Shivansh Tiwari
18A91004
1022763
Assignment of information security & cyber laws

Shivansh

Q1
Ans vulnerabilities

(i) SQL Injections

- sql injection 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 the back end database.

(ii) Cross site scripting (XSS)

(XSS) targets an application's users 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.

iii) Broken Authentication & Session Management

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

iv) Insecure Direct Object Reference.

Insecure direct object reference is when a web application exposes a reference to an internal implementation object. Internal implementation objects include files, database records, directories and database keys. When an application exposes a reference to one of the objects in a URL, or hidden parameter. It is possible to gain access to a user personal data.

v) Security Misconfiguration

Security misconfiguration encompasses several types of vulnerabilities all centered on a lack of maintenance or a lack of attention to the web application configuration [redacted]

vii) 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.