COMP307   Assignment 7

Instructions

Work in teams of maximum four students. Read the sample documents

Marks

This assignment is marked out of 10

- Read the materials from eCentennial:
    - OWASP Dev Guide,
    - OWASP Code Review Guide and
    - OWASP Testing Guide.
- Review the SAMM framework in the document SAMM_Core_V1-5_FINAL.pdf
- Once you finish reading the materials please answer the following questions:

1) What are some guidelines for handling credit cards on websites?

2) What are some known data validation strategies?

3) When should the testing process be introduced in the SDLC?

4) What is black-box testing?

5) What are some basic practices for handling authentication in web apps?

6) Identify and describe the four maturity levels for security practice of OpenSAMM.

7) What are some activities an organization could perform for the security practice of "Threat Assessment"?

8) What are the two recommended assessment styles for SAMM and how are they used?

Submit in dropbox. Class discussions (time permitting).