

Youssef Mohamed

Offensive Security

01107012987 - 01008020997 | Egypt | ymh796d68@gmail.com

LinkedIn- [Youssef Mohamed](#)

Github - [Houdini-Y](#)

About Me

High-achieving Computer Science Undergraduate specializing in Offensive Security. Proactive researcher with proven practical experience in web application security, successfully identifying paid vulnerabilities in live bug bounty programs. Demonstrates strong technical proficiency through the completion of 80+ advanced labs in PortSwigger Web Security Academy and the development of custom security automation tools in Python. Eager to leverage skills in vulnerability assessment and manual exploitation in a professional security role.

EDUCATION

Bachelor of Computer Science

Expected Graduation: 2027

- Minya National University, 3.6 GPA

WORK EXPERIENCE

Programming Language Coach

New Vision Academy
Minya, Egypt

June/2023 - October/2024

Educational institution focused on programming and technology training

- Delivered over 50 hours of instruction in Python and C++ programming fundamentals to diverse groups of students.
- Guided over 10 students through course completion, ensuring foundational understanding of complex programming concepts.
- Developed and organized programming competitions for students under 18, utilizing technical communication skills to simplify complex concepts and drive engagement.

Offensive Security Experience

Bug Bounty (HackerOne / Bugcrowd / Private Programs)

- Secured a monetary bounty for identifying a critical **Session Management/Logic Flaw** that allowed complete account life-cycle bypass and subsequent account takeover via concurrent active sessions after the deletion process was initiated.

- Conducted vulnerability research on public and private programs, resulting in **one paid finding and two valid duplicate reports**.
- Execute a hybrid testing methodology combining automated reconnaissance (using httpx, nuclei, and custom Python scripts) with deep-dive manual exploitation.
- **Key Areas of Focus:** Business Logic Errors, Authentication Flaws, Access Control Violations (IDOR), and Complex Session Management.

PortSwigger Web Security Academy – 80+ Labs Completed

SQL Injection, Authentication flaws, CSRF, Logic Bugs, SSTI, JWT attacks, Session management, Access-Control vulnerabilities.

OverTheWire CTFs

- **Bandit:** Linux file system attacks, environment abuse, privilege escalation primitives
- **Natas:** authentication bypass, file inclusion, command injection, web exploitation

Reverse Engineering

- Completed **Assembly 1001**
- Practicing malware analysis basics: disassembly, registers, stack operations

Security Projects

Linux Process Monitor (ncurses-based)

- Developed a real-time system monitor in C++ that parses the core Linux /proc filesystem data and utilizes the ncurses library for a terminal-based user interface, demonstrating low-level systems programming skills.

Python Port Scanner (Multithreaded)

- Custom multithreaded scanner supporting user-defined port ranges, banner grabbing, and DNS resolution.

Steganography Tool (Python)

LSB encoder/decoder with built-in compression and benchmarking features.

Core Offensive Security Skills

Web Hacking: SQLi, SSTI, CSRF, JWT cracking, Access Control bypass, Rate-limiting bypass

Tools: Burp Suite, ffuf, gobuster, nmap, Wireshark, httpx, nuclei

Bug Bounty: Recon, endpoint analysis, session attacks, API testing

Reverse Engineering: Assembly x86-64 1001, GDB, objdump

Programming: Python, C++, Bash

Certificates

IBM Cyber Security | Mahara Network Security | Mahara Ethical Hacking | RHCSA Intro
Cloud & Virtualization | ITI Web Fundamental | Cisco Network security (self study)