ISEC 400 Homework 0 Name: Megan Leonard

Answer the following questions (normally, these are based on your reading of the textbooks, any supplemental material, and the instructor’s presentation this week, but this is due before any of that). 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. **[15 points]** Watch the keynote video for NDC Sydney, 2016 called “[50 Shades of AppSec](https://www.youtube.com/watch?v=3-Dy1GmiSoE)” by Troy Hunt (warning, some NSFW text on the screen). Summarize the speaker’s main points and critically analyze the content. What kinds of challenges do companies, users, and developers face in preventing data breaches? What was interesting, confusing, or surprising in what you saw and heard? Related to this video, what do you hope to learn from this class?

Hacking has become quite accessible and there have been applications created that help find vulnerabilities that you can exploit. The applications make it easy to gather information and you can even hire hackers. Developers have made it easier through the forgot password option and how passwords tend to be stored with the username associated with it making it easier to find. Users must also be able to protect the passwords they make as the video showed a man giving an interview, standing in front of a wall of passwords. Companies also will provide the security they use without thinking about it like saying they use Norton. I found it interesting with just how easy hacking has started to become thanks to the help of different applications and people. In my previous security classes, we looked at how to gather data from the network and databases so I hope that in this class we can see more of web side of security.

1. **[5 points]** Watch the OWASP Appsec Tutorial Series, [Episode 1: Appsec Basics](https://www.youtube.com/watch?v=CDbWvEwBBxo). Contrasting this video to the previous one, connect some of the technical details of vulnerabilities described to the examples from Troy Hunt. How is Appsec different from network security?

The main difference between the two videos are how they address the problems and how they see it happening. The 50 shades video goes over how people are hacking and then discusses user error and problems with the code. The basics video has a focus more on the code and how it works. The video focuses on developers and what they can do while the previous one looks more at hacking itself. Appsec is different from network security because of its focus being the internet and how the server connects to it as well as the website itself. Network security has a wider focus on the databases and the use of firewalls and some different hardware.

1. **[5 points]** Locate the OWASP website and browse some of the resources there. Pick one OWASP project and describe its purpose and how it fits into the context of application security.

The OWASP project I found interesting from the list is the OWASP Juice Shop. The project is made to be an insecure web application as a means of learning how different attacks work. It fits well in the context of application security as it helps people understand how the different attacks work and where they are targeted. This gives people a better idea of how to stop the attacks and which areas need more enforcing or just need to be changed. A lot of the security classes I have taken have done methods like this to teach us about the problems we will likely face.

1. **[5 points]** Summarize the security-related content from your previous web-development course (normally WEBD 236). What were some of the best practices that were discussed and why were they considered best practices?

My previous web course discussed SQL injection and how encryption works. Some practices that were discussed was authentication and how we can set up role based access control to limit the amount of access people have to different areas. There is also setting up encryption techniques like hashing to help protect stored information. There is also making sure that inputs from the web page do not allow SQL code to help prevent SQL injection.

*Owasp Juice Shop*. OWASP Juice Shop | OWASP Foundation. (n.d.). Retrieved January 25, 2023, from https://owasp.org/www-project-juice-shop/