Logan Breckenridge
Cybersecurity Engineering Student

Linkedin linkedin.com/in/logan-breckenridge
Personal Website br3xinn.github.io/Portfolio

For the longest time, spanning back to early high school I was always interested in discovering vulnerabilities/exploits whether it be in a video game or sophisticated software such as Respondus Lockdown browser. This very interest led me to obtain experience ranging anywhere from developing real-time bots via Python, to reverse engineering and exploiting Lockdowns systems. For this reason, I'm looking for the opportunity of continuous learning. In return, I offer my full commitment and eagerness to learn.

RELEVANT WORK EXPERIENCE

Software Developer | *(Mar 2023 - Present)*

- 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.

University | Research Assistant | *(Feb 2023 - Present)*

Gained extensive knowledge surrounding strategic, tactical, and operational level planning. Furthermore, gained immense experience working on team-oriented and individualized tasks, presenting findings to audiences, which included sponsors such as **DARPA and Linquest**.

PROJECTS

Reverse Engineering and Vulnerability Assessment

Performed vulnerability assessments on the widely used Respondus Lockdown browser. This led me to not only identify the ways they administered certain features but even reverse-engineered them in hopes of discovering possible exploits(which I did). For example, I concluded that they were changing the Windows registry values, to find out the extent of this, I developed a script that accessed Winreg keys/values and would monitor the changes over a period of time. To reverse engineer some features of their locked-down environment, I worked with many of the Windows APIS to grab all active process names, handles, and their status. I later combined this with PowerShell scripts to spoof the active window, this allows for the possibility of bypassing a majority of Lockdown's features.

Data collection and Web Scraping

Developed scripts to access and store data found in my organization's Outlook address book. This allowed me to obtain key/value formatted data for over 300,000 users. I then, to obtain additional data parameters, researched and coded means of web scraping a public organizational website. While doing this, I created algorithms to bring an estimated 14 hours of processing, down to sub 20 minutes.

EDUCATION

University - B.S. Cyber Security Engineering - GPA: 3.88 *(2022– 2026)*
- *Freelance Tutoring (Computer Science)*
- *CyberSec Club*

SKILLS

Programming Languages - Python, C, HTML ,CSS

Certifications - 98-381:MTA Intro to python (Microsoft), 98-367:MTA Security Fundamentals

Applications - Visual Studio Code, Protege, Git, Adobe Photoshop, Hitfilm Express

Tools/Libraries - Pyautogui, Pywin32, BeautifulSoup, Requests, Geopy, Json, Csv, Pillow, Folium, Owlready2, Whatchanged, Shutil, Os, Itertools