Name: POONAM
University Roll No: 1022748 (38)

Q1. Study the ------ ---------- application.

Ans:- The different types of vulnerabilities which can lend a helping hand to hackers for hacking a website or web application are as follows:-

1: SQL Injection:

⇒ It is a kind of code injection attacks. The hacker in a code injection attack inserts a piece of code in a computer program.
An attacker first of all finds an input to include it in an SQL query. The attaker than inserts the malicious payload which is included in that query and executed by the server. Now, the attacker can create, read, update, alter and delete records maintained in the database.

2. Broken authentication and session management:

⇒ Incorrect implementation of functionality related to session management and authentication can result in these type of website vulnerabilities. Exploiting this vulnerability, an attacker can thieve session IDs or passwords.

3. Cross Site Scripting (XSS):

⇒ In this attack, the browser is targeted indirec When the victim visits the infected page, the malicious JavaScript code is delivered to the browser. Once this malicious code is executed,

Poonam

the attacker can access objects like cookies.

4. Insecure direct object reference:

⇒ Attacker exploiting this vulnerability is an authorized user having limited privileges. By changing parameter value directly referring to that object, the user can gain access the object.

5. Wrong Security Configuration:

⇒ An attacker can easily enjoy the privileges of the admin if you stick with the default configurations like using default username and password.

6. Cross Site Request Forgery (CSRF):

⇒ In this kind of attack, the attacker tricks an authorized user of a website to perform an unwanted action like change password, transfer funds etc and the victim does not unknowingly sends a malicious request to a trusted website.

7. Remote Code Execution:

→ The attacker can retrieve or alter the information stored in the server.

8. Username Enumeration:

⇒ Apart from login page, the attacker can also make attempts on registration, change password and forget password page. This vulnerability exists in applications displaying an error message to tell if the username is valid or not.

Poonam