Dominic Lagle

29 June 2024

Final Reflections

https://youtu.be/fIjV2WoaDN8

Completing CS 470 has been instrumental in advancing my professional goal of becoming a Red Team cyber analyst. This course has equipped me with a comprehensive understanding of full-stack web application development, focusing on cloud environments. I have honed skills in API development, cloud service integration, and thorough project testing. These abilities are critical for a Red Team cyber analyst, as they enable me to identify and exploit vulnerabilities in web applications and cloud infrastructures. Additionally, my experience with documenting processes and presenting technical information strengthens my ability to communicate findings and strategies effectively, a key skill in cybersecurity roles.

My strengths as a software developer include advanced debugging techniques and proficiency in multiple programming languages, including Python, Java, and JavaScript. These skills enhance my ability to write secure code and effectively troubleshoot issues, ensuring robust application security. Furthermore, my background in IT security and hands-on experience with secure coding practices position me well for identifying and mitigating security risks. With these capabilities, I am prepared to take on roles such as a cybersecurity analyst, penetration tester, or security engineer, where I can leverage my technical expertise to enhance organizational security.

In planning for the future growth of my web application, I would utilize my knowledge of cloud services to ensure scalability and efficient management. Implementing microservices architecture would allow for independent scaling of application components, improving fault tolerance and error handling. Serverless computing could also be employed to automatically scale resources based on demand, reducing operational overhead and optimizing costs. These approaches not only ensure the application can handle increased traffic but also enhance its resilience to attacks, a critical aspect of cybersecurity.

Handling scale and error management in a cloud environment involves leveraging auto-scaling groups and monitoring services to dynamically adjust resources and maintain application performance. Predicting costs requires analyzing usage patterns and selecting the appropriate pricing models offered by cloud providers. Serverless computing generally provides more predictable costs for unpredictable workloads, as billing is based on actual usage rather than pre-allocated resources. This cost-efficiency is crucial for maintaining sustainable growth without compromising security investments.

The pros of microservices and serverless architectures include increased flexibility, reduced operational complexity, and cost efficiency. However, they also introduce challenges such as increased architectural complexity and potential latency issues. Elasticity and pay-for-service models are crucial considerations for future growth, as they allow for resource optimization and cost management based on actual demand. This approach ensures that the web application can efficiently scale to meet user needs while controlling expenses, aligning with the strategic goals of scalability, resilience, and security. By planning for these factors, I can ensure that the application remains secure and robust as it grows, supporting my role in cybersecurity.