Carmen Mosquera

CS 405 – 10932-M01

08 / 24 /2024

Journal: Portfolio

In this reflection, I'll discuss the work I did throughout the course, particularly focusing on four key areas: the adoption of a secure coding standard, risk evaluation and assessment, the zero trust model, and the implementation and recommendations of security policies.

1. Adoption of a Secure Coding Standard

One of the most critical lessons that I learned from this course is the importance of adopting a secure coding standard early in the development process. If we integrate security considerations from the beginning, we ensure that our code is robust against potential vulnerabilities. This approach prevents security from being an afterthought, reducing the likelihood of costly and time-consuming patches later. As I move forward, I will continue to advocate for security as a foundational aspect of coding, emphasizing the need to align with established secure coding practices throughout the development lifecycle.

2. Evaluation and Assessment of Risk and Cost-Benefit of Mitigation

During the development of the security policy for the project, I conducted thorough assessments of potential threats and weighed the cost of mitigating these risks against the potential impact of not addressing them. This process underscored the importance of making informed decisions about which vulnerabilities to prioritize. If we understand the trade-offs, we can balance security with practical constraints like budget and time, ensuring that our security measures are both effective and efficient.

3. Zero Trust

The zero trust model, which operates on the principle that no one is inherently trusted inside or outside the network, has proven to be a valuable security best practice. In my security policy I adopted this model to minimize the risk of insider threats and unauthorized access. By implementing strict access controls and continuous verification, we can ensure that every request for access is authenticated and authorized. This is particularly relevant nowadays where breaches often occur from within. Embracing zero trust has reinforced the need to remain vigilant and skeptical, protecting our systems from both external and internal threats.

4. Implementation and Recommendations of Security Policies

The implementation of security policies provides clear guidelines and expectations for secure coding, data protection, and risk management. During the development of our security policy, I made many recommendations to ensure that these policies are practical and enforceable. This included integrating automated tools into the DevSecOps pipeline to continuously monitor and enforce compliance. I also emphasized the importance of regular training to keep teams updated on the latest security practices. This course has reinforced the importance of making security an integral part of our development process, not just a final step.