Ans ① SQL INJECTIONS

Sql injection is a type of web application security vulnerability in which an attacker attempts to used application code to a cross or corrupt database content. If successful, this allows the attacker to create, read, update, alter or delete data stored in the back end database.

② CROSS SITE SCRIPTING (XSS)

Cross-site scripting (XSS) targets an application's user by injecting code, usually a client side script such as Javascript, 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 and session management encompass several security issues, all of them having to do with maintaining the identity of a user. If authentication credentials and session identifiers are not protected at all times.

④ Insecure direct object References

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

⑤ Security misconfiguration

Security misconfiguration encompasses several type of vulnerabilities all centered on a lack of maintenance or a lack of attention to the web application configuration. A secure configuration must be defined and deployed for the application

...work, application server, web server, database layer and platform.

(6) CROSS-SITE REQUEST FORGERY (CSRF)

Cross-site Request forgery (CSRF) is a malicious attack where a user is tricked into performing an action he or she didn't intend to do. A third-party website will send a request to a web application that a user is already authenticated against (eg their bank)