Mahmoud Ouf

Application Security & Offensive Security Engineer

Application Security · Offensive Security Engineering · B.Sc. Software Engineering

Contact

Email: contact@mahmoudouf.com ↗

Location: Based in Egypt (UTC+2)

Availability: Open to Remote & Global Relocation
Visa Sponsorship / B2B Contract

Portfolio: mahmoudouf.com ↗

LinkedIn: linkedin.com/in/mahmoudadel0x01 ↗

GitHub: github.com/mahmoud0x01 ↗

Telegram: t.me/rdmsr ↗

Date of Birth: 22/09/2002

Profile

Cybersecurity engineer specializing in application security and offensive security — ranked in the top 0.55% of Hack The Box's global leaderboard, with 20+ Bugcrowd Hall of Fame acknowledgments (Verisign, DigitalOcean, Pinterest, Dell) for vulnerabilities found and fixed in production. Peers nicknamed me "Kernel" for a systems-level curiosity that goes past the surface — the same approach behind a CNSP certification (with Merit) and hands-on penetration-testing and SOC-fundamentals work across both offense and defense.

Experience

Software Engineer Intern Feb 2025 – June 2026

National Research Tomsk State University ↗

- Delivered **2 MVPs + 12 diagrams** (UML/SDLC) — builds system reasoning for reproducible findings.

Security Engineering Intern July 10 – September 10, 2024

Bastion Security ↗ — Security Engineering Internship

- Completed Penetration Testing & Application Security internship track — company-led lectures, CTF challenges, vulnerability-exploitation lab work.
- Conducted a research project analyzing web application cache-attack techniques.
- Ranked **Top 5 of 100** in internal penetration-testing and privilege-escalation challenges.

View Credential ↗ ↗ · Bastion Security internship certificate

Education

B.Sc. Software Engineering — Conferred Jul 2026
Tomsk State University
Sep 2022 – Jul 2026

Security Recognition & Evidence

- **Bug Bounty Hall of Fame — 20+ acknowledgments** via Bugcrowd (bugcrowd.com/h/mahmoud_adel ↗) — Named: Verisign $1,000 CSRF→Account Takeover (DomainScope OAuth state, Apr 2018), DigitalOcean (Apr 2019), Pinterest & Dell (2018). **Critical**
- **Competitive & labs:** Bastion internal CTF **Top 5/100**; Hack The Box **Top 0.55% Pro Hacker** — verified badges ↗; TryHackMe **Top 1%** — @iamkernel ↗. **Verified**
- **Detection & research:** ELK SOC Home Lab — 50k+ events, 5 Sigma MITRE-mapped, Kibana dashboards & triage workflow; IR malware triage (isolated Windows 10 VM, Sysmon/KAPE); AppArmor RCE mitigation; API security & AD attack paths. **Lab**

Practical Labs & CTF Platforms

- Hack The Box — Verified Badges · Top 0.55% Pro Hacker ↗
- TryHackMe — @iamkernel · Top 1% ↗

Credentials & Training

- **Certified Network Security Practitioner (CNSP)** — The SecOps Group · 2026 · with Merit · ID 11896945 · Verify ↗ ↗
- **Blue Team Junior Analyst** — SecurityBlue Team · 2023 · Verify ↗ ↗
- **Cyber Threat Intelligence** — IBM · 2023 · Verify badge ↗ ↗
- **Jr Penetration Tester** — TryHackMe · 2024 · Verify PDF ↗ ↗

Core Skills

CORE

Web/API Security, Vulnerability Assessment, Linux, Windows, TCP/IP, Privilege Escalation (lab), Burp Suite, Nmap, Python, Bash

APPLIED

OWASP, Network Security, Active Directory, Kerberos, Wireshark, BloodHound, Impacket, Docker, System Administration, Firewall, SIEM (ELK), Incident Response, MITRE ATT&CK, Cloud Security (AWS IAM)

FAMILIAR

Ghidra (lab), Metasploit (lab), Cobalt Strike (exposure), Sliver (lab), Nuclei (lab), SQLMap (lab), ffuf (lab), Malware Analysis (lab), Threat Intel (exposure), Exploit Dev (lab), Red Team (lab), YARA (lab), Sigma (lab), Suricata (lab), Splunk (lab)

ENGINEERING

JavaScript, C/C++, Assembly, SQL, Git, Presentation, Problem Solving

Languages

Arabic · Native

English · C2 Proficient

Russian · C1 Advanced

Security Research

- **Verisign CSRF → Account Takeover** — Missing OAuth state → Google-link hijack → persistent ATO + password set ($1,000 reward, Bug Bounty HoF Apr 2018). Write-up ↗ ↗
- **AppArmor RCE Killswitch** — Deny /bin/** + network → audit DENIED exec /bin/sh → allowlist containment + hardening. Write-up ↗ ↗
- **ELK SOC Detection Engineering** — 50k+ events, 5 Sigma MITRE-mapped rules, Kibana dashboards & triage workflow. Write-up ↗ ↗

Portfolio: mahmoudouf.com ↗ · All security testing described was performed in authorized, lab, or responsible-disclosure contexts. · References & assessment logs available upon request.