

Abdennour CHAHAT

✉ abdennourchahat@gmail.com ☎ 0625649737 🔗 <https://ch47t.github.io/my-portfolio/>
in <https://www.linkedin.com/in/chahat-abdennour/> 🔗 <https://github.com/ch47t>

RESUME

Highly motivated and skilled **full-stack developer and cybersecurity** enthusiast with expertise in web development and penetration testing. Currently pursuing a degree in **Digital Development and Cybersecurity Engineering** at the National School of Applied Sciences Fes (ENSAF). Eager to apply my technical skills, including ethical hacking, full-stack development, and risk management, to a challenging role in the tech industry.

Technical Skills

- **Web Development:** *HTML , CSS , JavaScript , React.js , PHP , Bootstrap , Tailwind CSS , Vite , SQL , Laravel , ShadCN , RESTful JSON.*
- **Cybersecurity:** *OWASP Top 10 , SQL Injection (SQLi) , Cross-Site Scripting (XSS) , Cross-Site Request Forgery (CSRF) , Server-Side Request Forgery (SSRF) , Local File Inclusion (LFI) , Remote File Inclusion (RFI) , Ethical Hacking , Reconnaissance , Scanning & Enumeration , Exploitation , Post-Exploitation , Reporting & Mitigation .*
- **Networking & Security:** *TCP/IP Protocol Suite , Network Protocols (DNS , DHCP , HTTP , HTTPS) , Routing & Switching , Firewall Configuration , Intrusion Detection & Prevention Systems (IDS/IPS) , Virtual Private Networks (VPN) , Wireshark for Packet Analysis , Vulnerability Scanning , Risk Management & Mitigation , IPsec , SSH/SSL Security , Wireless Security (WPA/WPA2).*

Experience

Telstra, Security Team Member

Remote
July 2024

- **Responding to a Malware Attack:** Upon receiving an alert at the Security Operations Center (SOC), I triaged the alert and responded to the malware attack by promptly contacting the appropriate team for further action.
- **Analyzing the Attack:** I analyzed the data from the malware attack to understand how the malware spreads. By identifying patterns used by the attacker, I was able to prepare a firewall rule to prevent the virus from spreading further.
- **Mitigating the Malware Attack:** Using the identified patterns, I developed a Python script to create a firewall rule that effectively mitigates the spread of the malware.
- **Incident Postmortem:** After resolving the incident, I compiled a comprehensive postmortem report to reflect on the details of the incident, including the response, analysis, mitigation efforts, and lessons learned.

Mastercard, Identify and prevent security risks

Remote
July 2024

- **Design a Phishing Email Simulation:** I developed a phishing email simulation aimed at raising awareness about one of the most prevalent threats faced by organizations today. This simulation serves as an educational tool to help employees recognize and avoid phishing attempts.
- **Interpret Phishing Simulation Results:** I analyzed the outcomes of the phishing email simulation to identify areas of improvement and delivered targeted phishing prevention training to the affected teams. This ensures that our employees are better equipped to handle phishing threats and reinforces our overall security posture.

Certifications

Fortinet Certified Fundamentals in Cybersecurity	FCF
CompTIA Security+ (Prep)	
Certified in Cybersecurity	CC
Practical Ethical Hacking	PEH
Certified Information Systems Security Professional (Short course)	CISSP


Education

National School of Applied Sciences (ENSAF) Digital Development and Cybersecurity	Sept 2022 – May 2027
Cisco Networking Academy Cybersecurity track	Aug 2024 – Sep 2024

Projects


Comprehensive Encryption Tool

- User-friendly tool for encrypting, decrypting, and hashing text, featuring hands-on learning with Caesar and substitution ciphers.
- **Tools Used:** Python, MD5, SHA-256, ASCII art for enhanced user experience.

github.com/ch47t/cybersecurity-projects 


Hash Breaker

- Developed a tool for cracking and recovering passwords from hashed data using various algorithms.
- **Tools Used:** Python, Hashcat, bcrypt, MD5, SHA-256.

github.com/ch47t/cybersecurity-projects 


WiFi Security Analysis Tool

- Scanning for nearby networks, discover accessible WiFi networks and capture handshakes for potential password cracking.
- **Tools Used:** Python, Wireshark, Aircrack-ng, and Hashcat for analyzing security vulnerabilities and generating reports.

github.com/ch47t/cybersecurity-projects 

Network Security Scanner and Service Cracker

- **Scanning for open ports:** Identify potential vulnerabilities by discovering active ports on target systems and detecting service versions running on those ports.
- **Tools Used:** Nmap, Netcat, Hydra, and Burp Suite for cracking SSH and FTP credentials during ethical testing.

github.com/ch47t/cybersecurity-projects 

Technologies

Languages: C++, C, SQL, JavaScript, PHP, Python.

Technologies: React.js, Laravel, Tailwind CSS, ShadCN, MySQL, Vite, Postman, Docker.

Cybersecurity Tools: Burp Suite, Metasploit, Wireshark, Nessus.

Languages

Languages: Arabic (Native), English (Fluent), French (Technical), Spanish (Beginner)