Web Securities

True or False

1. Sensitive Data Exposure most likely occurs when an application does not have a proper protect sensitive information.

* True

1. To prevent sensitive data exposure, the data should never be placed in a text that is very clear.

* True

1. Injection is the most popular or the number one list on OWASP.

– True

1. Broken Description will include all types of flaws which are mostly caused by some errors in implementing a management session.

* False

1. Security Misconfiguration is a type, or a component is very susceptible to a configuration that has many insecurities and is being classified as a protector or as a security that leads to a misconfiguration.

-true

6. Cross-Site Scripting is yet another kind of an attack being done, that can be tag along or carried out on compromised people or the users of a website.

-True

7. Insufficient Logging and Monitoring, instead of having no vulnerabilities.

- False

8. The XML External Entity (XXE) Attack is considered to be not a type of server-side request forgery.

- False

9. Insecure Deserialization is a vulnerability which usually happens when a trusted data is being processed or is being used for the misused of the applications logic.

-False

10. To prevent Insecure Deserialization, you must not accept those objects that are serialized.

-True