Brenda Hensley

606.939.5430 | hensley.brenda@protonmail.com | LinkedIn | GitHub | Portfolio

SUMMARY

Application Security Engineer (CySA+, PenTest+, Security+, SSCP) with a B.S. in Cybersecurity and 1+ years of experience in red team simulations, CTFs, and application-layer vulnerability testing. Skilled in OWASP Top 10, Burp Suite, and threat modeling using MITRE ATT&CK. Proven ability to identify, exploit, and clearly communicate security issues while collaborating across security and development teams.

SKILLS

Web App Security: OWASP Top 10, Burp Suite, OWASP ZAP, Vulnerability Discovery

Offensive Security: Phishing Simulations, Red Teaming, Cloud Attacks (AWS), CTFs

Tools & Techniques: Nmap, GoBuster, Hydra, Metasploit, WPScan, MITRE ATT&CK

Scripting & Analysis: Python, Bash, SQL, Linux Privilege Escalation, Recon & Enumeration, Static Code Analysis

CERTIFICATIONS

Pentest+ | CySA+ | SSCP | Security+ | SAL1 | CC | ITIL v4 | Linux Essentials | Network+

EXPERIENCE

Penetration Testing Intern | Cybertection | *March 2025 – May 2025*

- Simulated attacker behavior targeting a Dropbox account to identify cloud security risks.
- Conducted phishing simulations and adversary emulation aligned with MITRE ATT&CK.
- Contributed to detection strategy refinement through attacker behavior analysis.

Legal Support Representative | Black Hills AI | *December 2020 – Present*

- Ensured 100% compliance with data handling protocols while processing 80+ legal documents daily, reducing audit discrepancies by 20% through systematic QA reviews.
- Improved data accuracy by 30% through audits and documentation optimization.
- Collaborated with legal and IT teams to resolve high-priority data anomalies under 24-hour SLAs, preserving data accuracy and timeliness.

PROJECTS

Adversary Simulation Lab (AWS SOC Homelab) | April 2025

- Deployed vulnerable EC2 instances in AWS to simulate enterprise targets and test adversary TTPs in a controlled environment.
- Executed attacks including privilege escalation and lateral movement using Kali Linux tools.
- Collected and analyzed logs via Splunk to assess detection coverage and improve response capabilities based on MITRE ATT&CK mappings.

Application Security Project | CodeSphere (Open Source) | *April 2025 – Present*

- Identified and documented application-layer vulnerabilities in locally hosted web applications.
- Collaborated with developers to improve authentication logic and remediate insecure configurations.
- Contributed to threat modeling efforts and supported secure DevSecOps practices.

TryHackMe: Bricks Heist | March 2025

- Exploited WordPress CVE-2024-25600 to gain shell access using WPScan, Metasploit, and enumeration techniques.
- Documented findings and mapped actions to MITRE ATT&CK to reinforce adversary emulation practices.

Cyber Sentinel Challenge – Correlation One (DoD-Sponsored) | *June 2025*

- Selected participant in a national DoD-sponsored program assessing forensics, reverse engineering, OSINT, networking, and web security skills through real-world simulations.

EDUCATION

Bachelor of Science in Cybersecurity and Information Assurance | Western Governors University
September 2024 – February 2025

Relevant Coursework: Legal Issues in Information Security, Digital Forensics, Managing Information Security, Managing Cloud Security, Cyber Defense and Countermeasures