



# Mohamed El-Gendy Junior Penetration Tester

✉ mohamedelgende150@gmail.com    ☎ +20 112 253 8851     [linkedin.com/in/mohamed-elgendy](https://www.linkedin.com/in/mohamed-elgendy)  
 [github.com/ElgendyMan](https://github.com/ElgendyMan)

## Profile Summary

---

A proactive Junior Penetration Tester, combining a BSc in Information Technology with intensive NTI training. Demonstrated practical expertise by identifying and documenting over 20 vulnerabilities (including authentication bypass) in a major academic project. Proficient in Web, Network, and API testing, backed by dedicated API security training and hands-on lab practice, with a strategic focus on developing future capabilities in Red Teaming and OT Security.

## Education

---

05/2022 – 06/2025 Elmnoufia, Egypt	<b>Delta Technological University</b> BSc in Information Technology, Network Specialization   GPA: 3.7 <ul style="list-style-type: none"><li>• <b>Relevant Courses:</b> Network Security, Operating Systems, Database Systems, Web Technologies, Programming, IoT Security, SecOps, Encryption Algorithms</li></ul>
10/2025 – 01/2026 Smart Village	<b>National Telecommunication Institute (NTI)</b> RedTeaming - HireReady Program (4-Month Diploma) A comprehensive, hands-on program covering the full spectrum of offensive and defensive security. <b>Core Modules:</b> Web Penetration Testing, Network Penetration Testing, MITRE ATT&CK, Mobile Security (Android), Python for Pentesters.

## Hands-On Experience & Projects

---

01/2025 – 05/2025 Remote	<b>Web Application Pentester,</b> Integrated Academic Service System (IASS) Delta Technological University <ul style="list-style-type: none"><li>• Identified and documented over 20 vulnerabilities, including High-risk Broken Authentication, leading to a project grade of A+.</li><li>• Performed manual business logic testing using Burp Suite to discover an authentication bypass flaw, gaining unauthorized access to administrative functions.</li><li>• Developed a Proof-of-Concept (PoC) Python script to automate the exploitation of a rate-limiting vulnerability in a RESTful JSON-based API, enabling large-scale unauthorized requests.</li><li>• Authored a professional 35-page penetration test report detailing findings, CVSS 3.1 risk ratings, and actionable remediation guidance for the development team.</li><li>• <a href="#">MohamedEl-Gendy-IASS-Report</a></li></ul> <b>Additional Penetration testing Practice</b> <ul style="list-style-type: none"><li>• Regularly solve PortSwigger Web Security Academy labs, publishing detailed exploitation writeups on GitHub (<a href="https://github.com/ElgendyMan/portswigger-writeups">github.com/ElgendyMan/portswigger-writeups</a>). Completed 40%+ of all labs (ongoing).</li><li>• Solve labs in HackTheBox platform</li></ul>
-----------------------------	---

## Certifications & Training

---

**API Penetration Testing**  
APIsecurity .io

**NovaDev Company**  
Penetration Testing training

**Sprints x Microsoft**  
(40hrs)

**Cyber Security (Information  
Technological Institute)**

**Innovative Leadership and  
Strategic Thinking (Vital)**

**Network Essentials (CISCO)**

## Coursework

---

**Security+**  
Completed

**Linux+**  
Completed

**eJPTv2**  
Completed

**eWAPTv2**  
Completed

**eCCPTv2**  
In Progress

**Red Teaming Diploma  
(Udemy)**  
In Progress

## Skills

---

### Methodologies & Standards

OWASP Top 10, PTES, Information Gathering (Passive/Active), Vulnerability Analysis, Exposure to post-exploitation, privilege escalation, and lateral movement concepts through labs and training.

### Tools & Platforms

Burp Suite, Zaproxy, Nessus, Acunetix, Nmap, Masscan, Metasploit, John the Ripper, Hashcat, Google Dorking, Xmind, Notion, VPS Management.

### Web/Network Security

SQL Injection (SQLi, SQLmap), Cross-Site Scripting (XSS), IDOR, Broken Access Control, Logic Vulnerabilities, Subdomain Takeover, Protocol Hacking (FTP, SMB, SMTP, DHCP), Man-in-the-Middle Attack (MiTM).

### Programming & Scripting

Python (for Automation, Exploit Development), PHP (for cybersecurity purposes), SQL (Database querying and injection testing), Bash Scripting (System administration and network scanning), C++, C, Java (OOP), JavaScript (for client-side security testing)

### Soft Skills

Teamwork & Collaboration, Communication Skills, Good Explanation Skills, Analytical Problem-solving, Continuous Learning, Leadership mentality, Project Management

## Language

---

**English**  
B2

**Arabic**  
Native