<center>04-30-2024</center>

What is the OWASP Top 10:

- The OWASP Top 10 is a list of the most common attack methods attackers might initiate to compromise a web server. The current top five is:
  - **Broken Access Control**
    * Methods with which attackers can use to perform actions outside of the intended permissions.
  - **Cryptographic Failures**
    * Old/weak cryptographic algorithms, lack of encryption, no digital certificates
  - **Injection**
    * Lack of input sanitization, attackers can utilize SQL inputs to manipulate data or retrieve data from a server.
  - **Insecure Design**
    * Pretty general attack method. Stems from bad infrastructure design by things like having a single point of failure, prioritizing high availability over security.
  - **Security Misconfiguration**
    * Lack of authentication methods, zero hardening, no error handling.

What is a Common Weakness Enumeration (CWE):

- Common Weakness Enumeration is a categorized system for weaknesses and vulnerabilities in hardware and software programs. The current top 10 >?/

What is the correlation between the two