Mohamed Ahmed Tarek Abbas

Web&Network Penetration Tester

mohamedahmedtarek0@gmail.com
01279163428
6th of October, Giza, EG
linkedin.com/in/mohamed-ahmed-tarek-bb2b03293
https://m-2004-lap.github.io/Mohamed-Ahmed-Tarek/

Summary

Junior Penetration Tester and Application Security enthusiast with hands-on experience in web application penetration testing, vulnerability assessment, and code review. Skilled in identifying and exploiting vulnerabilities including SQL Injection, XSS, CSRF, SSRF, and XXE. Proficient with industry-standard security tools: Burp Suite, Nmap, Metasploit, and Wireshark. Familiar with SAST and DAST concepts, threat modeling methodologies (STRIDE), and security standards including OWASP. Experienced in writing structured penetration testing and vulnerability assessment reports with CVSS risk ratings and actionable remediation recommendations. Seeking an application security and penetration testing internship to apply skills in real-world security engagements.

Work

CyberSecurity student

Jul 2026 – Present

Information Technology Institute (ITI)

Participating in a comprehensive Cyber Security training program at the Information Technology Institute (ITI), covering core offensive and defensive security domains. Conducting penetration testing exercises on web applications and network infrastructures within a structured, hands-on curriculum. Performing vulnerability assessments and exploitation analysis using tools such as Burp Suite, Nmap, and Metasploit. Applying knowledge from real-world CVE case studies and CTF machines to strengthen practical exploitation and enumeration skills. Documenting findings and technical write-ups to reinforce report-writing and professional communication in security assessments. Collaborating with fellow trainees on labs and simulated environments to build red-team and offensive security proficiency.

Intern Cybersecurity Engineer – Vulnerability Analyst & Penetration Tester

Nov 2025 – Jul 2026

DEPI (Digital Egypt Pioneers Initiative)

Performed web application penetration testing and application security assessments targeting OWASP Top 10 vulnerabilities: SQL Injection, XSS, CSRF, SSRF, and XXE. Conducted vulnerability scanning and network security assessments using Nmap for host discovery, port scanning, and service enumeration; exploited findings using Metasploit Framework. Performed source code review on the Hackazon vulnerable web application to identify SSRF vulnerabilities, analyzing insecure code patterns and producing secure coding recommendations. Executed a full black-box penetration test on TryHackMe VulnNet: reconnaissance, LFI exploitation, PHP reverse shell deployment, credential cracking (John the Ripper), and privilege escalation via tar wildcard injection. Participated in threat modeling exercises to identify potential attack vectors across systems and applications using structured security assessment methodologies. Delivered structured penetration testing and vulnerability assessment reports with CVSS risk ratings, proof-of- concept evidence, and step-by-step remediation guidance aligned with NIST and OWASP standards.

Intern Cybersecurity Engineer

Jul 2025 – Nov 2025

CIB Egypt (Commercial International Bank)

Participated in security awareness initiatives and learned incident response workflows in a banking environment governed by strict cybersecurity policies.

Student Cybersecurity Engineer

Aug 2025 – Sep 2025

Sprints x Microsoft Summer Camp – Cybersecurity

Completed an intensive cybersecurity training covering web application security, network security, ethical hacking.

Education

Alexandria National University

2023

Computer Science & Information Security | B.Sc.

Languages

Arabic (Native), English

Skills

Penetration Testing & AppSec
Penetration Testing, Application Security, Vulnerability Assessment

Programming & Code Review
Code Review, Python, scripting & automation, Bash scripting, JavaScript, source code review, Java, reading level, C++

Vulnerability Classes
SQL Injection, XSS, CSRF, SSRF, XXE, IDOR, LFI/RFI, Broken Authentication, Command Injection, OWASP Top 10

Security Tools
Burp Suite, Proxy, Repeater, Intruder, Scanner, Nmap, Metasploit Framework, Wireshark, Gobuster, Nikto, Dirb,

John the Ripper, Netcat

Network & Infrastructure Security
TCP/IP, DNS, HTTP/HTTPS, Firewalls, IDS/IPS, Encryption Technologies, Network Enumeration, Service Fingerprinting

Secure Development
Secure SDLC, Secure Coding Practices, Input Validation, Authentication Security

Reporting
Penetration Testing Reports, Vulnerability Assessment Reports, CVSS Risk Ratings, Remediation Documentation,

Executive Summaries

Threat Identification
Threat Identification, Risk Assessment, CVSS Scoring

Web Application Pentesting
Black-Box Testing, Exploit Development, Privilege Escalation, SAST, DAST

Projects

Present

Secure Software Development – Application Security Assessment

Conducted a structured application security assessment and code review of a web application, identifying security flaws in authentication, input validation, session management, and secure coding practices. Applied SAST concepts to review source code for vulnerabilities and produced developer-facing remediation documentation aligned with secure SDLC practices.

Present

OWASP Juice Shop – Web Application Penetration Testing

Exploited OWASP Top 10 vulnerabilities including SQL Injection, XSS, IDOR, CSRF, and Broken Authentication; applied DAST techniques using Burp Suite (Proxy, Repeater, Intruder). Documented all findings with reproduction steps, severity ratings, and remediation recommendations