ISEC 400 Homework 8 Name: Megan Leonard

Answer the following questions based on your reading of the textbooks, any supplemental material, and the instructor’s presentation this week. If you use an external source (i.e. a web page, the required textbook, or an additional book) to help you answer the questions then be sure to cite that source. Hint: you should probably always be citing a source.

## Questions

1. **[5 points]** Explain, in your own words, the vulnerabilities that lead to successful XSS attacks and what methods can be applied to prevent them.

The vulnerabilities that lead to a successful XSS attack are when information is kept client side or scripts can be entered client side and are able to interact with the server. The best ways to prevent these attacks are to use cookies and to not allow input commands that contain html code or JavaScript.

1. **[5 points]** Explain, in your own words, the vulnerabilities that lead to successful CSRF attacks and what methods can be applied to prevent them.

Vulnerabilities that lead to successful CSRF attacks are usually the authorization based on cookies and accepting get methods written client side. The methods that can be used to prevent this are using cookies with another form of authentication or just using the session id as the token.

1. **[5 points]** Explain, in your own words, the vulnerabilities that lead to successful reflection attacks and what methods can be applied to prevent them.

The vulnerabilities here are allowing access to the html and letting the client side add script into it and send cookies to the alternative path or allow the addition of cookies. The best way to protect against this is to use session cookies and authentication.

1. **[5 points]** The claim was made that a nonce can be used to prevent the “double submission” problem in web applications. What is a nonce? What is the double submission problem and how can a server can detect and prevent it with a nonce?

A nonce is a hidden stored number that is set for the specific user id as a means of authentication. The double submission problem is when a submit can be clicked twice which ends up sending the submitted information twice. The nonce can protect against this by creating a number that is saved and used to make check the submit meaning that if it is submitted once, it sees there is no match for its number and updates or saves with the submit and upon the second submit, it sees that there is already an entry with its number and prevents any updating.

1. **[5 points]** What are the advantages and disadvantages to using an alternative markup syntax for text formatting in web applications (e.g. wiki syntax, Markdown, Textile, or reStructuredText)

Advantages of alternative markup syntax are the speed and simplicity of the syntax. The disadvantages are that it is not dynamic and can be easy to get through or alter such with XSS attacks.

1. **[5 points]** In approximately 300 to 400 of prose (i.e. sentences, not bullet lists) using APA style citations if needed, summarize and interact with the content that was covered this week in class. In your summary, you should highlight the major topics, theories, practices, and knowledge that were covered. Your summary should also interact with the material through personal observations, reflections, and applications to the field of study. In particular, highlight what surprised, enlightened, or otherwise engaged you. Make sure to include at least one thing that you’re still confused about. In other words, you should think and write critically not just about what was presented but also what you have learned through the session. Ask at least one question that your instructor can answer in the returned assignment or class discussion.

This week we went over client side manipulation and how we can prevent against these attacks. This is not a new topic to me but some of the parts are expanded prior to what I learned such as the different types of XSS. Nonce is a new term that I can see coming up again as it seems very useful with protecting against CSRF and double submits. Double submits are one of those things that are quite common so having a way to stop it would be very useful. My question for this week is when it comes to different client-side attacks, which one do you find the easiest to handle and which one is the hardest to handle?

Citation:

Whittaker, T., &amp; Whitney, T. (2022). Week08 Power Point. Retrieved March 19, 2023, from <https://franklin.instructure.com/courses/11070/files/1516722?module_item_id=623555>