Unit 1

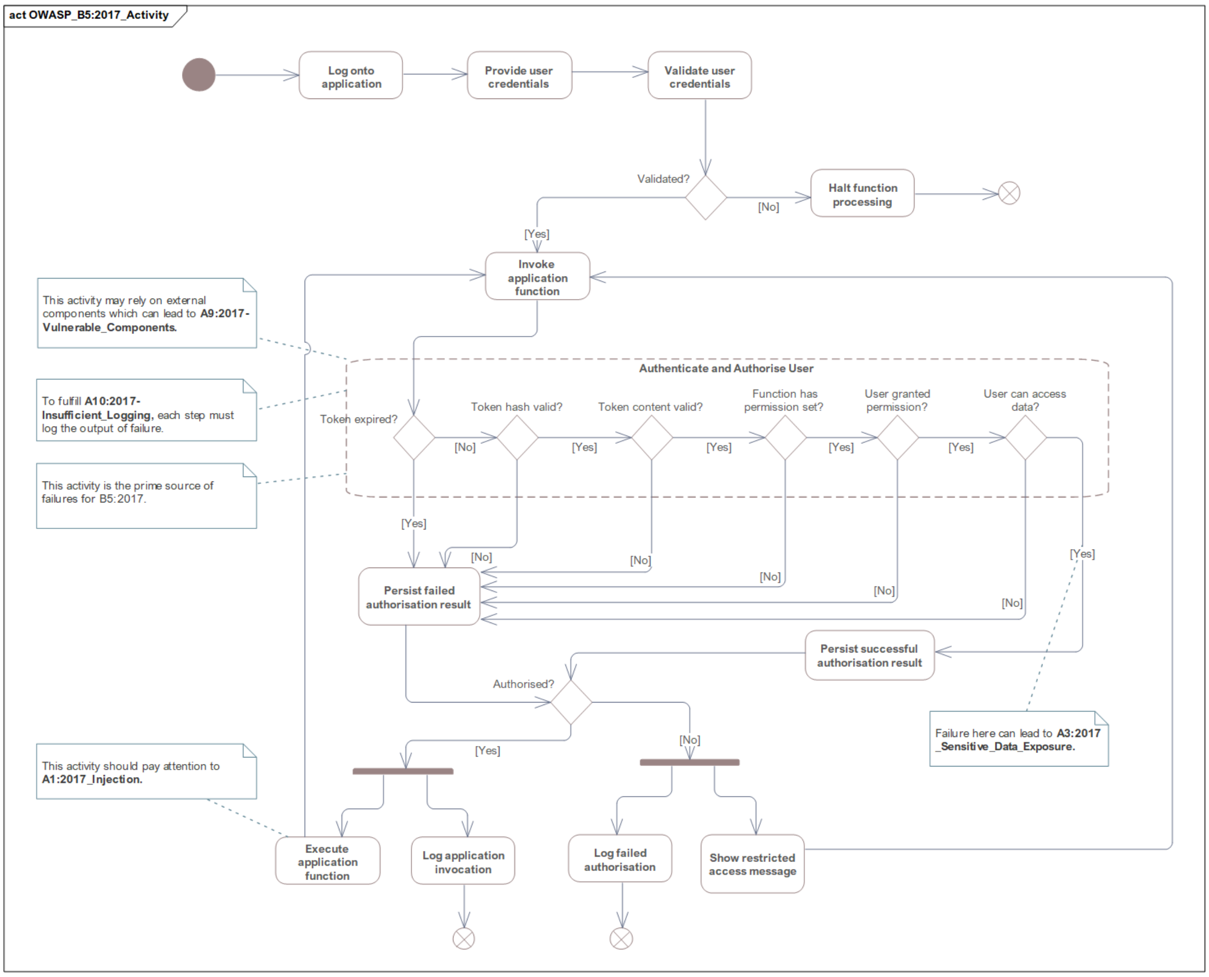
Introduction to Information Systems

Discussion Forum – Identify an OWASP Weakness

Broken Access Control (A5:2017) (OWASP, 2021)—a merger of “A7:2013” and “A4:2013” (Sϕhoel 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.


act OWASP_B5:2017_Activity
Log onto application
Provide user credentials
Validate user credentials
Validated?
[No]
Halt function processing
[Yes]
Invoke application function
This activity may rely on external components which can lead to A9:2017-Vulnerable_Components.
To fulfil A10:2017-Insufficient_Logging, each step must log the output of failure.
This activity is the prime source of failures for B5:2017.
Authenticate and Authorise User
Token expired?
Token hash valid?
Token content valid?
Function has permission set?
User granted permission?
User can access data?
[No]
[Yes]
[Yes]
[Yes]
[Yes]
[Yes]
[No]
[No]
[No]
[No]
[No]
[Yes]
Persist failed authorisation result
Persist successful authorisation result
Authorised?
[Yes]
[No]
Failure here can lead to A3:2017 _Sensitive_Data_Exposure.
This activity should pay attention to A1:2017_Injection.
Execute application function
Log application invocation
Log failed authorisation
Show restricted access message

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]

Sϕhoel, 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