CALEBAFEWORK

+1(678)852-4887 ⋄ Denver, CO

calebafework@gmail.com ⋄ https://www.linkedin.com/in/calebc0des/ ⋄ https://calebc0des.com/
https://medium.com/@calebafework

OBJECTIVE

Focused and highly motivated cybersecurity professional with expertise in offensive security, penetration testing, and secure coding practices. Adept at analyzing complex systems, identifying vulnerabilities, and developing innovative solutions to mitigate risks. I am skilled in communicating technical concepts to diverse audiences and promoting a collaborative team environment.

EDUCATION

Bachelor of Cybersecurity and Information Assurance, Western Governors University	Expected 2025
Adult Technology Training Bootcamp, Urban Tech Academy	2023
Software Engineering Immersive Program, General Assembly	2021

CERTIFICATIONS

Practical Network Penetration Tester (PNPT), TCM Security	Expected 2025
SOC Core Skills, Antisyphon	Jan 2025
Intro to Cloud Security, Antisyphon	Jan 2025

SKILLS

Skills	Software Development, OSINT, Vulnerability Assessment and Penetration Testing, Report Writing, Log Analysis, Incident Detection
Languages and Tools	JavaScript, SQL, Vue, Git, HTML, CSS, React.js, Express.js, Node.js, LotusScript, Python, Bash, VBScript, Docker, Jenkins, Jest, Nmap, Tenable Nessus, Metasploit, Netcat, Hashcat, Responder, Bloodhound, BurpSuite, AWS Cloud, Virtualization Platforms

EXPERIENCE

Cyber Threat Intelligence Analyst (Volunteer)   Nov 2022 - Current
BDPA Foundation   *Chicago, Il*

- Supported the collection and analysis of open-source intelligence (OSINT) to identify potential threats targeting industries such as manufacturing, healthcare, and retail.

- Participated in team exercises to understand and address social engineering risks, including developing basic social media strategies to reduce vulnerabilities.

- Gained hands-on experience with the MITRE ATT&CK framework by helping identify and document tactics, techniques, and procedures (TTPs), indicators of attack (IOAs), and indicators of compromise (IOCs).

- Assisted in integrating and managing threat intelligence data within SIEM platforms under the guidance of senior team members.

- Contributed to categorizing and tracking threat actors and campaigns as part of a team, ensuring alignment with goals and priorities.

Software Support Engineer III   Oct 2021 - Nov 2024
K-Care   *Austin, TX*

- Updated and maintained application components using custom HTML, JavaScript, JSON, HCL "formula language," and LotusScript to support cross-platform functionality for a user base exceeding 25,000 customers. Ensured integrity and compliance of regulatory documents by auditing and validating them to meet foster care and general case management standards, safeguarding business value and proper auditing by various agencies.

- Developed JavaScript input validation and regex checks to ensure data accuracy, security, and adherence to best practices for secure data manipulation (NIST SP 800-218, NIST SP 800-53, HIPPA). Designed and implemented JavaScript tools to automate sensitive document handling processes, reducing processing time by 30% while enhancing efficiency.

- Conducted log analysis and incident detection by reviewing server logs for application errors, performance issues, and potential security threats. Identified anomalies, troubleshooting root causes, and implementing proactive measures to enhance system reliability and security.

- Authored and maintained detailed internal documentation, including database management procedures, secure coding practices, troubleshooting techniques, and process optimizations, fostering team-wide knowledge sharing and operational consistency.

- Managed and secured databases by creating, updating, and deleting sensitive data stores to support application functionality and meet customer requirements, while adhering to industry standard security protocols to ensure data integrity and prevent unauthorized access.

Frontend Software Engineering Intern   June 2021 - Aug 2021
Moogsoft   *San Francisco, CA*

- Refactored 60 functional components, optimizing our code for Vue 3 by eliminating redundancies, reorganizing code, and adopting best practices.

- Spearheaded UAT unit tests in Jest, keeping code coverage above 90% - this allowed any potential issues to be identified earlier in the development cycle, not only resulting in more secure and higher quality code (lowered frequency of patching as well).

- Migrated the developer build chain to Apple M1 architecture, enhancing development efficiency and compatibility with modern environments.

- Applied performance optimization techniques (e.g., prefetch and preload) to improve load times and user experience, indirectly supporting security by reducing exposure windows during page loads. (Lighthouse score of 92 post implementation).

PROJECTS

Custom Form Data Cleansing

Implemented team process improvements that allowed for cross training and collaboration, increased efficiency (80%), and the reduction of code errors (85%) by accomplishing the following:

• Developed and tested scripts using HCL formula language to fetch client-side data and fields correctly (previous script would only import partial data and in an incorrect format).

• Diagnosed and mitigated a flaw that caused a site-wide issue with inline CSS failing inside of a web application. Since this web application could not undergo an outage or designated maintenance window, I resolved the issue by leveraging LotusScript agents to sanitize the client site payload.

AWS Cloud Lab

Designed and deployed a virtualized cloud lab on Amazon Web Services (AWS) to simulate real-world cybersecurity scenarios and perform penetration testing using the following:

- Virtual Private Cloud (VPC) Configuration: Created a secure, isolated environment for hosting vulnerable virtual machines (VMs). Configured subnets, route tables, and a VPN endpoint for secure remote access. • Elastic Compute Cloud (EC2) Instances: Deployed and managed multiple EC2 instances, including a Kali Linux attack box for security testing and analysis. Ensured scalability and reliability of the lab environment.

- Amazon Machine Image (AMI): Utilized AWS EC2 AMI to store and manage VM images, including importing the "Breach" OVA. Automated deployment tasks with AWS Command Line Interface (CLI) for efficient resource management.

LEADERSHIP

Blacks in Technology, Chapter President/Founder – Denver, CO (Volunteer)   2021 - Current

As a founding member of the Denver chapter, I led its vision, outreach, and educational initiatives, helping the organization grow from 4 to over 250 active members. My work focused on empowering and connecting Black professionals through impactful programs and events.

- Presented community talks on career development and industry trends, educating hundreds of professionals.

- Organized and hosted networking events that connected members with companies and industry leaders.

- Developed and implemented outreach strategies to expand membership and increase community engagement.