Collaborative Discussion 1

Topic: Select one of the coding weaknesses which have been identified by OWASP and create a flowchart of the steps which may have led to the weakness occurring.

According to the Top 10 Web application Security risks as of 2021, Cross-Site Scripting (XSS) has been brought under the Injection category as one of the Top 10 security risks (OWASP, 2021). XSS is a form of injection in which a Bad Actor will send a malicious script, under the guise of a trusted source, to a user which will then be displayed by their browser. The consequences of XSS can range from stealing cookie data, personal information, or hijacking sessions to take control of the user accounts (Rodriguez et al. ,2020)

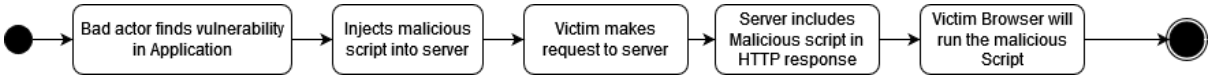
There are multiple types of XSS:

Reflected XSS (non-persistent): The malicious input is returned immediately by the vulnerable application through a HTTP response.

Stored XSS (persistent): The malicious input is stored in the server and sent to the victim when requested.

DOM based XSS: The malicious source is within the DOM (Document Object Model) and does not depend on the server to be embedded in the response (Klein, 2005).

For the purposes of this exercise, I have illustrated the Stored (Persistent) XSS in the flowchart below:



References

OWASP (2021) OWASP Top Ten. Available from: https://owasp.org/www-project-top-ten/ [Accessed: 23/10/22]

Rodriguez, G., Torres, J., Flores, P. & Benavides, D. (2020) Cross-site scripting (XSS) attacks and mitigation: A Survey. *Computer Networks* 166

Klein, A. (2005) DOM Based Cross Site Scripting or XSS of the Third Kind - WASC article. Available from: http://www.webappsec.org/projects/articles/071105.shtml [Accessed: 23/10/22]