BRAINWARE UNIVERSITY

Term End Examination 2025-2026
Programme – B.Sc.(ANCS)-Hons-2023/B.Sc.(ANCS)-Hons-2024
Course Name – Web Application Penetration Testing
Course Code - BNC40112/BNC40107
(Semester IV)

Full Marks : 60 **Time : 2:30 Hours**

[The figure in the margin indicates full marks. Candidates are required to give their answers in their own words as far as practicable.]

Group-A
(Multiple Choice Type Question) 1 x 15=15

1. *Choose the correct alternative from the following :*

(i) Compare the advantages of using REST over GraphQL for API communication.
   a) REST is faster b) REST is widely adopted
   c) REST reduces API flexibility d) REST improves query efficiency

(ii) How can rate-limiting techniques reduce server overload?
   a) Use cookies b) Use WebSockets
   c) Limit API requests per user d) Increase connection timeout

(iii) Why is input validation important in preventing XSS attacks?
   a) To sanitize database entries b) To prevent malicious scripts from executing
   c) To block user authentication d) To enable secure session cookies

(iv) Evaluate the impact of DOM-Based XSS on client-side security.
   a) Compromises only network security b) Compromises browser behavior
   c) Steals server credentials d) Hijacks admin credentials

(v) Identify the method to inspect DOM elements for vulnerabilities.
   a) Using browser developer tools b) Scanning the server
   c) Modifying database entries d) Running automated scripts

(vi) Determine the correct clause for filtering records in an SQL query.
   a) FROM b) WHERE
   c) ORDER BY d) GROUP BY

(vii) Identify how an attacker could exploit UNION-based SQL Injection.
   a) By appending UNION SELECT username, password FROM users b) By using ORDER BY to arrange data
   c) By encrypting SQL queries d) By limiting database user privileges

(viii) Classify the primary mitigation strategies against SQL Injection.

a) Parameterized queries, input validation, least privilege access
b) Encryption, system restart, increasing RAM
c) Storing logs, creating backups, database clustering
d) Using long queries, optimizing indexes, reducing errors

(ix) Recognize a key reason for session expiration implementation.

a) To prevent long-term unauthorized access
b) To speed up user authentication
c) To allow multiple users on the same session
d) To store session data permanently

(x) Choose the best security measure for preventing session hijacking.

a) Implementing token-based authentication
b) Storing session IDs in local storage
c) Using weakly encrypted session identifiers
d) Sharing session cookies across domains

(xi) Differentiate between session hijacking and session fixation.

a) Session hijacking steals an active session, while session fixation forces a user to use a predefined session
b) Both attacks require password cracking
c) Session fixation involves network sniffing
d) Session hijacking only affects mobile devices

(xii) Choose the most effective defense against session replay attacks.

a) Implementing time-based session tokens
b) Allowing users to log in from multiple devices at the same time
c) Disabling automatic session expiration
d) Encrypting cookies with a weak algorithm

(xiii) Identify the main risk associated with Remote File Inclusion (RFI).

a) Increased website performance
b) Execution of malicious scripts from external servers
c) Protection against brute-force attacks
d) Automatic file encryption

(xiv) Describe the impact of a successful path traversal attack.

a) Automatic session termination
b) Unauthorized access to system files and application data
c) Faster access to cached files
d) Improved website navigation

(xv) Predict the best approach to prevent file upload abuse.

a) Preventing users from accessing file upload forms
b) Storing uploaded files in executable directories
c) Implementing strict allowlists and server-side validation
d) Allowing all file types to be uploaded

Group-B

(Short Answer Type Questions) 3 x 5=15

2. Explain session sniffing and its role in compromising security. (3)
3. Illustrate the authentication and authorization process of JWT (JSON Web token) using a proper diagram. (3)
4. Apply input validation techniques to mitigate XSS attacks. (3)
5. Illustrate the role of the WHERE clause in SQL queries. (3)
6. Assess the impact of weak input validation on file inclusion attacks. (3)

OR

Evaluate security measures to prevent Local and Remote File Inclusion attacks. (3)

Group-C

(Long Answer Type Questions) 5 x 6=30

7. Analyze the importance of session security in web applications and describe two common attacks that target session management. (5)
8. What are RESTful APIs, and why are they important? (5)

9. Explain how Content Security Policy (CSP) mitigates XSS attacks. (5)
10. Claasify SQL Injection and its impact on database security. (5)
11. Evaluate the key factors that contribute to SQL Injection vulnerabilities. (5)
12. Assess the role of Content-Disposition headers in preventing file execution vulnerabilities. (5)

OR

Evaluate the impact of weak file permissions on web server security. (5)

****