ENPM 809W – Introduction to Secure Software Engineering

Homework 5

Date Due: November 9th, 2021, by 11:59 PM EST.

Please read the journal article attached in this week's (Week 10) module on 'JAW: Studying Client-Side CSRF with Hybrid Property Graphs and Declarative Traversals' and answer the following questions.

1. The paper suggests that CSRF vulnerabilities still abound despite the protection mechanisms that are currently available. True or False.
2. The paper references Code Property Graphs or CPGs, which assume that transfer of control only happens via function calls. However, in Javascript, transfer of control also happen via events from the environment (for example, mouse-events or user-defined events. The paper references Listing 1 here. Which line(s) of Listing 1 shows this?
3. As per the paper, a Code Property Graph is a combination of which three representations of the C source code?
4. What is the paper trying to do with the PDG, CFG, IPCG, and ERDDG for detecting client CSRF?
5. How do the authors handle third party libraries for doing what is being done in Question 4 above?
6. What inputs does JAW take for performing the client side CSRF analysis?
7. The JAW analysis also reports False Positives (where JAW says there is a potential CSRF possible, but it is not). True or False.
8. The authors of JAW identified 9 applications that allow an attacker to modify the URL domain making it possible to do cross-origin requests. Are the authors assuming that CORS is enabled for the web application? Yes or No? Why?
9. The authors point out that the client-side CSRF attacks also enable other kinds of attacks. What are those attacks?
10. As per the authors, how many percentage of application was the attacker able to overwrite a parameter in the request body to perform the client-side request forgery?