ISEC 400 Homework 7 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]** Watch the talk from AppSec USA 2012 called “[The Same-Origin Saga](https://www.youtube.com/watch?v=Nd3srHK3K2A)” given by Brendan Eich (the author of JavaScript). Ignoring much of the developer jargon, summarize why and how Mr. Eich implemented same origin and what issues were subsequently discovered.

The reason that Mr. Eich gave for implementing same-origin is to protect against untrusted sites while helping the relation between user/website. They started by implementing a same origin check within the URL but found the issues that you couldn’t just label everything with origin. Now they are implementing the same origin back where you cannot touch it from the outside.

1. **[5 points]** Watch the talk from AppSec USA 2012 called “[Origin(al) Sins](https://www.youtube.com/watch?v=97uk0FYxk-Q)” given by Alex Russell of Google. Again, ignoring much of the developer jargon, summarize the fundamental issues of browser security and how Google is attempting to address them.

The problem with browsers was that the user had to be given full permissions to access them and that gave full permissions to the set of authenticated sessions which is why they addressed this problem with adding session tokens. There is a lot of different behaviors of the browser so they are working on a way to be able to turn the behavior off like inline scripts and URL requests.

1. **[5 points]** Watch the talk from AppSec USA 2012 called “[Securing JavaScript](https://www.youtube.com/watch?v=T6TTQoqln7c)” given by Douglas Crockford author of JSON and JSLint. Again, ignoring much of the developer jargon, discuss the difficulty of writing secure JavaScript.

The difficulty of writing secure JavaScript is that there are a lot of chances of XSS attacks and that the websites use a lot of different languages together so they need to be able to work with other languages without conflict. It also does not any type of linker so all of the scripts it makes end up in the common global space where they have to run against the other programs and scripts.

1. **[5 points]** Explain the problems associated with using hidden form fields for keeping session state? How did keeping a session ID embedded in a hidden form field improve (or not) on the first idea?

Every page needs a level of complexity to maintain data without problems. It also is maintained on the server side with only text being used. It has improved by providing better security and the ability to share resources without problems.

1. **[5 points]** Another approach to session state was to use a HMAC to authenticate the data kept in hidden form fields. Explain how HMACs work and how and why they are considered secure. Contrast that with the solution that keeps state on the server and accessed by browser cookies.

HMAC executes a cryptographic hash function to be authenticated. They are considered more secure as they give a layer of security with the encryption and the need for a secret key. The cookies keep information stored where it is harder to reach on the one side while the HMACs can be attacked by using brute force.

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 the same origin policy where pages can only connect with other pages that match the port numbers, domains, and protocols as a means of securing cookies and protecting the user from accessing untrustworthy sites. It also can be used to affect scripts to keep from loading any strange third-party scripts. My question for the week is there a time when the header should be allowed more access? This is like how you need to keep important information out of the header and make sure that it can not be altered with added code to give the person access where they should not be. So, is there a time when this would be allowed without causing more security risk?

Citation:

aLoneStrideraLoneStrider 17311 gold badge55 silver badges1313 bronze badges, SilverlightFoxSilverlightFox 32k1111 gold badges7474 silver badges146146 bronze badges, & SherifSherif 11.7k33 gold badges3232 silver badges5757 bronze badges. (1962, March 1). *Session ID placement: Form hidden field vs. httponly cookie*. Stack Overflow. Retrieved March 13, 2023, from <https://stackoverflow.com/questions/30012422/session-id-placement-form-hidden-field-vs-httponly-cookie>

GeeksforGeeks. (2021, August 31). *What is hmac(hash based message authentication code)?* GeeksforGeeks. Retrieved March 13, 2023, from <https://www.geeksforgeeks.org/what-is-hmachash-based-message-authentication-code/>

Villanueva, J. C. (n.d.). *What is HMAC and how does it secure file transfers?* JSCAPE. Retrieved March 13, 2023, from <https://www.jscape.com/blog/what-is-hmac-and-how-does-it-secure-file-transfers>

Whittaker, T., &amp; Whitney, T. (2022). Week07 Power Point. Retrieved March 12, 2023, from <https://franklin.instructure.com/courses/11070/files/1516721?module_item_id=623554>