Name - ASEEM SONI Course - B.Sc(IT) 6th Sem
Subject - Information Security Univ Roll no - 1022775

Q1 SQL Injections

In this 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

Cross Site Scripting (XSS)

In this an application's users are targeted by injecting code, usually a client side-script such as JavaScript, into a web applications output. This results in manipulation of client-side scripts of a web application to execute the manner desired by the attacker.

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, an attacker can hijack an active session and assume the identity of a user.

Insecure Direct Object References

Insecure direct object reference is when a web application exposes a reference to an internal implementation object which includes files, database records, database keys and directories. When an application ~~can access~~ exposes a reference to one of these objects in a URL, hackers can manipulate it to gain access to a user's personal data

Security Misconfiguration

It includes several vulnerabilities all centered on a lack of maintenance or a lack of attention to the web application configuration. Security misconfiguration gives hackers access to private data or features and can result in a complete system compromise.

Cross-Site Request Forgery

In this attack a user is tricked into performing an action he didn't intend to do. A third party website sends a web request to a web app that a user is already authenticated against. The attacker can then access functionality via the victim's already authenticated browser