Chris Annett

Omaha, Nebraska | +1 (402) 305-9135 |cwayneannett@gmail.com | www.linkedin.com/in/christopher-annett-ab342b108

WORK EXPERIENCE

Operations Support Specialist | Charles Schwab| Omaha Nebraska April 2020 – December 2023

As a professional at Charles Schwab and TD-Ameritrade, I honed my client-centric skills, developing personalized financial solutions, and advising on complex matters like estate and divorce settlements. My focus is on understanding and mitigating risks, crucial for GRC roles. I collaborate with diverse teams to resolve technical problems and optimize operations, ensuring operational efficiency and compliance within governance frameworks.

Technical Skills

Tools and Technologies: Burp Suite, Wireshark, ELK (Elasticsearch, Logstash, Kibana) SIEM, Metasploit, Nmap, Nessus, GitHub, Netsparker, MS Office Suite, Apache Server, phpMyAdmin, AWS, Azure, and Rapid7. Jack the Ripper, Metasploit, Nmap

Programming Languages: Python, C and C++, Java, SQL, HTML, PHP, and CSS.
Operating Systems: Kali Linux, Windows, MacOS, Ubuntu, Android, iOS.

Frameworks: NIST, MITRE ATT&CK, CIS, NIST, ISO, GDPR, PCI-DSS
Abilities: Penetration Testing, Asset Management, Network Forensics, Log Analysis, Process Optimization, MFA Cloud Security, Data Visualization, and Compliance Testing.

Certifications

- **CompTIA Security+ (Sec+)**
- **Google IT Specialist Certificate**
- **Google Professional Cybersecurity Certificate**
- **LinkedIn: Cybersecurity**
- **LinkedIn: Ethical Hacking with JavaScript ● LinkedIn: Learning the OWASP Top 10 ● University of Maryland, Cybersecurity**

Projects and Achievements

- ● **7Fortify.co:** A freelancing project and blog devoted to preventing internet counterfeiting and safeguarding brands. Disseminate cybersecurity knowledge and enable brands to combat scams.
- ● **Configuration of a Network:** Configured an entire organizational network on CISCO Packet Tracer, incorporating 5 servers, 10 switches, and 20 computers.
- ● **Security Research and Testing:** Performed in-depth penetration testing on various websites to identify vulnerabilities and weaknesses in their security infrastructure.
- ● **Phishing Simulation and Security Assessment:** Led a comprehensive security assessment by simulating real-world phishing attacks and bypassing Microsoft's Multifactor Factor Authentication by incorporating reverse proxy methods. (Done in a secure, testing environment with the necessary permissions.)
- ● **Shell Access Development:** Developed a Python script to gain shell access to a host computer and demonstrate remote code execution (RCE).