CSE 484 In-section Worksheet #7

Q1. In Lab2, the `codered.cs` server automatically loads your malicious pages. This won't necessarily be the case in real exploits. How might an attacker compel a user to load a malicious page or, more generally, do some action that triggers malicious results?

Q2. Besides location, what other user-released data might an attacker attempt to access?

Q3. What is another web-based attack that might compel a user to release data?

Q4. What are the ethics of clickjacking? At what point do we put the burden of responsibility on the user? Should browsers try to prevent against this?

Q5. What are some defenses that a browser might use to defend against clickjacking?