BUGGY

Cybersecurity Enthusiast — Aspiring RedTeam Operator

buggymaytricks.github.io buggymaytricks@proton.me

About

Offensive security enthusiast with **2+ years** of hands-on lab, CTF, and internship experience. Top **2% on TryHackMe globally**, holder of **HTB CJCA**, and actively pursuing **CPTS** and **CWES**. Focused on web exploitation, Active Directory attacks, and real-world adversary simulation.

Education

Sinhgad Academy of Engineering — **Pune, Maharashtra**
B.E. Computer Engineering — *September 2024 – May 2028*

Experience & Achievements

Cybersecurity Intern — **June 2025 – July 2025**
ENCODERSPRO Private Limited — *Remote*

- Built a cross-platform botnet simulation framework to study C2 communication and malware behavior.
- Analyzed bot-to-C2 traffic via Wireshark to identify indicators of compromise and improve detection signatures.
- Practiced OSINT, SIGINT, and digital forensics methodologies in a structured training environment.

Cybersecurity Intern — **March 2025 – April 2025**
Threat Prism — *Remote*

- Built a recon automation tool covering information gathering, network scanning, and web application enumeration.
- Developed phishing simulation frameworks for evaluating social engineering susceptibility across targets.

Capture The Flag (CTF) & Competitions — **2022 – Present**
TryHackMe, HackTheBox & Various Platforms — *Remote*

- **Top 2% TryHackMe Globally**: 120+ red team labs completed.
- **Hackfinity CTF**: Ranked 229/4,309 in TryHackMe's flagship competition.
- **Rise Get Set Hack**: Ranked 85/22,000+ participants nationwide.
- Active in DamnCon CTF, NahamCon CTF, and international red team competitions.

Featured Projects

ECSIP Botnet Simulation & Analysis | *Python, Flask, Wireshark, VirtualBox* | GitHub — **2025**

- Built a modular botnet in an isolated VirtualBox lab for ethical malware and C2 research.
- Implemented a Flask C2 dashboard for centralized remote task control and real-time bot monitoring.
- Developed cross-platform Python agents (Linux & Windows) with keylogger, DoS, brute-force, and credential stealer modules.
- Analyzed C2 and DDoS traffic patterns via Wireshark to study real-world malware communication behavior.

Active Directory Lab | *Windows Server, PowerShell, BloodHound, Impacket, CrackMapExec* — **2024**

- Built a home AD lab to practice red team attack techniques against a realistic enterprise environment.
- Practiced attack chains including Kerberoasting, Pass-the-Hash, and lateral movement scenarios.
- Mapped attack paths using BloodHound and practiced post-exploitation persistence techniques.

Hash-Verify | *Python, CLI, Cryptography* | GitHub — **2024**

- Open-source file integrity tool supporting MD5, SHA1, SHA256, SHA3-256, SHA512, and SHA3-512.
- Dual-mode CLI: interactive guided mode and command-line mode for scripting; cross-platform under MIT license.

Technical Skills

Offensive Security: Web App Testing, Network Pentesting, Active Directory Attacks, Post-Exploitation, Adversary Simulation
Security Tools: Nmap, Metasploit, Burp Suite, FFUF, BloodHound, Impacket, CrackMapExec, Responder, Nessus, Nikto
OSINT & Recon: Shodan, Recon-ng, theHarvester, Maltego
Programming: Python, Bash, C, C++, Java, SQL
Operating Systems: Linux (Kali, Parrot, Ubuntu, Mint), Windows Server

Certifications

HTB: Certified Junior Cybersecurity Associate (CJCA) **2026**

HTB: Certified Web Exploitation Specialist (CWES) *(Currently Pursuing)* **HackTheBox**

HTB: Certified Penetration Testing Specialist (CPTS) *(In Progress)* **HackTheBox**

TCM Security: Practical Ethical Hacking **2024**

Certified AppSec Practitioner (CAP) **2024**

Community & Red Team Focus

Technical Blog: buggymaytricks.github.io, covering red team techniques, CTF writeups, and lab setups.
Open Source: GitHub contributor focused on red team tooling and offensive security research projects.
Knowledge Sharing: CTF writeups, red team technique breakdowns, and research notes.
Conferences: Engaged at **Seasides**, **APISECON**, and **DEF CON** with the offensive security community.