Week 5 Reflection

This week's lectures focused on **web security and continued exploration of malicious software**, emphasizing vulnerabilities in web applications and common attack methods. Topics included a recap of malicious software, an introduction to web security, the **OWASP (Open Web Application Security Project)**, server-side and client-side attacks, and **cross-site scripting (XSS)**.

What I Learned

- The recap of **malicious software** reinforced the importance of defending systems against viruses, worms, and other malware.
- I learned the basics of **web security**, including why web applications are frequent targets for attacks.
- **OWASP** was introduced as a critical framework for understanding common web application vulnerabilities and best practices for mitigation.
- I gained insight into **server-side attacks**, where attackers exploit vulnerabilities in the backend of web applications, such as SQL injection or file inclusion.
- **Client-side attacks** were discussed, including threats to users' browsers and scripts, like XSS.
- **Cross-Site Scripting (XSS)** was explained as a method where malicious scripts are injected into trusted websites to steal information, hijack sessions, or deface content.

Challenges Faced

- Understanding the differences between **server-side and client-side attacks** and how vulnerabilities manifest in each layer required careful attention.
- Grasping the technical mechanisms of **XSS attacks** was initially complex, especially in understanding how scripts are injected and executed.

Reflection and Personal Growth

- This week highlighted that security is **not only about protecting devices or networks** but also about securing applications that interact with users.

- I realized the importance of **following OWASP guidelines** to identify, prevent, and mitigate vulnerabilities in web applications.

- The lectures emphasized that even small coding mistakes can have **serious security implications**, motivating me to adopt secure coding practices.

Next Steps

- I plan to **practice identifying vulnerabilities** using safe web application labs or environments to gain hands-on experience.

- I will explore **OWASP's top 10 vulnerabilities** in more depth to understand common patterns and mitigation techniques.

- I aim to **connect web security concepts with previous lessons on malware, authentication, and network security** to develop a comprehensive approach to cybersecurity.