# JARRED CARTER

## EDUCATION

**MS Cybersecurity** • New York University • May 2025 • GPA 3.8/4.0

- Coursework: Application Security, Web Application Exploiting Information Security and Privacy, Network Security, Pentesting and Vulnerability Analysis, Application Security, Computer Networking, Digital Forensics, Reverse Engineering,
- Certifications: CompTIA Security+, Pentest+ (in progress)

**BS Computer Science, BS Cybersecurity** • Marshall University • Dec. 2022 • GPA 3.7/4.0

## RELEVANT EXPERIENCE

***Security Analyst*** 06/2024 – 09/2024

Open Law Library, Washington, D.C.

- Achieved 25% increase in efficiency of setup process by parallelizing backend operations in 14 code dependencies for data fetching and streamlining logging output verbosity for government law repositories.
- Impacted UX for 40k+ users across high-traffic open-source repositories by resolving 6 critical GitHub issues, boosting repository health and reducing delays and bug-related downtime during edits to repositories.

***Information Systems Specialist I*** 05/2018 – 08/2023

WorkForce West Virginia, Charleston, WV

- Reduced costs by ~$150k by designing and implementing in-house resume construction system using ASP.NET, C#, HTML5, and SQL to eliminate need for Microsoft Office 365 licenses at 18 career centers statewide.
- Spearheaded comprehensive user support and training documentation process to optimize future employee onboarding and decrease time spent on future software development and feature addition efforts.
- Decreased setup errors by 40% and accelerated new-hire readiness by streamlining user onboarding through comprehensive training documentation and standardized Salesforce CRM provisioning.
- Strengthened agency cybersecurity posture by conducting continuous vulnerability assessments using Nessus, correlating results to known CVEs for remediation planning, and coordinating mitigation efforts with technical teams to ensure timely patching and compliance with federal security guidelines.

***Penetration Testing Engineer*** 08/2022 – 12/2022

City National Bank, Cross Lanes, WV

- Communicated security risks to IT and business stakeholders in business terms, enabling informed decision-making on remediation priorities and resource allocation.
- Enhanced enterprise threat detection and network security by configuring and deploying honeypots using Raspberry Pi.
- Performed comprehensive network penetration testing and verified patching of previously discovered vulnerabilities by exploiting web applications and scanning network traffic logs using Metasploit, Wireshark, Maltego, and Shodan.

***PSL Research Test Engineer*** 06/2021 – 08/2021

NASA Glenn Research Center, Cleveland, OH

- Saved ~$1m in costs per test run by developing a virtual fuel simulator in IEC Structured Text, enabling accurate propulsion system emulation for NASA mechanical test engineers.
- Authored paper detailing the processes, calculations, scalability, and results of the completed simulator addition.

## SKILLS

- Proficient in English and Spanish (reading, writing, speaking)
- SIEM and Monitoring: Splunk, tcpdump, Wireshark, network traffic analysis, incident response
- Threat Intelligence & Analysis: MITRE ATT&CK, malware analysis, threat hunting, TTP identification, SQL querying, pattern recognition, anomaly detection
- Pentesting & Vulnerability Assessment: Metasploit, Nmap, Recon-ng, AMASS, Maltego, Shodan, FOCA, Nessus, Scalpel, FTK Imager, Autopsy, GDB, Binary Ninja/Ghidra, BurpSuite, IDA Pro, Django Security, Container Security, Mobile Application Security, automated security testing
- Programs and OS: macOS, Windows, Kali, Ubuntu, Articulate 360, Adobe InDesign, Git, GitHub
- Programming Languages: Python, SQL, C#, ASP.NET, Java, HTML, CSS, Flask
- Communication for technical and non-technical stakeholders

## AWARDS AND PUBLICATIONS

- CyberCorps Scholarship for Service Scholar, awarded to top 1% of the class for two years in a row.
- J. M. Carter, H. S. Narman, O. Cosgun and J. Liu, Trade-off Model of Fog-Cloud Computing for Space Information Networks, 2020 IEEE Cloud Summit (2020), pp. 91-96, doi: 10.1109/IEEECloudSummit48914.2020.00020.
- J.M. Carter, C.E. Morris, M.J. Oliver, Addition of Stahl Heater to the Propulsion Systems Laboratory Simulator's 450lb Airline, NASA Internal Paper (2021).

## PROJECTS

***Offensive Security CTF Challenges*** Fall 2024

- Analyzed malicious artifacts and reverse engineered 20+ malware samples using Ghidra and Binary Ninja to identify threat actor TTPs and attack chains.
- Exploited 20+ vulnerabilities across buffer overflows, register corruption, and glibc/heap memory issues by completing 4 weekly CTF challenges for 14 weeks using reverse engineering tools including Ghidra and Binary Ninja to analyze C executables and develop exploitation techniques
- Achieved root access on 5 servers by leveraging HTML encoding and SQL-based exploits for web challenges, documenting vulnerabilities and binary analysis findings, exploitation techniques, and payloads in extreme detail.

***SQL Database Modeling and Querying Project*** Fall 2024

- Designed and executed complex SQL queries for threat hunting across 5,000+ data records, enabling rapid identification of anomalous patterns and indicators of compromise.
- Enabled real-time inventory lookup of over 5k+ items by designing normalized relational schemas from ER diagrams and writing/executing complex CREATE TABLE, INSERT, SELECT, and JOIN statements using MySQL to simulate a donation system for furniture items.
- Validated the design of 3 schemas and database performance by simulating full-stack backend logic using MySQL.

***Digital Forensics Final Project*** Spring 2024

- Conducted threat intelligence analysis by reassembling deleted evidence from 8 system images and correlating findings to identify attack patterns and TTPs
- Reassembled deleted and obfuscated evidence from 8 system images using Scalpel and FTK Imager for recovery of hashes, user accounts, logs, documents, and metadata to deepen digital evidence recovery insights.
- Identified 80+ functions, libraries, and security vulnerabilities by reverse engineering unknown executables, creating and inspecting forensic images/file systems with Procmon and Pestudio.

***Application Security Engineering Projects*** Spring 2024

- **Web App Security Assessment:** Identified and remediated 4 critical vulnerabilities (XSS, CSRF, SQL Injection, command injection) in Django web application; implemented comprehensive security fixes and automated regression testing via GitHub Actions.
- **Mobile App Security:** Conducted security audit of Android gift card application, fixing Intent vulnerabilities, implementing HTTPS encryption for REST API communications, and removing privacy-invasive monitoring code.
- **Container & Kubernetes Security:** Secured containerized application deployment by implementing Kubernetes Sealed Secrets for credential management, configured Prometheus monitoring with custom security metrics, and established CI/CD pipeline with automated security testing.
- **Binary Security & Fuzzing:** Identified and fixed 6 buffer overflow and memory corruption vulnerabilities, achieving an 85%+ code coverage through systematic case development by performing a vulnerability assessment on legacy C application using AFL++ fuzzer and coverage analysis.

***Cyberassess: Cybersecurity Competency Assessment*** Spring 2022

- Designed and developed 75% of the interactive assessment modules in Articulate 360 while acting as primary liaison between the team and professor, implanting proactive deadline strategies for delay prevention.
- Spearheaded the design and delivery of 4 final project materials and accompanying presentation to an audience of over 60 colleagues, faculty members, and guests from other projects and the surrounding community.
- Informed 10+ team and faculty members of individual task progress, status, and projected completion times by compiling and distributing 15 comprehensive weekly reports.