Secure Software Development

CLD1 - Initial post:

The Coding weakness identified by OWASP Top 10

OWASP (2021) have identified security logging and monitoring (A09) to be in the top 10 of the most critical risks to web applications. Therefore, being able to correctly log and monitor systems and activities is fundamental in security and vulnerability (Breach) management. At present, there are many standards and regulations which organizations implement and follow, such as ISO27001 and GDPR. These standards and regulations often require logging mechanisms to be in place (Zeng et al, 2016).

However, There are many challenges for logging, such as ensuring the protection of their confidentiality and integrity (Kent & Souppaya, 2006), also, compliance and forensics investigations issue can arise when logs are unknowingly spread over several cloud data centers and cross into different areas of compliance and regulations (Mell et al, 2016).

Furthermore, According to OWASP (2021), Without logging and monitoring, breaches cannot be detected. If detection fails, then the confidentiality, availability and integrity of systems and data may be compromised. According to IBM (2022), it takes an average of 277 days to identify a breach and an average saving of $1.12 Million dollars can be achieved if the breach is detected within 200 days or less.

Therefore, effective logging formats and clear monitoring is paramount to information and system security.

Steps which may have led to the weakness occurring (Breach)

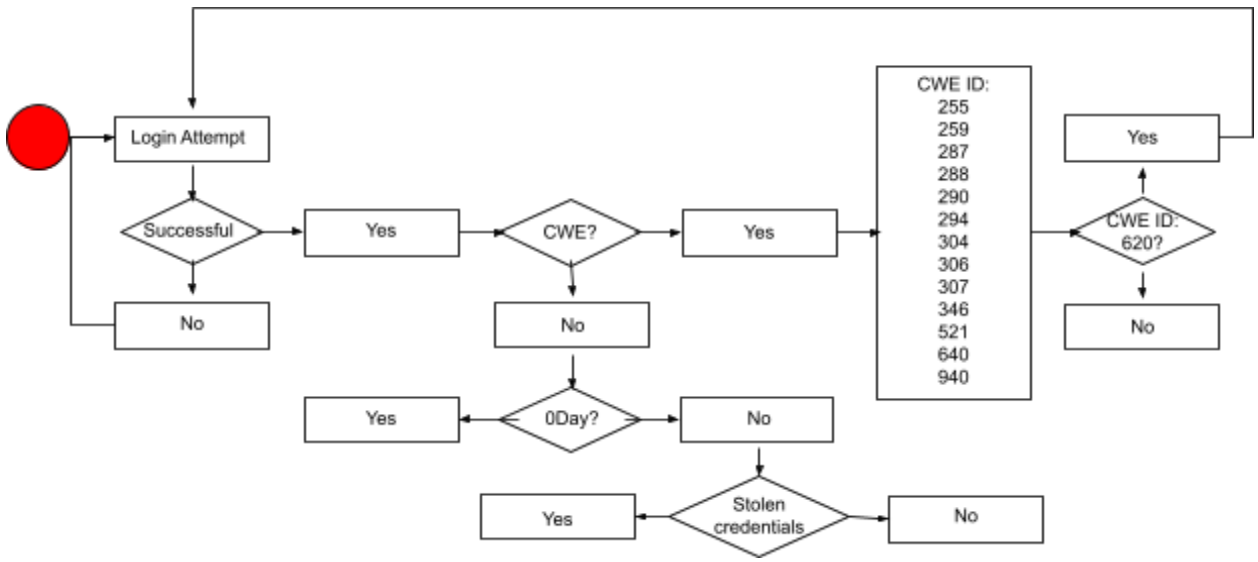

Figure1. Steps which may have led to the weakness occurring

UML models and justification to present the design of proposed software?

It is highly likely that the UML Models that could be use for presenting the design of a proposed software to help secure and mitigate against potential vulnerabilities as highlighted in the flowchart (Fig.1) would be both a sequence diagram and an activity diagram. The sequence diagram could map out which log sensors are required at various stages to provide event correlation capabilities for breach analysis. The activity diagram to map out the behavior dependencies to ensure secure development of each phase.

References

Gupta, S. (2012) Logging and monitoring to detect network intrusions and compliance violations in the environment. SANS. Available from: https://sansorg.egnyte.com/dl/DdNa8WPM2p [Accessed on 11th March 2023].

IBM (2022) Cost of a data breach 2022. Available from: https://www.ibm.com/reports/data-breach [Accessed on 12th March 2023]

Kent, K & Souppaya, M. (2006) Guide to computer security log management. NIST 800-92. Available from: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-92.pdf [Accessed on 12th March 2023]

Mell, P., Gavrila, S. & Shook, J. (2016) Restricting Insider Access through Efficient Implementation of Multi-Policy Access Control Systems. MIST '16: Proceedings of the 8th ACM CCS International Workshop on Managing Insider Security Threats, Vienna, Austria, October 24-28, pp. 13-22.

OWASPS (2021) Top 10. Available from: https://owasp.org/Top10/ [Accessed on 11th March 2023]

Zeng, L., Xiao, Y., Chen, H., Sun, B. and Han, W., (2016). Computer operating system logging and security issues: a survey. Security and communication networks, 9(17), pp.4804-4821.