Niraianbu porchezhian
21BCE0965
Task 5

Task-5

EXPLAIN ANY 10 WEB SERVER ATTACKS

1. SQL Injection (SQLi):

- Description: SQL Injection, often referred to as SQLi, is an attack where malicious SQL queries are injected into input fields or URL parameters. This exploits vulnerabilities in insufficient input validation, potentially leading to unauthorized access, data theft, or database manipulation.

2. Cross-Site Scripting (XSS):

- Description: Cross-Site Scripting (XSS) attacks involve the injection of malicious scripts into web pages. When other users view these pages, their browsers execute the injected scripts, enabling attackers to steal cookies, hijack sessions, or deface websites.

3. Cross-Site Request Forgery (CSRF):

- Description: CSRF attacks deceive authenticated users into unknowingly executing unwanted actions on a different site. Exploiting trust between users and vulnerable websites, attackers can manipulate settings, make unauthorized transactions, or perform actions on behalf of victims.

4. Distributed Denial of Service (DDoS):

- Description: Distributed Denial of Service (DDoS) attacks overwhelm web servers with a massive volume of traffic from various sources, rendering them unresponsive. This results in downtime, financial losses, and a poor user experience.

5. Server-Side Request Forgery (SSRF):

- Description: Server-Side Request Forgery (SSRF) attacks trick web applications into making requests to internal or external resources. Attackers can gain unauthorized access, retrieve sensitive data, or bypass firewalls using SSRF.

6. Directory Traversal:

- Description: Directory Traversal, also known as Path Traversal, permits attackers to access files and directories outside a web server's root directory by manipulating input. This can lead to unauthorized access to sensitive files.

7. Remote File Inclusion (RFI):

- Description: Remote File Inclusion (RFI) attacks involve including external files through a web server, potentially leading to arbitrary code execution. Attackers can compromise servers and execute malicious code.

8. Brute Force Attack:

- Description: Brute Force Attacks involve repeated attempts to guess usernames and passwords until the correct combination is found. Successful attacks can result in unauthorized access to user accounts or the web server itself.

9. Zero-Day Exploits:

- Description: Zero-Day Exploits target vulnerabilities in web server software or plugins that are unknown to the software vendor, allowing attackers to exploit these vulnerabilities before patches become available.

10. HTTP Response Splitting:

- Description: HTTP Response Splitting attacks manipulate the content of HTTP responses, enabling attackers to inject malicious content into web pages. This can lead to arbitrary code execution, session hijacking, or other security breaches.