**Semester – End Examination Question Bank**

Course Coordinator Name: Mr. Puneethraj K

Department: Computer Science

Programme Name: Bachelor of Computer Applications

Course Name: Application and Web Security

Course Type: Discipline Specific Elective – DSE

Credit: 4

Semester: V

Total Marks: 75

Year: 2025 – 2026

|  |  |  |  |
| --- | --- | --- | --- |
| **UNIT I** | | | |
| **Multiple Choice Questions** | | **CO, PO, PSO** | **Bloom's Level** |
| 1 | What does SQL Injection target?  a. Client Browser b. Database  c. File System d. Network Switch  **Answer: b. Database** | CO5, PO4, PSO2 | Remember |
| 2 | Which status code indicates “Page Not Found”?  a. 200 b. 500 c. 404 d. 301  **Answer: c. 404** | CO2, PO2, PSO1 | Remember |
| 3 | HTTPS is more secure than HTTP because it uses: a. Cookies b. TLS/SSL  c. HTML d. REST  **Answer: b. TLS/SSL** | CO2, PO6, PSO1 | Understand |
| 4 | What is the use of a reverse proxy?  a. Encrypts content  b. Filters users  c. Forwards client requests to servers  d. Blocks malware  **Answer: c. Forwards client requests to servers** | CO2, PO4, PSO1 | Understand |
| 5 | Base64 encoding is mainly used to:  a. Encrypt password b. Store logs  c. Send binary data as text d. Minify JS  **Answer: c. Send binary data as text** | CO2, PO2, PSO1 | Remember |
| 6 | Cookies are used for:  a. Memory allocation b. Hardware security  c. Session tracking d. Virus scanning  **Answer: c. Session tracking** | CO2, PO5, PSO1 | Understand |
| 7 | Which encoding is used to make URLs safe?  a. HTML encoding b. JSON encoding  c. URL encoding d. MIME encoding  **Answer: c. URL encoding** | CO2, PO2, PSO1 | Remember |
| 8 | A zombie cookie:  a. Gets deleted by user  b. Disappears after session  c. Reappears after deletion  d. Is harmless  **Answer: c. Reappears after deletion** | CO2, PO6, PSO2 | Understand |
| 9 | Which of these is NOT a method in HTTP?  a. GET b. SET c. POST d. DELETE  **Answer: b. SET** | CO2, PO2, PSO1 | Remember |
| 10 | Which component processes logic in 3-tier architecture?  a. Presentation b. Application  c. Data d. Network  **Answer: b. Application** | CO1, PO4, PSO1 | Understand |
| 11 | Which technique is used to discover hidden web content?  a. Hashing b. Spidering  c. Tokenization d. Sniffing  **Answer: b. Spidering** | CO3, PO5, PSO3 | Understand |
| 12 | Which response code is for permanent redirection?  a. 302 b. 403 c. 301 d. 500  **Answer: c. 301** | CO2 | Remember |
| 13 | Which header is used for authentication?  a. Set-Cookie b. Accept-Language  c. Authorization d. User-Agent  **Answer: c. Authorization** | CO2 | Understand |
| 14 | What is the purpose of a session ID?  a. Encrypt files b. Uniquely identify user  c. Manage logs d. Compress data  **Answer: b. Uniquely identify user** | CO2, PO5, PSO2 | Understand |
| 15 | What does XSS target?  a. Server database b. Client browser  c. Operating system d. Firewall  **Answer: b. Client browser** | CO5, PO4, PSO2 | Understand |
| 16 | Which of the following is NOT a valid authentication method?  a. Password b. OTP  c. CAPTCHA d. Proxy  **Answer: d. Proxy** | CO4, PO5, PSO1 | Understand |
| 17 | Which response code is for server-side error?  a. 200 b. 403 c. 404 d. 500  **Answer: d. 500** | CO5, PO4, PSO2 | Remember |
| 18 | What does SQL UNION operator do?  a. Insert data b. Delete data  c. Merge result sets d. Create index  **Answer: c. Merge result sets** | CO5, PO5, PSO3 | Understand |
| 19 | What is the primary cause of brute-force attacks?  a. Strong encryption b. Predictable passwords  c. HTML injection d. Cookies  **Answer: b. Predictable passwords** | CO4, PO7, PSO2 | Understand |
| 20 | Which layer handles rendering in 2-tier architecture?  a. Server b. Middleware  c. Client d. Proxy  **Answer: c. Client** | CO1, PO2, PSO1 | Remember |
| **5 Marks Questions** | | | |
| 1 | Explain the differences between HTML encoding and URL encoding. | CO2, PO2, PSO1 | Understand |
| 2 | Describe the process of authentication using headers. | CO2, PO4, PSO1 | Understand |
| 3 | Write short notes on phishing and spyware with examples. | CO1, PO7, PSO1 | Understand |
| 4 | What are session cookies and how are they used in authentication? | CO2, PO5, PSO2 | Understand |
| 5 | Explain the role of HTTPS and SSL in securing web apps. | CO2, PO6, PSO1 | Understand |
| 6 | Compare 2-tier and 3-tier architecture with examples. | CO1, PO4, PSO1 | Analyze |
| 7 | Describe the common signs of SQL injection. | CO5, PO5, PSO2 | Understand |
| 8 | What is web spidering and how is it helpful in application mapping? | CO3, PO4, PSO3 | Understand |
| 9 | How does Cross-Site Scripting (XSS) work? Explain with example. | CO5, PO4, PSO2 | Understand |
| 10 | Describe client-side vs server-side validation. | CO2, PO6, PSO1 | Understand |
| **10 Marks Questions** | | | |
| 1 | Describe the evolution of web applications from Web 1.0 to Web 3.0. | CO1, PO3, PSO1 | Understand |
| 2 | Discuss the role and implementation of secure session management. | CO4, PO5, PSO2 | Apply |
| 3 | Illustrate the use of encoding schemes (Base64, URL, HTML) in web security. | CO2, PO6, PSO1 | Apply |
| 4 | Explain SQL injection techniques with countermeasures. | CO5, PO5, PSO2 | Analyze |
| 5 | Describe different HTTP response codes and their relevance in web apps. | CO2, PO2, PSO1 | Understand |
| **15 Marks Questions** | | | |
| 1 | Design a secure login system addressing authentication flaws. | CO4, PO5, PSO4 | Creating |
| 2 | Develop a plan for protecting a website against SQL injection and XSS. | CO5, PO6, PSO4 | Creating |
| 3 | Map and analyze the vulnerabilities of a sample web app using OWASP Top 10. | CO3, PO5, PSO2 | Analyzing |
| 4 | Create a use-case comparing multiple architectures (2-tier, 3-tier, n-tier) in deployment. | CO1, PO4, PSO1 | Creating |
| 5 | Design a secure form handling and input validation mechanism. | CO2, PO6, PSO1 | Creating |

|  |  |  |  |
| --- | --- | --- | --- |
| **UNIT II** | | | |
| **Multiple Choice Questions** | | **CO, PO, PSO** | **Bloom's Level** |
| 1 | What does HTTP stand for?   1. HyperText Transfer Protocol 2. Hyper Tool Transfer Protocol 3. High Text Transfer Protocol 4. Hyper Transfer Text Protocol   **Answer: a. HyperText Transfer Protocol** | CO2, PO2, PSO1 | Remember |
| 2 | Which HTTP method is used to update existing resources?  a. GET b. POST c. PUT d. DELETE  **Answer: c. PUT** | CO2, PO2, PSO1 | Understand |
| 3 | What is the function of status code 404?  a. OK b. Found  c. Not Found d. Unauthorized  **Answer: c. Not Found** | CO2, PO2, PSO1 | Remember |
| 4 | Which protocol is more secure?  a. HTTP b. FTP c. SMTP d. HTTPS  **Answer: d. HTTPS** | CO2, PO2, PSO1 | Understand |
| 5 | SQL injection affects which layer?  a. Application b. Transport  c. Physical d. Network  **Answer: a. Application** | CO5, PO4, PSO3 | Apply |
| 6 | Which of the following is a safe HTTP method?  a. GET b. DELETE c. PUT d. PATCH  **Answer: a. GET** | CO2, PO5, PSO2 | Analyze |
| 7 | Which is used for session tracking?  a. Cookies b. HTML c. CSS d. IP address  **Answer: a. Cookies** | CO2, PO2, PSO1 | Understand |
| 8 | What is the full form of XSS?  a. Cross-Site Scan b. Cross-Site Scripting  c. Extra Secure Site d. None  **Answer: b. Cross-Site Scripting** | CO3, PO4, PSO2 | Remember |
| 9 | What is a common symptom of SQL injection?  a. Broken image b. Delay in loading  c. Unauthorized data access d. Page not found  **Answer: c. Unauthorized data access** | CO5, PO4, PSO3 | Analyze |
| 10 | Which of the following encoding schemes is used in URL?  a. Unicode b. HTML c. URL d. Base64  **Answer: c. URL** | CO2, PO2, PSO1 | Understand |
| 11 | Which tool is used for packet sniffing?  a. WordPress b. Wireshark  c. Canva d. Zoom  **Answer: b. Wireshark** | CO5, PO6, PSO3 | Apply |
| 12 | HTTPS uses which encryption protocol?  a. FTP b. SSL/TLS c. IPSEC d. AES  **Answer: b. SSL/TLS** | CO2, PO6, PSO1 | Understand |
| 13 | Which HTTP status code means success?  a. 200 b. 404 c. 403 d. 500  **Answer: a. 200** | CO2, PO2, PSO1 | Remember |
| 14 | Which method can retrieve data without changing server state?  a. POST b. DELETE c. GET d. PUT  **Answer: c. GET** | CO2, PO2, PSO1 | Understand |
| 15 | What is the purpose of authentication?  a. Hiding data b. Compressing data c. Identifying users d. Encrypting data  **Answer: c. Identifying users** | CO4, PO5, PSO1 | Understand |
| 16 | What is the default port for HTTP?  a. 21 b. 25 c. 443 d. 80  **Answer: d. 80** | CO2, PO2, PSO1 | Remember |
| 17 | Which is an access control vulnerability?  a. 404 error  b. SQL error  c. Insecure Direct Object Reference  d. Syntax error  **Answer: c. Insecure Direct Object Reference** | CO4, PO4, PSO3 | Apply |
| 18 | What does URL stand for?   1. Uniform Resource Locator 2. User Remote Login 3. Universal Result Location 4. Unidentified Resource Log   **Answer: a. Uniform Resource Locator** | CO2, PO2, PSO1 | Remember |
| 19 | Which HTTP method is **not** idempotent?  a. GET b. PUT c. POST d. DELETE  **Answer: c. POST** | CO2, PO2, PSO1 | Understand |
| 20 | Which tool is commonly used to test SQL injection?  a. Canva b. Zoom c. SQLmap d. Figma  **Answer: c. SQLmap** | CO5, PO6, PSO3 | Apply |
| **5 Marks Questions** | | | |
| 1 | Define HTTP and explain its components. | CO2, PO2, PSO1 | Understand |
| 2 | Differentiate between GET and POST methods. | CO2, PO2, PSO1 | Analyze |
| 3 | What are cookies and how do they support session management? | CO2, PO2, PSO1 | Understand |
| 4 | List and describe any 4 HTTP status codes. | CO2, PO2, PSO1 | Remember |
| 5 | Describe the purpose of URL encoding with examples. | CO2, PO2, PSO1 | Understand |
| 6 | Identify vulnerabilities in broken authentication. | CO4, PO4, PSO2 | Analyze |
| 7 | What is SQL Injection? Explain with an example. | CO5, PO4, PSO3 | Apply |
| 8 | State the difference between authentication and authorization. | CO4, PO4, PSO1 | Understand |
| 9 | Explain HTTPS and its advantages. | CO2, PO2, PSO1 | Understand |
| 10 | Describe HTML encoding and where it is used. | CO2, PO2, PSO1 | Understand |
| **10 Marks Questions** | | | |
| 1 | Analyze the complete HTTP request and response cycle with headers. | CO2, PO2, PSO1 | Analyze |
| 2 | Explain common access control vulnerabilities and their prevention. | CO4, PO4, PSO3 | Evaluate |
| 3 | Discuss the types of encoding schemes in web security. | CO2, PO2, PSO1 | Understand |
| 4 | Analyze the role of client-side vs server-side functionality. | CO2, PO2, PSO1 | Analyze |
| 5 | Explain SQL injection techniques and list preventive mechanisms. | CO5, PO5, PSO3 | Evaluate |
| **15 Marks Questions** | | | |
| 1 | Discuss various HTTP vulnerabilities and explain how to mitigate them with examples. | CO3, PO4, PSO2 | Evaluate |
| 2 | Design a secure login system highlighting potential attacks and defenses. | CO4, PO5, PSO2 | Create |
| 3 | Explain session management in detail and demonstrate session hijacking mitigation. | CO2, PO4, PSO2 | Evaluate |
| 4 | Develop a mini application that demonstrates SQL injection and its defense. | CO5, PO5, PSO3 | Create |
| 5 | Evaluate real-time case studies related to broken authentication and security breaches. | CO4, PO7, PSO2 | Evaluate |

|  |  |  |  |
| --- | --- | --- | --- |
| **UNIT III** | | | |
| **Multiple Choice Questions** | | **CO, PO, PSO** | **Bloom's Level** |
| 1 | What is the purpose of enumeration in application security?  a. To generate passwords  b. To gather system information  c. To encrypt data  d. To test speed  **Answer: b. To gather system information** | CO3, PO2, PSO2 | Understand |
| 2 | Which tool is used for NetBIOS enumeration?  a. nslookup b. nbtstat  c. traceroute d. whois  **Answer: b. nbtstat** | CO3, PO6, PSO2 | Remember |
| 3 | What is the main advantage of manual spidering?  a. It is automatic b. It avoids login  c. It is fast d. It identifies complex paths  **Answer: d. It identifies complex paths** | CO3, PO4, PSO2 | Understand |
| 4 | Which of the following is not a method of content discovery?  a. robots.txt b. sitemap.xml  c. traceroute d. favicon analysis  **Answer: c. traceroute** | CO3, PO4, PSO2 | Remember |
| 5 | Which command can perform automated content discovery?  a. ping b. dirb c. dig d. curl **Answer: b. dirb** | CO3, PO6, PSO2 | Apply |
| 6 | Hidden parameters can be found using:  a. CSS files b. HTML input fields  c. Meta tags d. Font files  **Answer: b. HTML input fields** | CO3, PO2, PSO2 | Understand |
| 7 | What is the use of 'Burp Suite'?  a. Detect malware b. Analyze logs  c. Intercept HTTP requests d. Write SQL queries  **Answer: c. Intercept HTTP requests** | CO3, PO6, PSO3 | Apply |
| 8 | DNS zone transfer can help in:  a. Encrypting traffic b. Discovering topology  c. Changing passwords d. Creating fake users  **Answer: b. Discovering topology** | CO3, PO2, PSO3 | Understand |
| 9 | A good way to prevent enumeration is:  a. Use weak passwords  b. Disable firewall  c. Allow open ports  d. Implement access controls  **Answer: d. Implement access controls** | CO3, PO5, PSO4 | Apply |
| 10 | What file instructs search engines to avoid indexing parts of a site?  a. sitemap.html b. robots.txt  c. index.php d. config.ini  **Answer: b. robots.txt** | CO3, PO2, PSO2 | Remember |
| 11 | Which tool helps find unreferenced parameters in Burp Suite?  a. Nikto b. ParamMiner  c. Wireshark d. Hydra  **Answer: b. ParamMiner** | CO3, PO6, PSO3 | Remember |
| 12 | What is an application page?  a. Login flow b. Logical sequence  c. UI component d. Code segment  **Answer: c. UI component** | CO3, PO2, PSO1 | Understand |
| 13 | What does REST stand for?  a. Realtime Secure Transfer  b. Reliable Execution State Tracker  c. Representational State Transfer  d. Rapid Encoding State Transfer  **Answer: c. Representational State Transfer** | CO2, PO2, PSO3 | Remember |
| 14 | Which one is a tool for automated discovery?  a. ping b. ffuf c. touch d. Ssh  **Answer: b. ffuf** | CO3, PO6, PSO3 | Apply |
| 15 | An example of a functional path is:  a. CSS rendering b. Login flow  c. JavaScript animation d. Favicon icon  **Answer: b. Login flow** | CO3, PO2, PSO2 | Understand |
| 16 | Server-side request forgery (SSRF) involves:  a. Client impersonation  b. Redirect loops  c. Server making unintended requests  d. Broken URLs  **Answer: c. Server making unintended requests** | CO4, PO4, PSO4 | Understand |
| 17 | Web spidering helps to:  a. Improve encryption  b. Track user input  c. Identify structure of web app  d. Store cookies  **Answer: c. Identify structure of web app** | CO3, PO2, PSO2 | Understand |
| 18 | LDAP enumeration helps identify:  a. Network speed b. Logged-in users  c. Directory services d. DNS info  **Answer: c. Directory services** | CO3, PO2, PSO2 | Remember |
| 19 | NTP enumeration is useful for:  a. Authentication b. Clock synchronization info  c. URL masking d. Firewall status  **Answer: b. Clock synchronization info** | CO3, PO2, PSO2 | Understand |
| 20 | Which method discovers entry points in web apps?  a. Robots exclusion b. Query string analysis  c. Font rendering d. HTML compression  **Answer: b. Query string analysis** | CO3, PO4, PSO3 | Apply |
| **5 Marks Questions** | | | |
| 1 | Explain the purpose and steps of manual spidering in web security. | CO3, PO4, PSO2 | Understand |
| 2 | What is the difference between application pages and functional paths? Give examples. | CO3, PO2, PSO1 | Understand |
| 3 | List different techniques used for enumeration and their purpose. | CO3, PO4, PSO2 | Remember |
| 4 | Discuss how tools like ffuf or dirb are used in content discovery. | CO3, PO6, PSO2 | Apply |
| 5 | Explain how robots.txt and sitemap.xml can expose hidden content. | CO3, PO4, PSO2 | Analyze |
| 6 | What is DNS zone transfer? How can it be exploited? | CO3, PO2, PSO3 | Understand |
| 7 | Define attack surface mapping and its importance in cybersecurity. | CO3, PO4, PSO4 | Understand |
| 8 | Describe parameter fuzzing and its role in vulnerability discovery. | CO3, PO6, PSO3 | Apply |
| 9 | What are the major tools used for finding entry points in a web application? | CO3, PO6, PSO3 | Understand |
| 10 | Describe SSRF vulnerability with an example. | CO4, PO4, PSO4 | Understand |
| **10 Marks Questions** | | | |
| 1 | Describe the steps of automated spidering. How does it differ from manual spidering? | CO3, PO4, PSO2 | Analyze |
| 2 | Discuss various types of enumeration (NetBIOS, LDAP, SNMP, etc.) and their tools. | CO3, PO6, PSO2 | Analyze |
| 3 | Explain the impact of discovering hidden content on web application security. | CO3, PO5, PSO3 | Analyze |
| 4 | Illustrate how identifying entry points helps in reducing the attack surface. | CO3, PO4, PSO4 | Analyze |
| 5 | Compare the functionalities and risks of REST, SOAP, and XML-RPC in web communication. | CO2, PO4, PSO3 | Analyze |
| **15 Marks Questions** | | | |
| 1 | Explain attack surface mapping in detail. List its types and the strategies to reduce them. | CO3, PO4, PSO4 | Evaluate |
| 2 | Design a full workflow to discover hidden parameters using Burp Suite, Arjun, or x8. | CO3, PO6, PSO3 | Create |
| 3 | Describe how a tester can analyze application architecture using both spidering and enumeration. | CO3, PO4, PSO2 | Analyze |
| 4 | Prepare a penetration testing plan using tools like ffuf, Burp, and dirb for content discovery. | CO3, PO5, PSO3 | Create |
| 5 | Analyze the differences between client-side and server-side functionality in web security. | CO4, PO4, PSO1 | Analyze |

|  |  |  |  |
| --- | --- | --- | --- |
| **UNIT IV** | | | |
| **Multiple Choice Questions** | | **CO, PO, PSO** | **Bloom's Level** |
| 1 | What does authentication verify?  a. User role b. User identity  c. User location d. User logs  **Answer: b. User identity** | CO4, PO2, PSO1 | Remember |
| 2 | Which authentication uses username and password only?  a. MFA b. 2FA c. SFA d. OTP  **Answer: c. SFA** | CO4, PO2, PSO1 | Remember |
| 3 | What is the main risk of "Remember Me" feature?  a. Slower login b. Session timeout  c. Token theft d. User logouts  **Answer: c. Token theft** | CO4, PO4, PSO4 | Understand |
| 4 | What is a good practice to secure passwords?  a. Store in plain text b. Use strong hashing  c. Use short length d. Share via email  **Answer: b. Use strong hashing** | CO4, PO6, PSO1 | Apply |
| 5 | What attack tries all possible password combinations?  a. SQLi b. CSRF c. Brute Force d. DDoS  **Answer: c. Brute Force** | CO4, PO4, PSO2 | Understand |
| 6 | OTP is used in which method?  a. Single-factor b. Two-factor  c. Role-based d. Token-based  **Answer: b. Two-factor** | CO4, PO2, PSO1 | Understand |
| 7 | Which tool can be used for brute-force login?  a. Hydra b. Nmap  c. Wireshark d. Metasploit  **Answer: a. Hydra** | CO4, PO6, PSO2 | Apply |
| 8 | What is a risk of using default passwords?  a. Easy debugging b. Credential leaks  c. Faster login d. Slower system  **Answer: b. Credential leaks** | CO4, PO4, PSO4 | Understand |
| 9 | Which is a sign of verbose failure messages?  a. Generic errors b. Stack traces  c. OTP prompts d. Login redirect  **Answer: b. Stack traces** | CO4, PO2, PSO1 | Remember |
| 10 | What is session fixation?  a. Modifying session token b. Reusing session ID  c. OTP delay d. Password reuse  **Answer: b. Reusing session ID** | CO4, PO4, PSO4 | Understand |
| 11 | Predictable usernames are vulnerable to:  a. XSS b. Credential stuffing  c. DNS spoofing d. Broken ACLs  **Answer: b. Credential stuffing** | CO4, PO5, PSO2 | Apply |
| 12 | Which is NOT an authentication type?  a. 2FA b. SSO c. MFA d. DNS  **Answer: d. DNS** | CO4, PO2, PSO1 | Remember |
| 13 | What should never be shared in plain text?  a. Username b. IP address  c. Credentials d. Domain name  **Answer: c. Credentials** | CO4, PO7, PSO3 | Understand |
| 14 | Validation of credentials happens during:  a. Logout b. Login c. Session expire d. Backup  **Answer: b. Login** | CO4, PO2, PSO1 | Remember |
| 15 | CSRF allows attackers to:  a. Modify HTML  b. Send commands as logged-in user  c. Delete server  d. Encrypt DB  **Answer: b. Send commands as logged-in user** | CO4, PO4, PSO2 | Understand |
| 16 | Which authentication stores token in cookies?  a. Token-based b. SFA c. OTP d. MFA  **Answer: a. Token-based** | CO4, PO6, PSO1 | Apply |
| 17 | What can happen with non-unique usernames?  a. More speed b. Impersonation  c. MFA bypass d. None  **Answer: b. Impersonation** | CO4, PO4, PSO3 | Understand |
| 18 | What should be done before changing password?  a. Logout b. Old password confirmation  c. Set username d. Enable cookies  **Answer: b. Old password confirmation** | CO4, PO2, PSO1 | Remember |
| 19 | What is a weak practice in password reset?  a. OTP usage b. Non-expiring link  c. Email link d. CAPTCHA  **Answer: b. Non-expiring link** | CO4, PO5, PSO2 | Understand |
| 20 | Example of insecure distribution of credentials?  a. Emailing password in plain text  b. SMS OTP  c. CAPTCHA  d. MFA  **Answer: a. Emailing password in plain text** | CO4, PO7, PSO3 | Understand |
| **5 Marks Questions** | | | |
| 1 | Explain Single-Factor and Two-Factor Authentication with examples. | CO4, PO2, PSO1 | Understand |
| 2 | Describe how "Remember Me" functionality works and how it can be exploited. | CO4, PO4, PSO4 | Analyze |
| 3 | What are verbose error messages? Mention how they can be exploited. | CO4, PO4, PSO2 | Understand |
| 4 | Describe insecure password practices and suggest strong password guidelines. | CO4, PO7, PSO2 | Apply |
| 5 | Explain the concept of credential validation and its importance. | CO4, PO2, PSO1 | Understand |
| 6 | Define brute-force login and explain how attackers perform it. | CO4, PO4, PSO2 | Understand |
| 7 | Mention different types of authentication and how MFA enhances security. | CO4, PO3, PSO1 | Understand |
| 8 | How can attackers use predictable usernames in brute-force attacks? | CO4, PO5, PSO2 | Analyze |
| 9 | Discuss problems caused by non-unique usernames in web applications. | CO4, PO4, PSO1 | Apply |
| 10 | Write short notes on insecure credential distribution methods. | CO4, PO7, PSO3 | Remember |
| **10 Marks Questions** | | | |
| 1 | Discuss the role of session management in authentication and its security concerns. | CO4, PO4, PSO1 | Analyze |
| 2 | Explain the various flaws found in password change and password reset functionalities. | CO4, PO4, PSO2 | Analyze |
| 3 | Explain the difference between multi-factor authentication and single sign-on with examples. | CO4, PO2, PSO1 | Understand |
| 4 | Explain the concept of brute-force login attacks. How can developers defend against them? | CO4, PO5, PSO2 | Analyze |
| 5 | List and explain common design flaws in authentication mechanisms. | CO4, PO4, PSO2 | Analyze |
| **15 Marks Questions** | | | |
| 1 | Describe in detail the different types of authentication mechanisms and explain their use in modern web applications. | CO4, PO2, PSO1 | Understand |
| 2 | Explain the working of token-based authentication and how improper session handling can lead to attacks. | CO4, PO4, PSO2 | Analyze |
| 3 | Discuss "Validation of Credentials" in detail with practical implementation considerations. | CO4, PO5, PSO3 | Apply |
| 4 | Write a detailed note on attacks possible via insecure distribution of credentials. How can they be prevented? | CO4, PO7, PSO3 | Evaluate |
| 5 | Design a secure authentication workflow for a banking website incorporating OTP, password policy, and session handling. | CO4, PO6, PSO3 | Create |