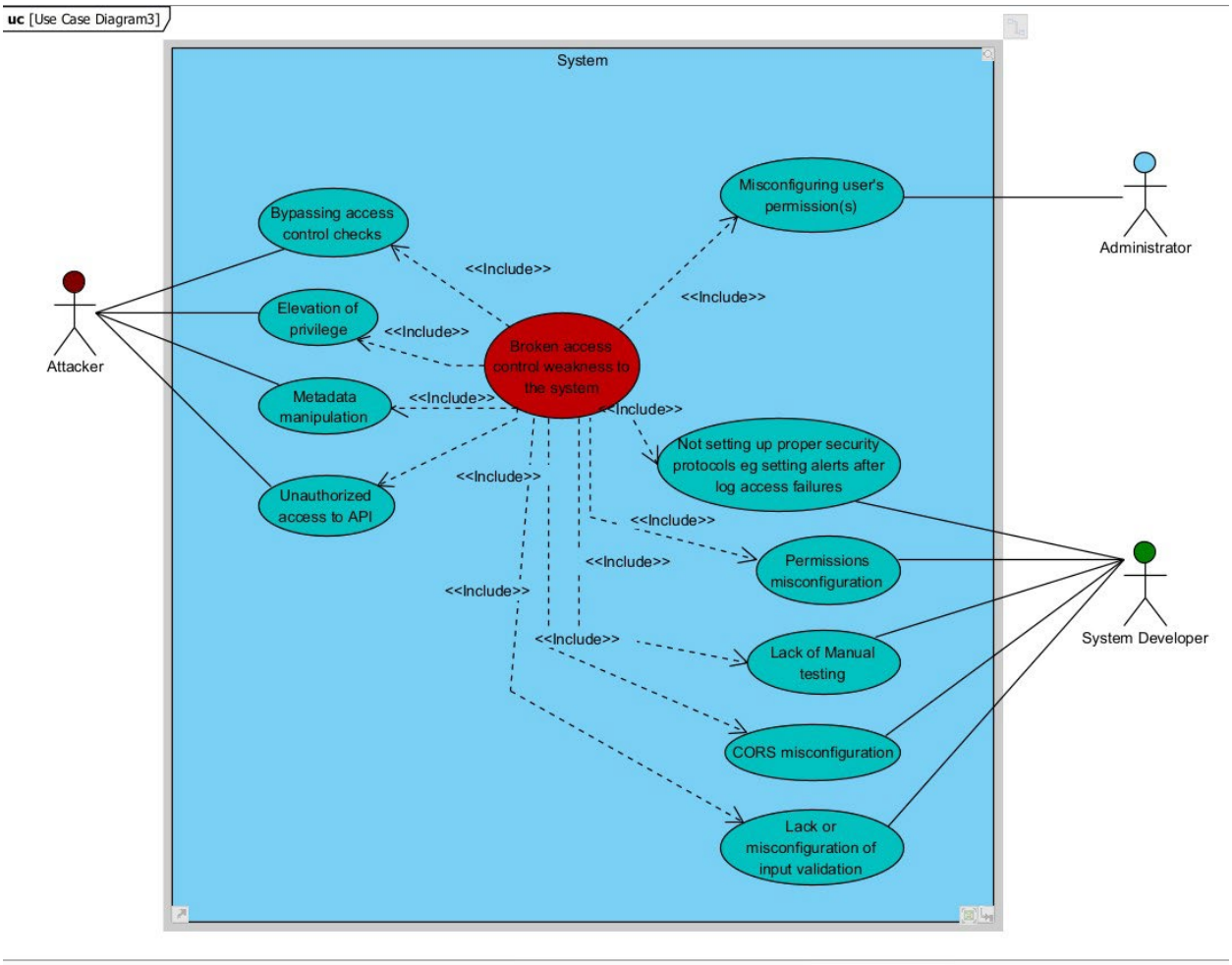
The Open Web Application Security Project (OWASP) is an online community that enables organizations to develop, purchase, and maintain secure applications and APIs by providing free and open methodologies, tools, documentation, cheat sheets, technologies, etc. (Anon, 2017).

As from (Anon, 2017), Broken Access Control is one of the OWASP top 10 most critical Web Application Security Risks (2017) (placed in category A5).

Before a user get access to a feature, some web applications check the user's access so as to control access, however, if requests are not checked, attackers will be able to gain access to features and even servers without the proper permission(s) (Fredj, et al., 2021)

(Anon, 2017) further describes that one of the common causes of this weakness been due to the lack of automated detection and effective functional testing by application developers. Therefore, manual testing is necessary and the most effective way to detect missing or ineffective access control.

Below is a use case diagram that shows some of the possible causes that may have led to occurrence of a broken access control.



Other than the use case diagram shown above, (which has been created with the use of one of the Open-source tools, Visual Paradigm), UML diagrams such as: sequence diagrams and activity diagrams, can give a more in-depth graphical description of this attack due to their ability to show interaction of operations or processes and show dynamic aspects of a system respectively.

References

Anon, 2017. *OWASP Top 10 - 2017.* [Online]
Available at: https://owasp.org/www-pdf-archive/OWASP_Top_10-2017_%28en%29.pdf.pdf
[Accessed 28 November 2022].

Fredj, O. B., Cheikhrouhou, O. & Krichen, M., 2021. *An OWASP Top Ten Driven Survey on Web Application Protection Methods.* s.l., Springer, Cham, pp. 235-252.