

RAYAN ALTHOBAITI

TAIF - SAUDI ARABIA, +966599622631, RAYAN.ALTHOBAITI.JOBS@GMAIL.COM, LinkedIn: [RayanAlthobaiti](#)

Cybersecurity Professional

Hands-on experience executing penetration testing on web applications, networks, and computer systems. Expertise in performing advanced exploitation and post-exploitation attacks. Strong knowledge and hands-on experience developing with interpreted or compiled languages: Python, GO, C/C++, PHP, JAVA, Javascript, C#. Experienced in code-review and identify weaknesses. Furthermore, Professional in CTF competitions, CVE research, and Bug Bounty recognition. In addition, well-versed in exploit development, Sandbox (SBX), and Anti-Virus (AV) evasion.

Education

Bachelor of Science: Computer Science, ABET accreditation MAY 2017

Graduated with 3.18/4 GPA | Taif University, Taif, Saudi Arabia

- [Distributed brute-force](#) (Capstone Project).

Research that aims to reduce time complexity, and collecting botnets to perform distribution brute-force.

Experience

Full-stack developer **Clouds seven** Taif, Saudi Arabia MAY 2018 – JAN 2020

- [Maghsalty Customer Service.](#)

- [Maghsalty Point of Sale system.](#)

Back-end built using NodeJS runtime environment (RE), ExpressJS CRUD (Create, Read, Update, Delete) Application Programming Interface (API), MySQL database, and Json Web Token (JWT) authorization middle-ware. Then developed an Application Programming Interface (API) for EPSON TM-P20 hardware. designed, maintained, and implemented the database, simple queries, and complex using joins, grouping, nested sub-queries. Installed, maintained, and configured the system on Linux Virtual Private Server (VPS). After that Front-end built using Angularjs and Syntactically Awesome Style Sheets (SASS).

Cyber Security Engineer **Technology Control Company** Riyadh, Saudi Arabia DEC 2020 – Present

Perform penetration testing on Networks, Web-based applications, and Computer systems. Reviewing source code to discover security weaknesses, bugs, and violations of programming standards.

Certifications

- Professional Accreditation. MAY 2021 – MAY 2024
- HackTheBox's Pro Labs: APTLabs. JAN 2021
- HackTheBox's Pro Labs: Rastalabs. MAY 2020
- HackTheBox's Pro Labs: Cybernetics. MAY 2020
- eLearn Security Web application Penetration Tester (eWPT). JAN 2020
- eLearn Security Certified Penetration Tester eXtreme (eCPTX). NOV 2019
- Offensive Security Certified Professional (OSCP). NOV 2019
- HackTheBox's Pro Labs: Offshore. SEP 2019
- eLearn Security Certified Professional Penetration Testerv2 (eCPPTv2). APR 2019
- Virtual hacking Labs (VHL). NOV 2018
- CCNA Routing and Switching Training JICC. DEC 2016

Projects

- [CVE-2019-10149](#)
CVE-2019-10149 is a remote command execution (RCE) exploit on Exim versions 4.87 to 4.9.
- [Pureftpd-FXPAbuse](#)
FXPAbuse is a tool to abuse Pureftpd FXP EPRT (RFC 2428) to obtain the IPv6 of the target server.
- [MySQL-DSN](#)
Exploit DSN injection using simulated MySQL server.
- [BFCanary](#)
BFCanary is a multiprocessing tool to brute-force x64 canary value, frame pointer, and return address.
- [ZabbixAPIAbuse](#)
ZabbixAPIAbuse is an abusing tool for Zabbix API to execute commands on Zabbix agents.

Activities &

Achievements

- [hacktheboxeu \(Diefunction\)](#)
Placed in the top 10 (#7) of the HOF of hacktheboxeu among 300K+ members, and active for 2+ years.
- [bugbounty.sa \(Rayan Althobaiti\)](#)
Reached to 1800 points, total number of submitted reports 34 between High and Critical vulnerabilities.
- [SYNACK Red Team Researcher \(Rayan Althobaiti\)](#)
SYNACK platform is an elite team of the world's top cybersecurity researchers.