Samuel Bravo

https://www.linkedin.com/in/sam-bravo-129085233/
https://tryhackme.com/p/slyripz

418 Bohme St
Uvalde, TX 78801
(830)279-3642
CyberSecBravo@gmail.com

Employment History

Freelance Computer Technician

Sept. 2013 - PRESENT

- Installed and performed minor repairs on hardware, software, and peripheral equipment following design or installation specifications.

- Customized commercial programs for internal needs.

- Executed commands and observed system functioning to verify correct operations and detect errors.

- Troubleshoot network connectivity issues.

- Conducted network security testing for clients.

EDUCATION

Western Governors University — *Bachelor of Science in Cyber Security*

Expected Graduation Date: December 2024

Bug Bounty Achievements

Bug Bounty Hunter — *Platforms: Intigriti, Hackerone, YesWeHack and Direct Reports to Companies.*

- Discovered and responsibly reported multiple security vulnerabilities in countless web applications.

- Successfully identified critical vulnerabilities such as Cross Site Scripting, Local File Inclusion and Security misconfigurations .

- Collaborated with development teams to ensure timely remediation of reported vulnerabilities.

EXAMPLE FINDINGS:

1. DOM Based XSS: Discovered and reported a cross-site scripting (XSS) vulnerability in Toyota.com and Target.com resulting in a secure patch.

2. Subdomain Takeover: Identified a Subdomain Takeover on a subsidiary of Nestle.com, leading to a prompt fix and a bounty reward.

3. IDOR: Detected an insecure direct object reference (IDOR) issue in TomorrowLand, contributing to improved security

SKILLS

Operating Systems:
Windows, Linux (Kali), Mac OSX.

Tools and Programs:

Nmap, Burp Suite, Metasploit, Hashcat, Impacket, Bloodhound, Nessus, VMWare, CrackMapExec, XSStrike, nuclei, SQLmap, Amass etc..

Certifications

Practical Network Penetration Tester (PNPT)

LANGUAGES

Python, PHP, Javascript, HTML, Bash, Powershell, C++

Additional Information

-Demonstrate commitment to ethical hacking and cybersecurity by actively participating in TryHackMe challenges and expanding skills.

-Gladly participate in unpaid Bug Bounty programs(VDP) in an attempt to make the internet more secure and safe.

References

Available upon requests.