Belizaire Bassette II

Syracuse, NY | 954-404-4123 | bebasset@syr.edu
LinkedIn: https://linkedin.com/in/belizaireb | Portfolio: https://bebasset.github.io/

Professional Summary

Offensive security practitioner and Junior Penetration Tester with hands-on experience conducting web application and network security assessments within a PTaaS consulting environment. Identified 73 vulnerabilities across 5 client engagements including high-impact findings such as IDOR, XSS, and Arbitrary File Upload. Promoted from intern to junior penetration tester based on consistent delivery of high-quality findings and professional reporting. Skilled in vulnerability discovery, exploitation, and professional reporting using tools such as Burp Suite, Nmap, Nessus, and Hydra. eJPT certified and currently pursuing OSCP and BSCP to further develop advanced penetration testing and web exploitation capabilities.

Technical Skills

Offensive Security Tools:	Burp Suite, Nmap, Nessus, Hydra, Metasploit
Programming / Scripting:	Python, Bash, SQL
Operating Systems:	Kali Linux, Linux, Windows
Security Techniques:	Web Application Testing, Network Enumeration, Privilege Escalation, Active Directory Exploitation, API Testing
Frameworks:	OWASP Top 10, MITRE ATT&CK, NIST Cybersecurity Framework

Professional Experience

Maltek Solutions LLC (Remote) Dec 2025 – Present

Junior Penetration Tester Apr 2026 – Present

Penetration Testing Intern Dec 2025 – Mar 2026

- Promoted to Junior Penetration Tester based on performance across internship engagements and quality of vulnerability findings and client deliverables.
- Conducted black-box and gray-box penetration tests across 5 web application engagements within a PTaaS consulting environment, identifying 73 total vulnerabilities.
- Discovered and validated high-impact findings including 7 IDOR, 10 XSS, 3 Arbitrary File Upload, 2 CSRF, and 1 Mass Assignment vulnerability, each with documented proof-of-concept exploits demonstrating business impact.
- Identified 26 Information Disclosure instances and 9 Missing Security Header misconfigurations, directly reducing client attack surface across multiple engagements.
- Uncovered specialized vulnerabilities including CSV/XLSX Formula Injection, Insecure Password Recovery Workflow, and Username Enumeration, demonstrating depth across OWASP Top 10 categories.
- Delivered professional penetration testing reports for each engagement including CVSS risk ratings, reproduction steps, and actionable remediation guidance for client development and security teams.

IT Risk Management Apprentice — Independent Pulmonary Therapy Services May 2024 – Dec 2024

- Performed HIPAA-aligned access control and policy audits across healthcare IT systems.
- Assisted with secure handling and classification of sensitive patient health information (PHI).

Security Projects & Labs

API Penetration Testing – BOLA / IDOR Exploitation

- Tested REST APIs for broken object-level authorization (BOLA), excessive data exposure, and weak access controls using JWT token manipulation and object reference tampering.
- Documented findings with reproduction steps, CVSS ratings, and remediation guidance mirroring professional client deliverable standards.

Archangel – TryHackMe Boot2Root (Linux Web Exploitation)

- Executed a full attack chain against a Linux target: exploited Local File Inclusion (LFI) vulnerability to perform log poisoning, achieving unauthenticated Remote Code Execution (RCE).
- Escalated privileges to root via cron job abuse and PATH hijacking, demonstrating end-to-end compromise from initial access to full system control.

pfSense Firewall Penetration Test – Enterprise Network Lab

- Assessed a Windows enterprise network protected by pfSense firewall using Nmap, Nessus, and OpenVAS to identify misconfigurations and exploitable services.
- Produced hardening recommendations including DMZ redesign and firewall policy updates based on a structured five-phase penetration testing methodology.

Central New York Hackathon – Cybersecurity Track

- Performed SOC-style alert triage and log analysis using simulated SIEM data.
- Identified indicators of compromise including suspicious IP activity and authentication abuse.

Education

Syracuse University — B.S. Information Management & Technology
Concentration: Information Security | Minor: Computer Science
Expected Graduation: May 2026

Certifications

eJPT — INE
OSCP — Offensive Security (In Progress)
BSCP — PortSwigger (In Progress)