1. Provide well-written, precise definitions of the following terms, each in ten words or less.
2. Risk –the likelihood of a problem occurring multiplied by the severity of its impact
3. Threat – a potential attack from either unauthorized outsiders or the program itself
4. Defect – problem with a program that jeopardizes the security or functionality of the program
5. Flaw – defect in the design of the program
6. Bug – defect in the code of the program
7. Vulnerability – defect that can be exploited by unauthorized outsiders
8. Weakness – an imperfection in software code, design, architecture, or deployment that could become a vulnerability or lead to creating vulnerabilities
9. Failure – when a program does not do what it was intended to
10. Exploit – code or data made by unauthorized outsiders to attack a system through a vulnerability
11. Integrity – the property that describes whether a component of a system has not been modified or destroyed in an unauthorized manner
12. Authentication – process of verifying the identity of an external entity, user, process, or device
13. Authorization – process of determining whether a subject is allowed to have access to a specified resource
14. Give the titles and complete URLs of the five Tom Scott security-related videos you watched (to completion), together with a sentence or two on the purpose or lesson of each video. Make sure the purpose or lesson is accurate and truly central to the video.
15. [From Missingno to Heartbleed: Buffer Exploits and Buffer Overflows](https://www.youtube.com/watch?v=rE5dW3BTpn4)

Tom Scott explains what a Buffer Overflow/Underflow Attack is and gives the Heartbleed OpenSSL attack as an example.

1. [How The Self-Retweeting Tweet Worked: Cross-Site Scripting (XSS) and Twitter](https://www.youtube.com/watch?v=zv0kZKC6GAM)   
   The lesson in this video is that secure software developers should never give back any input without first validating and filtering the input content.
2. [The Attack That Could Disrupt The Whole Internet - Computerphile](https://www.youtube.com/watch?v=BcDZS7iYNsA)  
   He explains what distributed denial of service (DDOS) attacks are and how they are used to shut down a company’s internet service for ransom.
3. [Cross Site Request Forgery - Computerphile](https://www.youtube.com/watch?v=vRBihr41JTo)
4. [The Shellshock Bug In About Four Minutes](https://www.youtube.com/watch?v=aKShnpOXqn0)
5. A one-paragraph summary of each of the following (you might have to do research outside the assigned reading): Heartbleed, XSS, Billion-Laughs, CSRF. Hit on both the impact of each (economic, societal) and be very precise in your technical explanations. Where relevant, use actual quantities. Pictures are nice but not required. Make your summaries understandable to undergraduate computer science students in their second year. Chatbots might be helpful here, but understand what they say and, if they get way too wordy, clean up their output and put things into your own words.
6. Heartbleed
7. XSS
8. Billion-Laughs
9. CSRF
10. [GitHub Link](https://github.com/Ulq15/CMSI662_Secure_Software_Development/tree/main/HW1)   
    [Repl Link](https://replit.com/@HassanUlq/CMSI-662-HW-1)