Mahmoud Mohamed Elshorbagy

Security Engineer

Cairo, Egypt | +20 155 668 8657 | mahmoud.elshorbagy0x1@gmail.com
LinkedIn | github.com/Falcon0x1 | elshorbagy.netlify.app | falcon0x1.github.io
Military Service: Completed

Professional Summary

Security Engineer with a B.Sc. in Systems & Computer Engineering and specialized in Web & Android Penetration Testing, with a strong focus on Bash automation and secure API architecture. Focused on Web, API, Mobile (Android), and IoT / Embedded Systems security, with practical experience in manual vulnerability discovery, exploitation, and reporting. Strong foundation in Linux, scripting, and system architecture, applying an attacker-mindset approach to identify real-world security risks. Actively engaged in security research, automation, and technical documentation.

Hands-on experience with structured penetration testing methodologies, emphasizing business-impact assessment and clear remediation guidance. Continuously developing technical depth through labs, security tooling, and real-world attack surface analysis.

Core Capabilities

- Web Application Penetration Testing (OWASP Top 10)
- API Security Testing (REST, Authentication, Authorization, Business Logic Flaws)
- Mobile Application Security (Android)
- Network & Authentication Security Fundamentals
- Manual Exploitation & Attack Chaining
- Vulnerability Assessment & Technical Reporting
- Linux & Bash Automation
- Security Research & Technical Documentation

Certifications

eLearnSecurity (INE)

- eWAPT — Web Application Penetration Tester · Verify Certificate

CyberTalents / ITI

- Certified Web Application Penetration Tester · Verify Certificate
- Certified Mobile Penetration Tester · Verify Certificate
- Certified Active Directory Penetration Tester · Verify Certificate

APIsec University

- API Penetration Testing · View Credential

Relevant Experience

Trainee — Offensive Security & Penetration Testing Track
Information Technology Institute (ITI), Nasr City, Cairo
07/2025 – 11/2025

- Conducted comprehensive Black-Box and Grey-Box penetration testing on 15+ lab targets mimicking real-world banking and e-commerce applications.
- Performed manual and automated penetration testing against OWASP Top 10 vulnerabilities
- Conducted web, API, and Active Directory attacks in controlled lab environments
- Applied industry-standard methodologies such as PTES and OSSTMM during security assessments
- Gained hands-on experience with Bash scripting and Red Hat Linux administration

Technical Skills

Web & API Security

- Burp Suite, OWASP ZAP, sqlmap, Postman, curl, JWT analysis, business logic testing

Mobile Application Security (Android)

- Frida, JADX, MobSF, objection, apktool, adb, static analysis, dynamic analysis

Network & Systems Security

- Nmap, Metasploit, Wireshark, authentication attacks, misconfiguration analysis, embedded systems fundamentals, secure API communication, system architecture

Languages & Systems

- Python, Bash, C/C++, JavaScript, SQL, Git, Linux (Arch, Kali, Red Hat), Windows

Security Research & Tooling

FalconRecon — Automated reconnaissance framework for early-stage attack surface mapping and target enumeration — GitHub Repository

- Bash-based automation tool integrating multiple scanners to streamline reconnaissance and target enumeration.

Technical Research & Writeups — Security-focused articles and walkthroughs — Medium Writeups

- Authored practical content on web, API, and mobile exploitation with emphasis on real-world attack vectors and mitigation.

Labs & CTF Platforms

PortSwigger Web Security Academy, TryHackMe, Hack The Box, CyberTalents

Education

Bachelor of Systems & Computer Engineering

Faculty of Engineering, Al-Azhar University — Cairo, Egypt

September 2019 – July 2024

- **Cumulative Grade:** Very Good
- **Graduation Project:** IoT / ICS Automation System — Security & Development (Smart Poultry Farm Automation System) — **Grade:** Excellent
- Designed a localized IoT-based control system integrating sensors, controllers, and a mobile interface
- Implemented remote access and API-based communication between embedded hardware and a mobile application
- Addressed security considerations related to unauthorized control, API exposure, and system integrity

Training & Courses

- Android Application Penetration Testing (Hextree)
- Red Hat Linux Administration I & II
- Bash Scripting
- MCSA
- CCNA

Professional Development

- **Communication, Business Etiquette, Interview Skills** – Almentor – Ministry of Youth & Sports

Languages

- Arabic — Native
- English — Professional Working Proficiency