Logan Breckenridge
Cybersecurity Engineering Student

loganbreck1@gmail.com
linkedin.com/in/logan-breckenridge
br3xinn.github.io/Portfolio

EDUCATION

George Mason University | B.S. Cyber Security Engineering | GPA: 3.7 *(2022– 2026)*
- Freelance Tutoring (Computer Science)
- Mason Competitive CyberSec Club

Relevant Coursework - Computer Programming, Operating Systems, Computer Networking, Secure Software Development, Cryptography, Secure RF Communications, Critical Infrastructure Protection, Systems Engineering, Object-Oriented Design and Modeling, Digital Electronics, Probability and Statistics

WORK EXPERIENCE

Company | Application Security (Hybrid) **|** *(May 2024 - Aug 2024)*
- Shadowed Application Security professionals, gaining hands-on experience in real-world vulnerability assessments and applying industry best practices.
- Researched web application core functionalities, gaining expertise in networking and communication protocols.
- Conducted vulnerability assessments on intentionally vulnerable web applications using tools like Burp Suite and DirBuster, enhancing my skills in detecting and addressing security flaws.
- Developed tools within Burp Suite to analyze real-time web traffic, offering additional insight and detection in identifying vulnerabilities

Company | Software Engineer (Fairfax VA) **|** *(Mar 2023 - May 2024)*
- Utilized data analytics and image processing to ensure data integrity, reformatting data such as mil2525c symbology and data properties.
- Built and established new means of constructing complex data for pre simulation analysis, increasing processing speeds by over 400%.
- Generated interactive websites housing data tables/geospatial products, aiding in decision-making and analysis.

George Mason University | Research Assistant (Fairfax VA) **|** *(Feb 2023 - May 2024)*
- Gained extensive knowledge surrounding strategic, tactical, and operational level planning.
- Presented findings to audiences, including sponsors such as DARPA and Linquest.

SKILLS

Coding Languages - Python, C, Bash, , Powershell, Javascript, Jython, HTML, CSS

Certifications - CompTIA Security+

Applications - Burp Suite, Linux, Docker, Wireshark, VMware, Protege, Git,

Tools/Libraries - Windows API, DirBuster, Nmap, Regex, BeautifulSoup, Requests, Pandas, Shutil, OS, Whatchanged, Itertools, Geopy, Pillow, Folium, Owlready2

PROJECTS

Developing Burp Suite tools for Application Vulnerability hunting
- Discovered multiple vulnerabilities in response headers across various web applications during penetration testing with Burp Suite, focusing on issues related to the server and set-cookie keys.
- Created custom scripts to automate the detection process for these specific vulnerabilities, ensuring consistent identification in both current and future web applications.
- Integrated these scripts with Burp Suite, enabling real-time analysis of web traffic and the immediate generation of detailed vulnerability reports.

Reverse Engineering and Vulnerability Assessment
- Conducted in-depth vulnerability assessments on the Respondus Lockdown browser, focusing on identifying potential exploits through reverse engineering of its features.
- Developed a custom script to access and monitor changes in Winreg keys/values over time, allowing for the detection of specific modifications made by Respondus.
- Utilized various Windows APIs to extract detailed information surrounding the locked-down environment.
- Combined these findings with PowerShell scripts to spoof the active window, enabling the possibility of bypassing a majority of Lockdown's restrictive features and demonstrating potential security flaws.