Priscilla Gomes-DaCosta

Southern New Hampshire University

6-1 Journal: Don't Leave Security to the End

12/04/2022

There are many practices and techniques that are used to improve the quality and security of software being developed. Normal code defects and vulnerabilities are correlated; therefore, vulnerabilities are eliminated when software defects are decreased. Not leaving security to the end as a best practice encourages the avoidance of coding defects being introduced that could lead to glitches and security breaches. Identifying and mitigating cyber attacks early in the development process is important to ensure the attack surface is reduced as much as possible.

Preventing threats requires anticipating and understanding the software so the proper resources can be allocated. Thread modeling involves the application’s architecture, a list of threats and can be used by project team members to understand threats to be addressed, the process is broken down in phases that includes identifying assets, creating an architecture overview, decomposing the application, identifying, documenting, and rating threads (Seacord, 2006, p. 174).

Security testing should be implemented in the earlier phases of the SDLC life cycle. Security processes like analysis for requirements and abuse/misuse cases, security risk analysis for designing, static and dynamic testing that can be accomplished using White and Black Box Testing, vulnerability scanning, penetration testing and impact analysis and implementing patches. The tests should include security-related test cases and scenarios, test data, tools and analyzing the test outputs from different security tools. Examples test scenarios would include ensuring passwords are encrypted, systems or applications not allowing invalid users, and checking cookies and session time for applications.

References

Seacord, R. C. (2006). Secure coding in C and C++. Addison-Wesley Professional.

What is security testing? Types with example. (2022, July 19).

Guru99. https://www.guru99.com/what-is-security-testing.html