Read Larson (2018) and Weidman (n.d.) then answer the questions below, adding them as evidence to your **e-portfolio**. You may want to complete this activity in conjunction with or after completing Seminar 2 preparation.

1. What is ReDOS and what part do ‘Evil Regex’ play?
2. What are the common problems associated with the use of regex? How can these be mitigated?
3. How and why could regex be used as part of a security solution?

**Answer:**

1. ReDOS stands for (Regular expression Denial of Service). A denial of service is when an attacker floods a machine or a network with requests that take a long time to process and either freezes the machine from doing any other work or crashes the machine or network (*What is a denial of service attack (dos) ?*). ReDOS is a type of Denial of Service that uses regex or Regular expressions. ReDOS uses evil Regex or regular expressions that take a very long time to process and in doing so crashes the machine or cause the system to hang for a long time.
2. There are many problems that can happen with regular expressions such as incorrect use of the wildcard, bad range, incorrect use of character set and more. The way to prevent these kind of issues is by using Regex tools that are readily available online such as regex101.com.
3. Regex is an extremely useful and power tool which helps the application check if a password pattern is correct or if a username or email address are typed correctly.

References:

read, 3min. *What is a denial of service attack (dos) ?*, *Palo Alto Networks*. Palo Alto Networks. Available at: https://www.paloaltonetworks.com/cyberpedia/what-is-a-denial-of-service-attack-dos#:~:text=A%20Denial%2Dof%2DService%20(,information%20that%20triggers%20a%20crash. (Accessed: December 11, 2022).