Name - Ajay Goswami

Rollno - 1022716106)

Ajay

(Que 1) Study the different type of vulnerability for hacking a web application.

(Ans) The most common web application security vulnerabilities are as follow:-

(1) SQL Injections:-

SQL injections 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 attacker to create, read, update, alter or delete data stored in backend database.

(2) Cross site scripting (XSS):-

Cross-site scripting (XSS) targets an application's users by injecting code, usually a client-side script such as Javascript, into a web application output. The concept of XSS is to manipulate client-side script of a web application to execute in the manner desired by the attacker

Name- Ajay Goswami Rollno-1022716(06)

Course- B.SC(I.T) 6th sem

(3) Broken authentication & session management!-

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

(4) Insecure Direct Object References!-

Insecure-direct object reference is when a web application exposes a refernce to an ~~wok~~ internal implementation object. Internal implementation objects include files, database, records, directories & database keys when an application exposes a refernce to one of these objects in a URL, hackers can manipulate it to gain access to user's data.

(5) security Misconfiguration!-

It encompasses several types of vulnerability all centered on a lack of maintenance or a lack of attention to the web application configuration, A secure configuration must be

Name-Ajay Goswami

Rollno - 1022716(06)

Ajay

defined & deployed for the application frameworks. security Misconfiguration gives hackers access to private data of features & can result in a complete system compromise.

(6) Cross site Request forgery (CSRF)

- It is a malicious attack where a user is tricked into performing an action he or she did'nt intend to do. A third party web cite will send a request to a web application that a user is already authenticated against (e.g. Her bank) the attacker can then access functionality via victim's already authenticated browser.