UNIT 5

Session Hijacking

Understanding Session Hijacking:

- **Definition**: A cyber-attack where an attacker takes over an active session between a client and a server.
- **Objective**: Impersonate a user to gain unauthorized access to sensitive information or services.

How it Works:

1. **Session Tokens**: These are unique identifiers assigned to users by a server during login.
2. **Attack Methods**:
   - **Packet Sniffing**: Capturing unencrypted tokens during data transmission.
   - **Cross-Site Scripting (XSS)**: Injecting malicious scripts to steal session cookies.
   - **Session Fixation**: Forcing a user to use a specific session token.

Defensive Strategies:

1. **Encryption**: Always use HTTPS to secure data in transit.
2. **Session Management**:
   - Regenerate session IDs after each login or privilege escalation.
   - Use timeouts for inactive sessions.
3. **Secure Cookies**: Mark cookies as **HttpOnly** and **Secure** to protect against theft.
4. **Multi-Factor Authentication (MFA)**: Adds an extra layer of verification.

Web Servers and Applications

Client-Server Relationship:

- **Client**: A device (like a browser) that requests resources.
- **Server**: A machine or program that provides those resources, like web pages, data, or services.

Common Vulnerabilities:

1. **Injection Flaws**:
   - Example: SQL Injection.
   - Impact: Allows attackers to manipulate the backend database.
2. **Cross-Site Scripting (XSS)**:
   - Attackers inject malicious scripts into web pages.
   - Victims unknowingly execute these scripts in their browsers.
3. **Weak Authentication**:
   - Poor password policies.
   - Lack of mechanisms like account lockout after repeated failed logins.
4. **Insecure File Uploads**:
   - Attackers upload malicious scripts disguised as legitimate files.

Testing Web Applications:

- **Dynamic Application Security Testing (DAST)**: Simulates real-world attacks on a running application.
- **Static Application Security Testing (SAST)**: Analyzes source code for vulnerabilities.
- **Manual Penetration Testing**: Human testers identify and exploit weaknesses.

Mitigation Strategies:

1. Regular updates and patching.
2. Use firewalls and Web Application Firewalls (WAFs).
3. Employ secure coding practices.

SQL Injection

Understanding SQL Injection:

- **Definition**: A technique used to exploit vulnerabilities in a database query by injecting malicious SQL code.
- **Entry Points**: Login forms, search fields, or any input areas that directly interact with the database.

How it Works:

- **Example Attack**:
  - Input: ' OR 1=1 --
  - Effect: Forces the SQL query to return all rows, bypassing authentication.

Steps in an SQL Injection Attack:

1. Find a vulnerable input field.
2. Inject malicious SQL commands.
3. Extract, modify, or delete database data.

Real-World Scenarios:

- Extracting usernames and passwords from a database.
- Deleting critical records from a database.

Countermeasures:

1. **Parameterized Queries and Prepared Statements**:
   - Use placeholders for user inputs in SQL queries.
2. **Input Validation**:
   - Reject or sanitize inputs containing dangerous characters (like ', --, ;).
3. **Database Permissions**:
   - Use the principle of least privilege.
   - Ensure user accounts have minimal access rights.
4. **Error Handling**:
   - Avoid exposing database errors to the user.
   - Example: Replace detailed error messages with generic ones like *"Invalid input."*

Imporantant MCQ for Unit 5

Session Hijacking

1. What is the primary target of session hijacking?
   a) User's login credentials
   b) User's session token
   c) User's browser history
   d) User's IP address
   Answer: b

2. Which protocol is most vulnerable to session hijacking attacks?
   a) HTTPS
   b) FTP
   c) HTTP
   d) SSH
   Answer: c

3. What does the HttpOnly attribute in cookies prevent?
   a) Cookie theft via XSS
   b) Session expiration
   c) Packet sniffing
   d) SQL injection
   Answer: a

4. Which tool can intercept and modify HTTP requests for session hijacking?
   a) Burp Suite
   b) Nmap
   c) Metasploit
   d) Wireshark
   Answer: a

5. Which of these is NOT a method to prevent session hijacking?
   a) Regenerating session IDs
   b) Encrypting session cookies
   c) Disabling MFA
   d) Using HTTPS
   Answer: c

6. What is the role of the Secure flag in cookies?
   a) Ensures cookies are sent over encrypted connections only
   b) Encrypts the cookies at rest
   c) Prevents the cookies from being read by any browser
   d) Extends the expiration time of cookies
   Answer: a

7. What is session fixation?
   a) Fixing bugs in the session management system
   b) Attacker sets a known session ID for the victim
   c) Extending session timeout by an attacker
   d) Hijacking a server's session data
   Answer: b

8. What is the first step in a session hijacking attack?
   a) Brute force session IDs
   b) Capture or guess the session token
   c) Exploit XSS vulnerabilities
   d) Steal user credentials
   Answer: b

9. How does HTTPS help prevent session hijacking?
   a) Encrypts session cookies during transmission
   b) Prevents brute force attacks
   c) Blocks malicious SQL queries
   d) Automatically regenerates session IDs
   Answer: a

10. Which is a defensive strategy against network session hijacking?
    a) Using a VPN
    b) Disabling HTTPS
    c) Enabling anonymous access
    d) Removing cookies after login
    Answer: a

Web Servers and Applications

11. What is the main role of a web server?
    a) Store static files only
    b) Process and deliver requests from clients
    c) Manage operating systems
    d) Encrypt user data
    Answer: b

12. Which of the following is an example of a web application vulnerability?
    a) Strong password policies
    b) Cross-Site Scripting (XSS)
    c) HTTPS encryption
    d) Two-factor authentication
    Answer: b

13. What is the relationship between a client and a server in web applications?
    a) The server sends requests to the client.
    b) The client processes the server's data.
    c) The client requests resources, and the server responds.
    d) They both perform encryption together.
    Answer: c

14. What type of attack involves injecting malicious scripts into web pages?
    a) SQL Injection
    b) Cross-Site Scripting (XSS)
    c) Denial-of-Service
    d) Session Hijacking
    Answer: b

15. Which tool is used for testing web application vulnerabilities?
    a) Burp Suite
    b) Wireshark
    c) Nmap
    d) Ettercap
    Answer: a

16. What does a Web Application Firewall (WAF) do?
    a) Scans for viruses on web servers
    b) Protects against web application attacks like SQLi and XSS
    c) Encrypts all client-server communication
    d) Prevents session timeout
    Answer: b

17. Which vulnerability allows attackers to bypass authentication and execute queries?
    a) SQL Injection
    b) XSS
    c) Man-in-the-Middle
    d) DNS Spoofing
    Answer: a

18. What does Dynamic Application Security Testing (DAST) test?
    a) Application source code
    b) Functionality of APIs
    c) Vulnerabilities in running web applications
    d) Network traffic logs
    Answer: c

19. What does the principle of least privilege entail for web applications?
    a) Limiting user access to only necessary permissions
    b) Allowing unrestricted access to databases
    c) Hiding user roles from attackers
    d) Avoiding encrypted connections
    Answer: a

20. Which HTTP method is commonly associated with retrieving data from a server?
    a) POST
    b) GET
    c) DELETE
    d) PUT
    Answer: b

SQL Injection

21. What is the main purpose of SQL injection?
    a) Modify or extract database data
    b) Encrypt database records
    c) Defend against network attacks
    d) Test session timeouts
    Answer: a

22. Which input could trigger an SQL injection attack?
    a) ' OR 1=1 --
    b) SELECT * FROM users
    c) 123456
    d) DROP TABLES;
    Answer: a

23. What is a common result of an SQL injection attack?
    a) Database corruption
    b) Faster database queries
    c) Improved user experience
    d) Automatic session hijacking
    Answer: a

24. What is the best way to prevent SQL injection?
    a) Use prepared statements and parameterized queries
    b) Use dynamic SQL queries
    c) Increase server timeout
    d) Encrypt all HTTP traffic
    Answer: a

25. Which is a vulnerable input for SQL injection?
    a) Input fields without validation
    b) Encrypted fields
    c) Read-only fields
    d) HTTPS-protected fields
    Answer: a

26. Which SQL command is likely to be misused in an injection attack?
    a) SELECT
    b) INSERT
    c) UPDATE
    d) All of the above
    Answer: d

27. What is a UNION-based SQL injection attack?
    a) Modifies server-side logic
    b) Combines results from multiple SELECT statements
    c) Exploits database functions
    d) Alters server configurations
    Answer: b

28. What is an indicator of a successful SQL injection attack?
    a) Errors revealing database structure
    b) Browser crashes
    c) Slow server response
    d) Encrypted communication failure
    Answer: a

29. Which of these is an effective countermeasure to SQL injection?
    a) Regular expressions in input fields
    b) Limiting database user permissions
    c) Using HTML encoding
    d) Allowing special characters in queries
    Answer: b

30. What is an error-based SQL injection?
    a) Exploits database error messages to extract information
    b) Injects malicious scripts into web pages
    c) Crashes the database server
    d) Hijacks session tokens
    Answer: a

---

20 More MCQs for Exam Preparation

Session Hijacking

1. Which of the following is an effective method to protect against session hijacking?
   a) Enabling anonymous login
   b) Using session timeouts
   c) Storing session tokens in plain text
   d) Sharing session tokens publicly
   Answer: b

2. What is the purpose of the "SameSite" cookie attribute?
   a) Restricts cookies from being sent with cross-site requests
   b) Prevents session expiration
   c) Enables cookies to work across multiple sites
   d) Encrypts cookie data at rest
   Answer: a

3. A session hijacking attack on a public Wi-Fi network is likely conducted using:
   a) DNS Spoofing
   b) Packet Sniffing
   c) SQL Injection
   d) Keylogger
   Answer: b

4. Which of the following attacks involves forcing a user to use a specific session ID?
   a) Session Expiry
   b) Session Fixation
   c) Session Replay
   d) Session Duplication
   Answer: b

5. Which protocol provides end-to-end encryption, mitigating session hijacking risks?
   a) Telnet
   b) HTTP
   c) HTTPS
   d) FTP
   Answer: c

Web Servers and Applications

6. What is the primary cause of Cross-Site Scripting (XSS) attacks?
   a) Weak encryption algorithms
   b) Insufficient input validation
   c) Lack of firewalls
   d) Poor database design
   Answer: b

7. What does a 404 HTTP response code signify?
   a) Unauthorized access
   b) Server not responding
   c) Resource not found
   d) Service temporarily unavailable
   Answer: c

8. Which type of web application vulnerability exploits user input to execute unauthorized database queries?
   a) Buffer Overflow
   b) Cross-Site Scripting
   c) SQL Injection
   d) DNS Spoofing
   Answer: c

9. What type of test simulates attacks to evaluate a web application’s security?
   a) Penetration Testing
   b) Load Testing
   c) Unit Testing
   d) Functional Testing
   Answer: a

10. Which HTTP method is commonly used to send sensitive data, such as login credentials?
    a) GET
    b) POST
    c) DELETE
    d) OPTIONS
    Answer: b

SQL Injection

11. Which input validation technique helps prevent SQL injection attacks?
    a) Allowing special characters
    b) Using parameterized queries
    c) Accepting all input as valid
    d) Storing inputs as plain text
    Answer: b

12. Which of the following SQL keywords can be exploited in an injection attack?
    a) SELECT
    b) INSERT
    c) DELETE
    d) All of the above
    Answer: d

13. Which type of SQL injection attack involves manipulating database errors?
    a) Union-based
    b) Error-based
    c) Boolean-based
    d) Time-based
    Answer: b

14. A successful SQL injection attack can result in:
    a) Unauthorized data access
    b) Server shutdown
    c) Network sniffing
    d) Denial of Service (DoS)
    Answer: a

15. Which technique alters data or retrieves information without triggering SQL errors?
    a) Blind SQL Injection
    b) Error-based SQL Injection
    c) Time-based SQL Injection
    d) Header-based SQL Injection
    Answer: a

Combined Topics

16. What is a common symptom of a successful session hijacking attack?
    a) Increased server response time
    b) Unauthorized transactions or access
    c) Application crashing
    d) Repeated session timeouts
    Answer: b

17. Which of these is a common tool used for SQL injection attacks?
    a) SQLmap
    b) Nmap
    c) Wireshark
    d) Metasploit
    Answer: a

18. Which type of attack manipulates a user into providing confidential information?
    a) Social Engineering
    b) SQL Injection
    c) Session Hijacking
    d) Denial of Service
    Answer: a

19. How can an attacker exploit an unvalidated redirect in a web application?
    a) Redirect users to malicious websites
    b) Encrypt sensitive data
    c) Trigger server restarts
    d) Force server session expiration
    Answer: a

20. What does the ARP Poisoning technique aim to achieve?
    a) Deceive devices into sending data to the attacker
    b) Destroy a device's ARP cache
    c) Execute malicious SQL queries
    d) Hijack web server traffic
    Answer: a