TASK 3

Overview

Explain about any 10 web server attacks.

Web Server Attacks

1. Distributed Denial of Service (DDoS):

Attack: Attackers flood a web server with a massive volume of traffic, overwhelming its resources and rendering it inaccessible to legitimate users.

Impact: Service disruption, downtime, and loss of revenue.

Prevention: Implement DDoS mitigation solutions, employ rate limiting, and use content delivery networks (CDNs).

2. Brute Force Attacks:

Attack: Attackers systematically try multiple username and password combinations to gain unauthorized access to a web server.

Impact: Compromised accounts, data breaches, and unauthorized server access.

Prevention: Enforce strong password policies, implement account lockout mechanisms, and use multi-factor authentication.

3. SQL Injection:

Attack: Attackers inject malicious SQL queries into input fields, exploiting vulnerabilities in the application's database interactions.

Impact: Unauthorized data access, data manipulation, and application compromise.

Prevention: Employ input validation, use parameterized queries, and follow secure coding practices.

4. Cross-Site Scripting (XSS):

Attack: Attackers inject malicious scripts into web pages that are then executed by users' browsers.

Impact: Data theft, session hijacking, and malware distribution to site visitors.

Prevention: Implement output encoding, use Content Security Policy (CSP), and validate user input.

5. File Inclusion Vulnerabilities:

Attack: Attackers exploit insecure file inclusion mechanisms to execute arbitrary code or access sensitive files.

Impact: Unauthorized access, remote code execution, and data exposure.

Prevention: Validate user input, restrict file inclusion to known directories, and use safer alternatives.

6. Directory Traversal:

Attack: Attackers manipulate input to access files and directories outside the web server's intended path.

Impact: Unauthorized access to sensitive files, data exposure, and potential code execution.

Prevention: Implement strict input validation and employ strong access controls.

7. Server Side Request Forgery (SSRF):

Attack: Attackers trick the server into making unauthorized requests to internal resources or external services.

Impact: Access to internal systems, data exfiltration, and potential denial of service.

Prevention: Implement input validation, firewall rules, and restrict resource access.

8. Shellshock (Bash Vulnerability):

Attack: Attackers exploit a vulnerability in the Bash shell to execute arbitrary commands on the server.

Impact: Remote code execution, unauthorized access, and data compromise.

Prevention: Apply security patches and update Bash, follow secure coding practices, and employ web application firewalls.

9. Remote File Inclusion (RFI):

Attack: Attackers include files from remote servers in web applications, potentially executing malicious code.

Impact: Remote code execution, unauthorized access, and data exposure.

Prevention: Implement strict file inclusion controls, validate user input, and restrict remote file inclusion.

10. HTTP Response Splitting:

Attack: Attackers manipulate HTTP responses to inject malicious content into the response sent to clients.

Impact: Cache poisoning, session hijacking, and defacement.

Prevention: Validate user input, sanitize HTTP headers, and apply security headers.