Task-5

Web Server Vulnerabilities

1.Cross-Site Request Forgery (CSRF):

Attackers trick users into performing actions on a web application without their consent, often leading to unauthorized operations.

2.Server-Side Request Forgery (SSRF):

Attackers manipulate a web server into making requests to internal resources, potentially exposing sensitive data or services.

3.File Inclusion Vulnerabilities:

Remote File Inclusion (RFI):

Attackers include external files on a web server, potentially executing malicious code.

Local File Inclusion (LFI):

Attackers exploit the inclusion of local files to gain unauthorized access or retrieve sensitive data.

4.Security Misconfigurations:

Poorly configured web servers might expose sensitive information, directories, or unnecessary services, providing attackers with potential entry points.

5.Brute Force Attacks:

Attackers attempt to guess usernames and passwords to gain unauthorized access to the web server or applications.

6.Remote Code Execution (RCE):

Attackers exploit vulnerabilities to execute arbitrary code on the server, gaining full control.

7.Insecure Deserialization:

Attackers exploit flaws in the deserialization process to execute arbitrary code or cause unexpected behaviour.

8.HTTP Header Vulnerabilities:

Insecure or misconfigured HTTP headers can lead to security issues such as information leakage or cross-site scripting.

9.Unvalidated Input:

Failure to validate and sanitize user inputs can lead to various vulnerabilities, including injection attacks.

10.Insecure Dependencies:

Using outdated or vulnerable third-party libraries and components can expose web servers to known exploits.