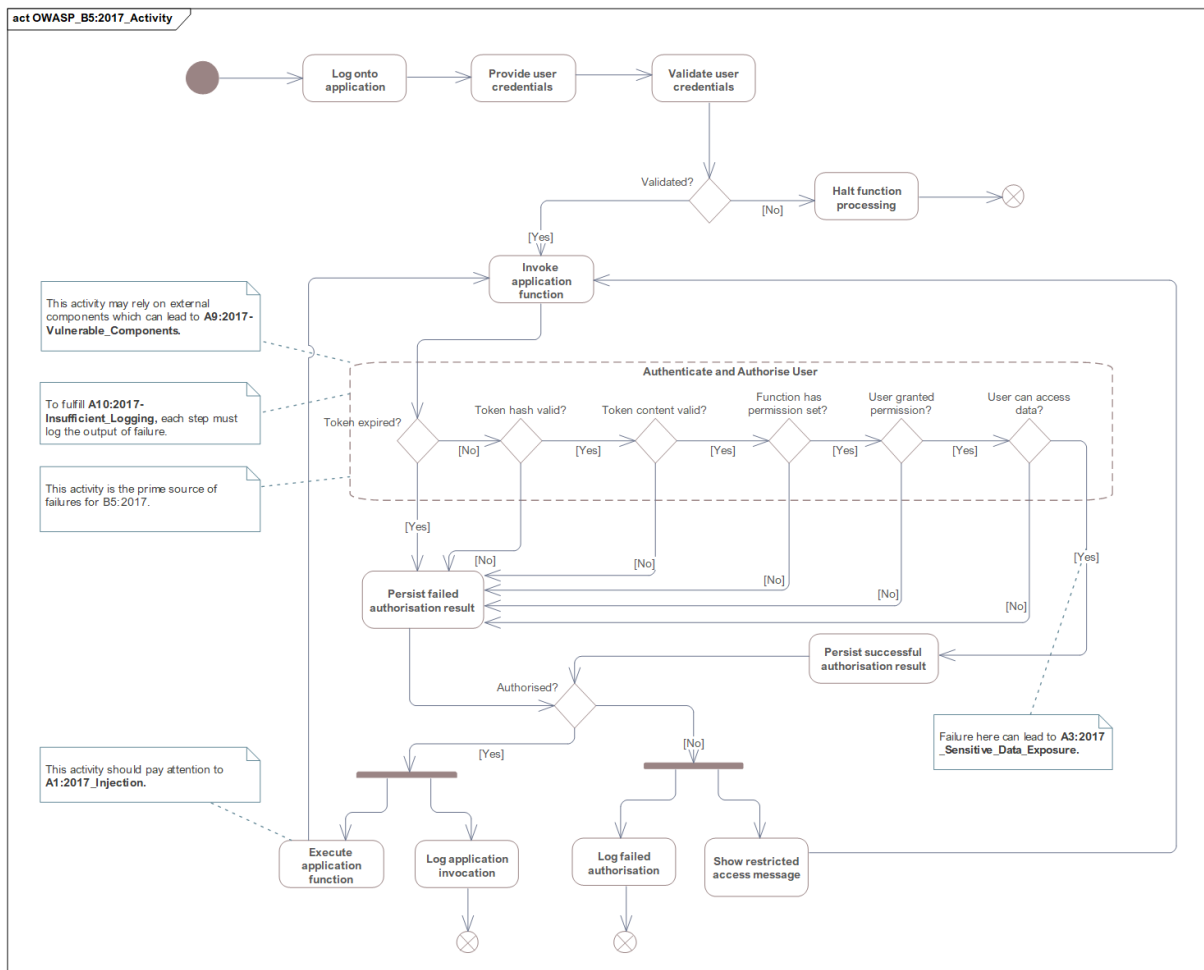


Collaborative Discussion – UML Flow Charts

Broken Access Control (A5:2017) (OWASP, 2021)—a merger of “A7:2013” and “A4:2013” (Sphoel et al., 2018)—is a vital point of security failure within applications. In this scenario, attackers exploit applications that do not perform sufficient access control checks before each function request. Successful attacks permit an attacker to perform unintended actions, access unauthorised information, or even remove and manipulate sensitive data. Common Weaknesses Enumeration (a database of software weaknesses maintained by the security community) highlights mitigations teams can leverage to reduce the vulnerability to Broken Access Control. For example, recommended are CWE-284 and CWE-285 (Mitre, 2021).

The following UML diagram shows a basic implementation of Broken Access Control within a generic application. The main vulnerability of A5:2017 lies within the **Authenticate and Authorise User** activity (or similar deployments). This activity consists of multiple security decisions to ensure a user is authorised. Suppose one or more decision points fail to validate the user’s security context correctly. In that case, the entire activity may conclude the user (or attacker) is approved. For example, if the decision of “User granted permission?” determines that no permissions are set up for the requested application function and therefore defaults to “granted”. In that case, the authorisation component has failed to secure the application and fallen foul of A5:2017.

The process is depicted as an activity diagram because it shows high-level concerns without focus on component implementation details or messages passed between components (sequence diagram). Such information is pertinent when developing frameworks.



References

- Mitre (2021). Common Weaknesses Enumeration. Available from <https://cwe.mitre.org/data/> [Accessed 16 Aug. 2021]
- OWASP (2021) OWASP Top Ten 2017: A5:2017-Broken Access Control. Available from https://owasp.org/www-project-top-ten/2017/A5_2017-Broken_Access_Control [Accessed 16 Aug. 2021]
- Søphoel, H., Jaatun, M.G. & Boyd, C. (2018) OWASP Top 10-Do Startups Care?. *International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*: 1-8. DOI: <https://doi.org/10.1109/CyberSecPODS.2018.8560666>