|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Roll No. |  |  |  |  |  |  |  |  |  |  |  |  |



**PRESIDENCY UNIVERSITY**

**Bengaluru**

|  |
| --- |
| **End - Term Examinations – MAY 2025** |
| **Date:** 22-05-2025 **Time:** 09:30 am – 12:30 pm |

|  |  |  |
| --- | --- | --- |
| **School:** SOCSE | **Program:** Computer Science & Engineering (Cyber Security) | |
| **Course Code :** CSE3097 | **Course Name:** Web Security | |
| **Semester**: VI | **Max Marks**: 100 | **Weightage**: 50% |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CO - Levels** | **CO1** | **CO2** | **CO3** | **CO4** |
| **Marks** | **24** | **24** | **26** | **26** |

**Instructions:**

1. *Read all questions carefully and answer accordingly.*
2. *Do not write anything on the question paper other than roll number.*

**Part A**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Answer ALL the Questions. Each question carries 2marks. 10Q x 2M=20M** | | | | |
| **1.** | What is the purpose of input validation in web security? | **2 Marks** | **L1** | **CO1** |
| **2.** | Differentiate between blacklist and whitelist validation. | **2 Marks** | **L2** | **CO1** |
| **3.** | What are the three factors used in multi-factor authentication? | **2 Marks** | **L1** | **CO2** |
| **4.** | Mention two common attacks on password-based authentication systems. | **2 Marks** | **L2** | **CO2** |
| **5.** | What is the importance of session token randomness in session management? | **2 Marks** | **L1** | **CO3** |
| **6.** | Define Cross-Site Scripting (XSS) and mention one way to prevent it. | **2 Marks** | **L1** | **CO3** |
| **7.** | What is the Same-Origin Policy in browsers? | **2 Marks** | **L1** | **CO3** |
| **8.** | Give an example of an SQL injection and its impact. | **2 Marks** | **L1** | **CO4** |
| **9.** | What is an HTTP header injection attack? | **2 Marks** | **L1** | **CO4** |
| **10.** | Explain the concept of forceful browsing. | **2 Marks** | **L1** | **CO4** |

**Part B**

**Answer the Questions. Total Marks 80M**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 11. | a. | Describe the role of cookies in web applications. How can cookies be exploited, and what measures can be taken to secure them? | 10 Marks | L1 | CO1 |
| Or | | | | | |
| 12. | **a.** | What is Attack Surface Reduction (ASR)? Discuss different strategies used to minimize the attack surface in web applications. | **10 Marks** | **L1** | **CO1** |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 13. | a. | Discuss the pros and cons of using password-based authentication for web applications. Suggest ways to make it more secure. | 10 Marks | L2 | CO2 |
| Or | | | | | |
| 14. | **a.** | Identify biometric authentication and password-less authentication in terms of security, usability, and implementation challenges. | **10 Marks** | **L2** | **CO2** |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 15. | a. | Explain the complete lifecycle of a web session and discuss the security concerns at each stage. | 10 Marks | L2 | CO3 |
| Or | | | | | |
| 16. | **a.** | Explain Cross-Site Scripting (XSS) vulnerabilities, their types, and methods to mitigate them. | **10 Marks** | **L2** | **CO3** |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 17. | a. | Examine the process of injecting malicious content into interpreted contexts. How does this pose a security threat in web applications? | 10 Marks | L3 | CO4 |
| Or | | | | | |
| 18. | **a.** | Apply HTTP Header Injection to an application. Explain how attackers manipulate headers and the implications for web security. | **10 Marks** | **L3** | **CO4** |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 19. | a. | Describe the working of Nessus as a vulnerability scanner. Illustrate how Nessus identifies high-risk vulnerabilities with examples from a real scan report. | 10 Marks | L1 | CO1 |
|  | **b.** | Explain the use of Wireshark in capturing and analyzing HTTP, HTTPS, and DNS packets. Explain how to detect anomalies in the traffic. | **10 Marks** | **L2** | **CO2** |
| Or | | | | | |
| 20. | **a.** | Describe active scanning and passive detection in Nessus. Evaluate their strengths and weaknesses in different environments. | **10 Marks** | **L1** | **CO1** |
|  | **b.** | Explain the role of HTTPS in protecting login credentials. Demonstrate how Wireshark behaves differently for HTTP vs HTTPS traffic capture. | **10 Marks** | **L2** | **CO2** |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 21. | a. | Explain how network traffic captured using Wireshark from a login page can expose security flaws such as credentials over plaintext protocols. | 10 Marks | L2 | CO3 |
|  | **b.** | Establish the use of Burp Suite to detect and exploit vulnerabilities like XSS or SQL Injection. | **10 Marks** | **L3** | **CO4** |
| Or | | | | | |
| 22. | **a.** | Describe the process of intercepting login requests using Burp Suite. Analyze how weak login mechanisms can be exploited using this tool. | **10 Marks** | **L2** | **CO3** |
|  | **b.** | Determine the various scan types in Nmap and their use in identifying live hosts and open ports. | **10 Marks** | **L3** | **CO4** |