actionable remediation guidance.
- Partner with development and engineering teams to reproduce exploits, validate fixes, and drive findings to closure.

Offensive Security Engineer, *BugSwagger.com* 04/2023 – 10/2023
Remote

- Conducted penetration tests for web applications, APIs, and thick-client applications using manual testing techniques and security assessment tools.
- Tested critical external-facing assets for vulnerabilities including access control flaws, injection issues, authentication weaknesses, and insecure configurations.
- Documented findings with clear proof-of-concept evidence, impact analysis, and practical remediation recommendations.

Bug Bounty Hunter | Freelance Vulnerability Researcher, *HackerOne* 11/2022 – Present
Remote

- Researched and reported OWASP Top 10 vulnerabilities across public bug bounty programs, including XSS, IDOR/BOLA, authentication flaws, access control issues, and business logic vulnerabilities.
- Recognized for vulnerability research through CVE-2026-44977 and multiple Security Hall of Fame acknowledgements.

SKILLS

Web Application Penetration Testing

Mobile Application Security Testing — Android, Dynamic Testing

Network Penetration Testing

Social Engineering & Phishing Simulations

AI / LLM Security

API Security Testing

Active Directory Penetration Testing

Agentic AI Development for Offensive Security

Secure Source Code Review

Cloud Security Assessment - AWS

CVEs

CVE-2026-44977, *Stored XSS in feedback upload leading to Account Takeover*

Projects

NAC-hunter - Autonomous Offensive Security Agent,
Personal project · Python, LLM orchestration, offensive automation

- Architected an autonomous penetration testing agent pairing a deterministic execution engine with LLM decision making for reproducible, adaptive workflows.
- Engineered safety controls for scope enforcement, destructive-action prevention, and credential handling, the primary operational risks in autonomous tooling.

TOOLS & TECHNOLOGIES

Burp Suite, OWASP ZAP, Nmap, Nessus, Acunetix, Metasploit, BloodHound, NetExec, Evil-WinRM, Evilginx2, GoPhish, Pacu,Python, Bash

Education

Bachelor of Dentistry, *Misr University for Science & Technology*

Languages

Arabic
Native

English
Professional Working Proficiency