Peer Response 3:

Collaborative Discussion 1: UML flowchart

In reply to Oi Lam Siu

Peer response

by Andrius Busilas - Thursday, 31 October 2024, 5:31 PM

Hi Hellen,

Selecting Open Web Application Security Project (OWASP) A07:2021 - Identification and Authentication Failures as your focus is highly relevant, given the increasing prevalence of credential-based attacks (OWASP, 2021). The vulnerabilities you identified, including insufficient account lockout measures, absence of multi-factor authentication (MFA), and inadequate password recovery processes, effectively showcase potential weaknesses in authentication systems. These selections align well with critical risk areas outlined in the OWASP Top 10 (OWASP, N.D.).

Your flowchart, created using Visual Paradigm, is commendable for its clarity and logical structure. It effectively illustrates various decision points, facilitating the visualization of potential attack vectors (Gedam & Meshram, 2023). The choice of an activity diagram format enhances accessibility for diverse audiences, including both technical and non-technical stakeholders.

To further improve the flowchart, consider incorporating a distinct path for account lockout following multiple failed login attempts (OWASP, N.D.). Additionally, implementing visual cues or color-coded elements for security-critical steps, such as MFA or session timeout checks, could enhance clarity. Elaborating on the password recovery process within the diagram would also be beneficial, allowing viewers to identify areas where knowledge-based authentication could be substituted with more robust methods like email or phone verification (OWASP, N.D.).

In conclusion, your diagram and analysis are well-constructed, and these minor enhancements could further elevate the comprehensiveness of your visualization.

References

Gedam, N., & Meshram, B. (2023). Proposed Secure Activity Diagram for Software Development. International Journal of Advanced Computer Science and Applications, 14(6), 671–680.

OWASP (2021). A07:2021 – Identification and Authentication Failures. Retrieved from https://owasp.org/Top10/A07_2021-Identification_and_Authentication_Failures/

OWASP (N.D.). Authentication Cheat Sheet. Retrieved from https://cheatsheetseries.owasp.org/cheatsheets/Authentication_Cheat_Sheet.html