Kriti Thakur
Roll no. 29
18512102

Ans)

① SQL INJECTIONS

SQL injection is a type of web applications security vulnerability in which an attack attempt to use application code to acces or corrupt database content.

② CROSS SITE SCRIPTING (XSS)

Cross-site scripting (xss) targets an applicati-on's users by injecting code, usually a client-side script such as JavaScripts, into a web application's output. The concept of XSS is to manipulate client-side scripts of web application to excute in the manner desire by the attacker.

③ BROKEN AUTHETICATION & SESSION MANGEMENT

Broke automcation and session mengment

encpass several security issues, all of them having to do with maintaing the identity of a user.

(4) INSECURE DIRECT OJECT REFERENCE

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

(5) SECURITY MISCONFIGURATION

It is a type of vulnarabilities all centered on a lack of maintance or a lack of attention to the web application configuration.

A Secure configuration must be defined and diploid for the application frame works, application server, web Servers, Database Secure & platforms.

(6) CROSS-SITE REQUST FORGURY (CSRF)

AGROHA

Date / /

Page No.

CSRF is a malicalous attack where a user is trigged into performing & action. he or she dont intend to todo. A third party website will send a request to a web application that the users is already authenticated against their Bank.