**Worksheet Questions**

1. These days, most of the websites use HTTPS, instead of HTTP. Do we still need to worry about CSRF attacks?

2. The forged HTTP request against Elgg in this chapter needs Boby’s user id (guid) to work properly. If Alice targets Boby specifically, before the attack, she needs to find ways to get Boby’s user id. Alice does not know Boby’s Elgg password, so she cannot log into Boby’s account to get the information. Please describe how Alice can find out Boby’s user id.

3. If Alice would like to launch the attack on anybody who visits her malicious web page. In this case, she does not know who is visiting the web page before hand. (1) Can she still launch a CSRF attack to modify the victim’s Elgg profile? Please explain. (2) Can she launch a CSRF attack to add her to the victim’s friend list? Please explain.

4. Do browsers know whether an HTTP request is cross-site or not?

5. Do servers know whether an HTTP request is cross-site or not?

6. What is the main difference between XSS and CSRF attacks?

7. Can the secret token countermeasure be used to defeat XSS attacks?

8. Can the same-site cookie countermeasure for CSRF attacks be used to defeat XSS attacks?

9. To defeat XSS attacks, a developer decides to implement filtering on the browser side. Basically, the developer plans to add JavaScript code on each page, so before data are sent to the server, it filters out any JavaScript code contained inside the data. Let’s assume that the filtering logic can be made perfect. Can this approach prevent XSS attacks?

10. Can CSP (Content Security Policy) be used to defeat CSRF attacks? Why or why not?