Priscilla Botugueno 1022723

Q1) most common Website Security Vulnerabilities

1) SQL Injections

SQL Injections is a type of web application security vulnerability in which an attacker attempts to use application code to access or corrupt database content.
If successful, this allows the attacker to create read, update, alter or delete data stored in back-end database.

2) Cross Site Scripting (XSS)

It targets on application's users by injecting code, usually a client-side script such as Java Script, into a web application's output.
The concept of XSS is to manipulate client-side scripts of a web application to execute in the manner desired by the attacker.

3) Broken Authentication & Session Management.

Broken Authentication encompass several security issues, all of them having to do with maintaining the identity of a user.
If authentication credentials and sessions identifiers are not protected at all times, an attacker can hijack an active session.

4) Insecure Direct object References

It is when a web application exposes a reference to an internal implementation object.
Internal implementation object includes files, database records, directories and database keys.

5) Security misconfiguration

It encompasses several types of vulnerabilities all centered on lack of absence to the web application configuration. A secure configuration must be defined and deployed for the application server, web server, database server and platform.