

Name - Aditya Sen
Rollno - 1022715/05

Ques-1

Most common website security vulnerability

- ① SQL injections - It is a type of web application security vulnerability in which an attacker attempts to use application code to access or corrupt database content.
- ② Cross site scripting - It targets an application users by injecting code, usually a client-side script such as Java-script into a web application to execute in the manner desired by the attacker.
- ③ Broken Authentication and session management - It encompasses several security issues, all of them having to do with maintaining the identity of a user. If authentication credentials & sessions identifications are not protected at all times, an attacker can hijack an active session of anyone the identity of a user.
- ④ Insecure direct object references:- It is when a web application exposes a reference to an internal implementation object. When an application exposes a reference to one of these objects in URL hackers.
- ⑤ Security Misconfiguration:- Encompasses several type of vulnerability all centered on a lack of attention to the web application configuration. Security misconfiguration gives hackers access to private data or features.

Aditya Sen