Collaborative Discussion – Michael Geiger – Initial Post

A number of UML models can be used to visualize the threat and the process of a Cross-Site Scripting (XSS) attack. The flowchart below offers the possibility of dividing the process of such an attack into instances and showing the respective possible courses. The advantage of this type of representation lies in the simple visualization and comprehensibility for new and non-cyber security specialists (Hooshyar et al., 2015). In addition, both courses, the case of a successful attack as well as an unsuccessful one, can be displayed.

Abuse-case models represent further display options for drawing attention to a XSS threat and its dangers. In this way, recommended behavior or avoidance strategies can be easily displayed for users without having to go into the technical aspects behind them (Okubo et al., 2009).

Another useful display option for this type of attack are sequence diagrams. These offer the advantage that the affected entities, such as the victim's web browser and the affected website from which the XSS originates, can be broken down as separate entities and thus the entities involved Parties and the respective participation in the attack can be visualized.

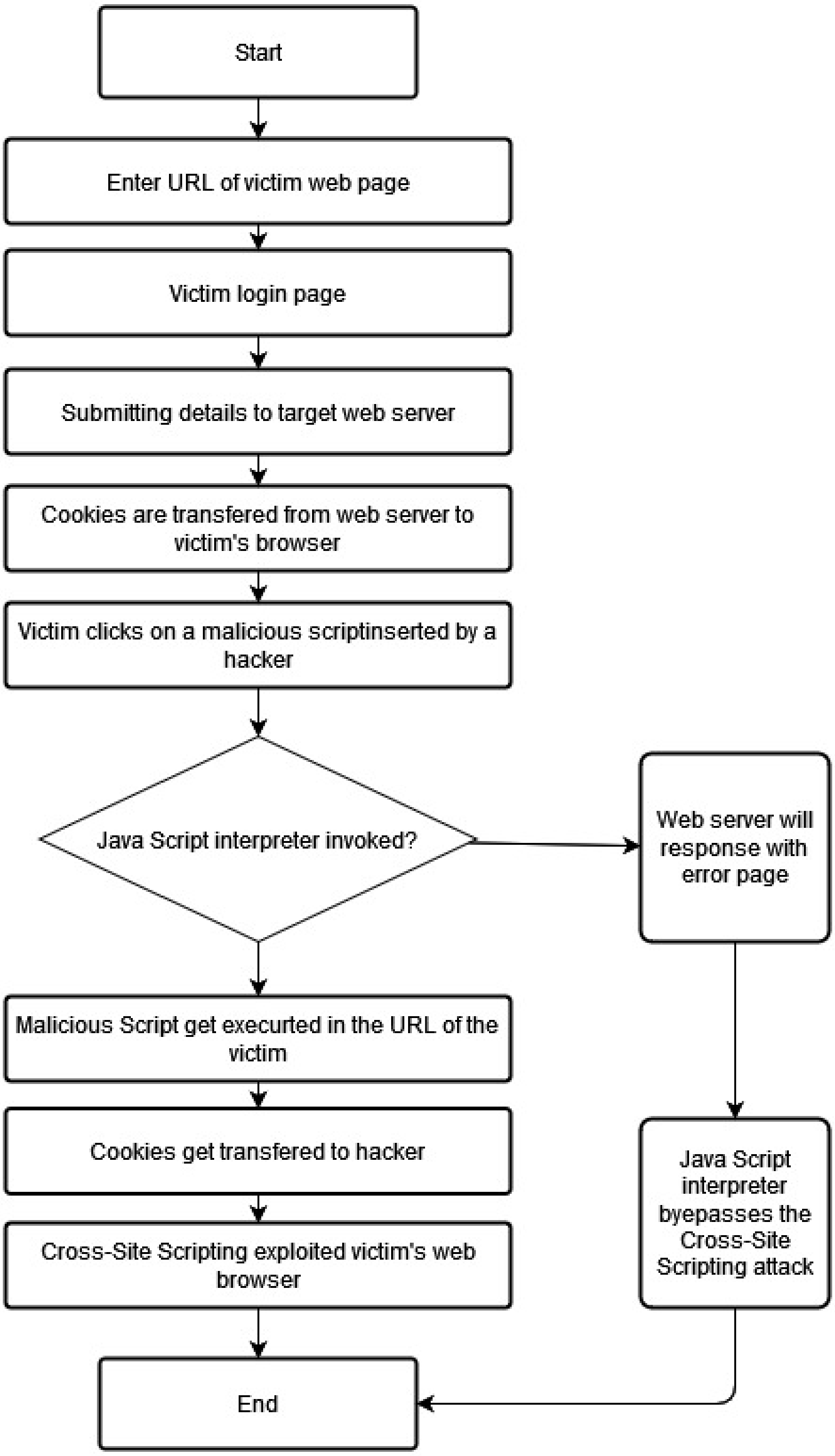
When looking at the model types, it is noticeable that flowcharts, like sequence diagrams, offer similar display options with regard to XSS attacks, but set different priorities. While the flowchart focuses on the course of the attack, the actors and instances involved can be highlighted with a sequence diagram.

It can therefore be concluded that, depending on who a UML diagram is addressed to, different forms of representation are preferred in order to visualize the information to be conveyed.

References:

Hooshyar, D., Ahmad, R., Yousefi, M., Yusop,F. & Horng, J. (2015) A flowchart-based intelligent tutoring system for improving problem-solving skills of novice programmers. Journal of Ccomputer Assisted Leraning. 31: 345-361. Available from: https://onlinelibrary.wiley.com/doi/epdf/10.1111/jcal.12099?saml_referrer [Accessed 10 March 2022].

Okubo, T., Taguchi, K. & Yoshioka, N. (2009) Misuse Cases + Assets + Security Goals. International Conference on Computational Science and Engineering. 424-429. Available from: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5283205 [Accessed 10 March 2022].


Start
Enter URL of victim web page
Victim login page
Submitting details to target web server
Cookies are transfered from web server to victim's browser
Victim clicks on a malicious scriptinserted by a hacker
Java Script interpreter invoked?
Web server will response with error page
Malicious Script get execurted in the URL of the victim
Cookies get transfered to hacker
Cross-Site Scripting exploited victim's web browser
Java Script interpreter byepasses the Cross-Site Scripting attack
End