RAYAN ALTHOBAITI

TAIF - SAUDI ARABIA, +966599622631, RAYAN.ALTHOBAITI.JOBS@GMAIL.COM
Blog: https://blog.diefunction.io , Twitter: @Diefunction , Linkedin: RayanAlthobaiti

Cybersecurity Professional

Experienced in web, network, system, and mobile application penetration testing. Proficient in advanced exploitation techniques, post-exploitation activities, and reverse engineering. Skilled in programming languages such as Python, Go, C/C++, PHP, Java, Javascript, and C#. Strong in exploit research, development, and vulnerability identification. Capable of developing and analyzing malware.

Education

Bachelor of Science: Computer Science, ABET accreditation — MAY 2017

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

- Distributed bruteforce Time Complexity Reduction for brute force via botnets

Experience

Full-stack developer — **Clouds Seven** — Taif — MAY 2018 – JAN 2020

Developed a customer service and Point of Sale (POS) system using Node.js, Express.js, MySQL, and JWT. Integrated EPSON TM-P20 hardware API. Managed and implemented the database with complex queries. Configured and maintained the system on a Linux VPS. Utilized AngularJS and SASS for the front end.

Cyber Security Engineer — **Technology Control Company** — Riyadh — DEC 2020 – July 2023

Principle Penetration Testing Consultant — **Technology Control Company** — Riyadh — July 2023 – Present

Perform penetration testing on networks, mobile, web-based applications, and computer systems. Review source code to identify security weaknesses, bugs, and programming standard violations. Conduct exploit research and development for red teaming purposes. Additionally, responsible for building the Capture the Flag (CTF) challenges for the main events.

Certifications

• Offensive Security Exploitation Expert (OSEE).	JAN 2024
• Offensive Security Certified Expert 3 (OSCE3).	NOV 2024
• Offensive Security Exploit Developer (OSED).	JUN 2024
• Offensive Security Web Expert (OSWE).	JAN 2022
• Offensive Security Experienced Penetration Tester (OSEP).	NOV 2024
• Offensive Security Certified Professional (OSCP).	NOV 2019
• eLearn Security Web application Penetration Tester (eWPT).	JAN 2020
• eLearn Security Certified Penetration Tester eXtreme (eCPTX).	NOV 2019
• eLearn Security Certified Professional Penetration Tester v2 (eCPPTv2).	APR 2019
• SCE Professional Accreditation.	MAY 2021 – MAY 2027
• HackTheBox's Pro Labs: APTLabs.	JAN 2021
• HackTheBox's Pro Labs: Rastalabs.	MAY 2020
• HackTheBox's Pro Labs: Cybernetics.	MAY 2020
• HackTheBox's Pro Labs: Offshore.	SEP 2019
• Virtual hacking Labs (VHL).	NOV 2018

Training

• Advanced Fuzzing and Crash Analysis. (FUZZING/IO)	JUL 2024
• Security and the Linux Kernel (LFD430).	JUL 2023
• Enterprise Attack Initial Access for red teamers (ANTISYPHON)	MAR 2022
• CCNA Routing and Switching. (JICC)	DEC 2016

Projects & Contributions

- CVE-2019-10149 is a remote command execution (RCE) exploit on Exim versions 4.87 to 4.9.
- CVE-2021-27928 is a remote code execution exploit for MariaDB.
- Pureftpd-FXPAbuse Exploiting Pureftpd FXP EPRT (RFC 2428) to Obtain Target Server's IPv6.
- MySQL-DSN Exploit DSN injection using a simulated MySQL server.
- BFCanary multiprocessing tool to brute-force x64 canary value, frame pointer, and return address.
- ZabbixAPIAbuse is a tool for Zabbix API to execute commands on agents.
- BNIDA is a plugin that provides the ability to transfer analysis data between IDA Pro and Binary Ninja.

Activities & Achievements

- hacktheboxeu (Diefunction) Ranked #7 in hacktheboxeu Hall of Fame (HOF), active for 4+ years.
- bugbounty.sa (Rayan Althobaiti) Ranked #3 with 2435 points and submitted 58 reports.
- SYNACK Red Team (Rayan Althobaiti) Part of SYNACK's elite cybersecurity research team.
- Winning the Flare-on 8 - 2021.
- Winning the Flare-on 9 - 2022.
- Winning the Flare-on 10 - 2023.
- Winning the Flare-on 11 - 2024.