Initial Post:

UML modelling can represent the OSWAP identified weakness of Broken Access Control. From the activity diagram attached, we understand how the weakness could occur; manual testing would be the preferred option as automated tools do not dive deep enough which can mean that access can be overlooked. Should testing not identify broken access control, a user could gain an elevation of privilege with rights/permissions they should not have, tamper with cookies or tokens, make primary key changes or bypass access control checks. The activity diagram (Figure 2) is a useful model as it provides a visual supplementation with a use case diagram and the processing logic offers a complete understanding (Bolloju & Sun, 2012).

The use case diagram (Figure 1) design also identifies the various users and vulnerabilities that may be presented when faced with broken access control. Normal users inadvertently gain administrative or auditing privileges that could tamper with information, and malicious users could access and disclose sensitive data. This could have severe repercussions on the business practice with a potential loss of earnings and data breach.

The benefit of the use case model indicates the potential threat and offers consistency in approach, which can be used when designing or reviewing policy (Hassan et al., 2018). Sequence diagrams also show a more operational process suggesting how components can interact and perform functions. This can be more useful in the development or review of policy procedures.

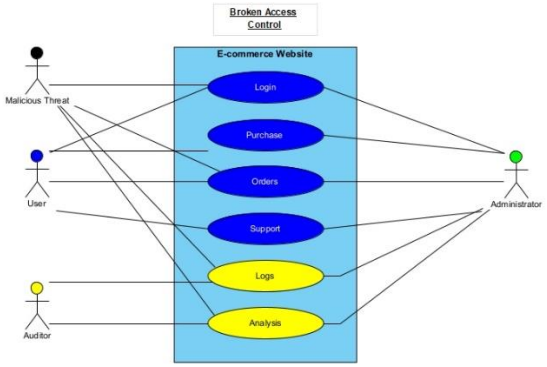

Figure 1: Use case diagram

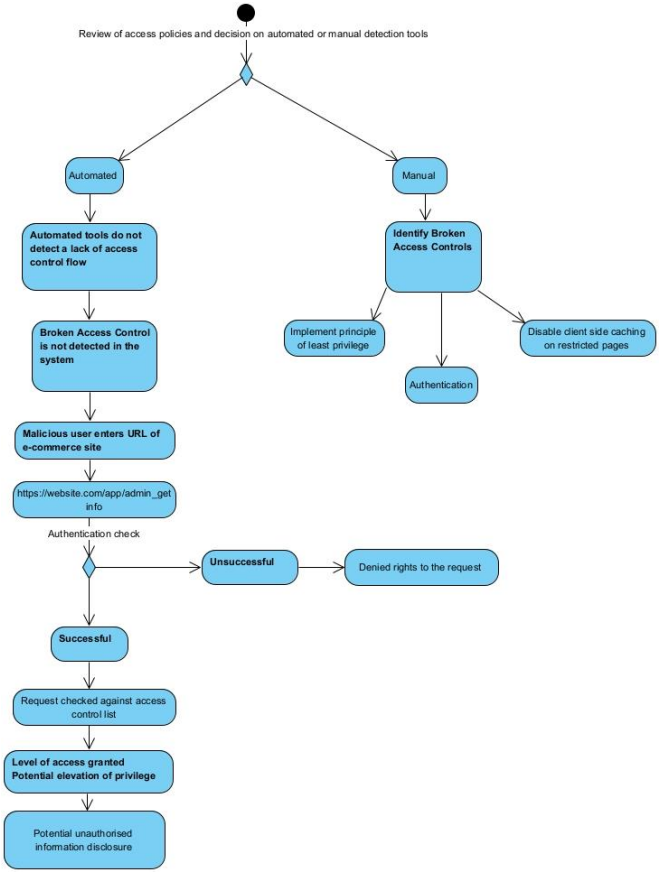

Figure 2: Activity diagram

Bolloju, N. & Sun, S. X. Y. (2012). Benefits of supplementing use case narratives with activity diagrams—An exploratory study. *Journal of Systems and Software,* 85, (9): 2182-2191.

Hassan, M., Ali, M., Bhuiyan, T., Sharif, M. & Biswas, S. Quantitative assessment on broken access control vulnerability in web applications. International Conference on Cyber Security and Computer Science 2018, 2018.