Adham Elhansye

Penetration Tester | Cybersecurity Engineer

Beni-Suef, Egypt | adhamelhansye@gmail.com | Linkedin | Github | Blog/Portfolio | +20 1140495914

PROFESSIONAL SUMMARY

Certified Penetration Tester and Cyber Security Engineer specializing in Web, Mobile, Network and API security with On-hands experience on Burp Suite, Nmap, Metasploit, Kali Linux and developing exploits using python. HOF in Nokia, IBM (Also reported DDR), Adobe, Nintendo and Microsoft for vulnerabilities with additional reports in LaunchDarkly, Anywhere Real State and HeroIC; Submitted +110 vulnerabilities on HackerOne – Top #87 Egypt (Q1 2025). Excited to progress towards Red Team ops and Blue Team defense, mastering Active Directory pentesting, post-exploitation methods and threat hunting for stronger cyber resilience.

PROFESSIONAL EXPERIENCE

Bug Bounty Specialist **2024 – Present**

HackerOne — Remote

- Conducted manual and automated penetration testing on web applications, APIs, and network infrastructure, identifying 110+ vulnerabilities aligned with OWASP Top 10 and MITRE ATT&CK.
- Reported critical flaws, including Remote Code Execution (RCE) in AT&T systems, earning Hall of Fame inclusions (Microsoft, Adobe, Nokia, Nintendo) and #1 in IBM Top Hackers 2025.
- Delivered technical vulnerability reports with Python/Bash PoC scripts for rapid remediation by engineering teams.

Cybersecurity Content Creator & Platform Lead **2021 – Present**

Hidden Lock — Remote

- Published 50+ articles/tutorials on penetration testing, exploit development, and secure coding, attracting 200K+ monthly visitors.
- Launched the first Arabic cybersecurity education platform, promoting ethical hacking, bug bounty programs, and tools (Burp Suite, Nmap, Metasploit).
- Boosted audience retention by 25% through engagement analytics, strengthening regional credibility in the MENA cybersecurity community.

Cybersecurity Virtual Experience Participant **2021 – 2022**

Mastercard (via Forage) — Remote

- Conducted simulated phishing assessments and risk evaluations.
- Developed security awareness training to counter social engineering and common cyber threats.
- Applied network security fundamentals and vulnerability scanning in a virtual lab to improve enterprise resilience.

EDUCATION

Bachelor of Computer Science – Cybersecurity Track **Expected Graduation: 2027**

- Beni-Suef National University, Egypt

PROJECTS

CVE-2000-0114 Exploit

GitHub | CVE Details | cve.imfht.com

- Python-based PoC for anonymous account disclosure in Microsoft FrontPage Server Extensions via /_vti_bin/shtml.dll.
- Published as an educational exploit on multiple CVE platforms.

CVE-2025-0133 Research & Disclosure
GitHub

- Discovered and responsibly disclosed a new vulnerability via a VDP, resulting in official CVE assignment.
- Provided technical analysis and remediation guidance.

VM Detection Evasion Techniques
GitHub

- Researched and implemented anti-VM techniques to understand malware evasion.
- Supports malware analysis and red teaming.

The Science of Human Hacking
GitHub

- Toolkit on social engineering, phishing simulation, and human-layer attacks.
- Includes templates and defensive strategies for security awareness training.

C2-GitHub Framework
GitHub

- Lightweight Command and Control (C2) simulator using GitHub for covert communication.
- Used for red team training and detection engineering.

Hidden Lock – Arabic Cybersecurity Platform

- Launched the first Arabic cybersecurity education platform with 50+ articles on penetration testing, exploits, and secure coding.
- Reaches 200,000+ monthly visitors; features tutorials on Burp Suite, Nmap, and Metasploit.

CERTIFICATIONS & TRAINING

- eJPT v1 & v2 – Netraiders Academy (Certified)
- CEH v11 & v12 – EC-Council
- CompTIA Security+ (SY0-401, SY0-601)
- CompTIA Network+
- CompTIA Linux+
- CCNA 200-301 – Cisco
- eWPTX v2 & eWPT v2
- API Penetration Testing – APISec (Certified)
- OWASP Top 10 (Web) 2021 – MaharaTech
- OSINT Fundamentals – MaharaTech
- eCPPT v1 & v2 & v3 (In Progress)
- Implementation of Computer Network Fundamentals – MaharaTech
- C3SA: Cybersecurity Analyst – CyberWarFare (Certified)
- Mastercard Cybersecurity Virtual Experience – Forage (Certified)

ACHIEVEMENTS

- Secured 1st Place in IBM Top Hackers 2025
  - Identified 13 vulnerabilities in IBM systems, earning top ranking on HackerOne.
- Identified Critical Vulnerability in AT&T
  - Uncovered a major security flaw in AT&T, preventing potential system compromise.
- Inducted into Nintendo Hall of Fame 2025
  - Detected a critical vulnerability in Nintendo’s platform, strengthening application security.
- Discovered 4 Vulnerabilities in NASA Systems
  - Identified security flaws in NASA infrastructure, supporting mission-critical cybersecurity.
- Reported Over 110 Vulnerabilities on HackerOne (Q1 2025)
  - Submitted 110+ reports (20 accepted), ranking #87 in Egypt.

- Inducted into Microsoft Hall of Fame Q1 2025
  - Discovered 6 vulnerabilities in Microsoft infrastructure, earning 2000 points.
- Discovered 4 Vulnerabilities in Stanford University Systems
  - Detected bugs in Stanford's digital infrastructure, improving academic system security.
- Inducted into Adobe Hall of Fame 2025
  - Reported 4 vulnerabilities in Adobe Systems, enhancing content management security.
- Inducted into Nokia Hall of Fame 2025
  - Uncovered 10 vulnerabilities in Nokia systems, improving web application security.

SKILLS

Technical Skills

- Penetration Testing (Web, Network, Mobile, API)
- Vulnerability Assessment & Scanning
- Exploitation & Post-Exploitation
- Web Application Security (OWASP Top 10)
- API Security Testing (REST/SOAP)
- Red Teaming & Bug Bounty
- Ethical Hacking
- Secure Code Review
- Security Frameworks: MITRE ATT&CK, OWASP
- Security Tools: Burp Suite, Nmap, Metasploit, Wireshark, Kali Linux
- Scripting & Automation: Python, Bash, JavaScript
- Mobile & Network Security
- Technical Report Writing
- Self-Directed Tool Mastery

Soft Skills

- Analytical Thinking
- Problem Solving
- Attention to Detail
- Communication & Technical Documentation
- Team Collaboration
- Self-Learning & Adaptability
- Ethical Conduct & Time Management

BOOKS

- Hacking: The Art of Exploitation, 2nd Edition – Jon Erickson
- The Bug Bounty Playbook: A Practical Guide to Finding and Reporting Vulnerabilities
- Bug Bounty Bootcamp: Hands-On Training to Become a Bug Bounty Hunter – Mitch E. W.
- RTFM: Red Team Field Manual – Ben Clark
- The Bug Bounty Handbook: A Guide to Understanding Bug Bounty Programs – A. K.
- Next Generation Red Teaming – Henry Dalziel
- Windows Internals, Part 1 (7th Edition) – Mark Russinovich, David Solomon, Alex Ionescu
- The Shellcoder's Handbook: Discovering and Exploiting Security Holes – Chris Anley, John Heasman, Felix Lindner, Gerardo Richarte
- Game Hacking: Developing Autonomous Bots for Online Games – Daniel Goldberg, Dylan Petruzzelli

LANGUAGES

- **Arabic:** Native
- **English:** Working Proficiency