0402E1423

Candidate's Seat No :_____

MSc Sem.-1 Examination

403

Cyber Security & Forensics

February-2025

Time : 2-30 Hours] [Max. Marks : 70

Question 1 Answer the following questions:

i. An API in a web application allows cross-origin requests from all domains without restriction, which attackers exploit by embedding malicious JavaScript on external websites. How does unrestricted CORS implementation pose a security risk, and what secure policy changes can be implemented? 7Marks

ii. Explain how DNS works, with example. Illustrate your explanation with a practical example of resolving a domain name to an IP address 7Marks

OR

i. What is a Three-Tier Architecture in web applications? Explain its components with an example of how they interact to handle a user request. 7Marks

ii. An online shopping website offers discounts to new users but uses browser cookies to track user eligibility. Returning customers delete their cookies to repeatedly claim discounts. How does this demonstrate a flaw in the application's logic? Propose a secure mechanism to track user eligibility that cannot be bypassed by clearing cookies. 7Marks

Question 2 Answer the following questions:

i. A user on a blogging platform accesses their profile by visiting https://example.com/profile?id=123. Changing the ID parameter in the URL allows the user to view other users' profiles. Describe the vulnerability, its impact on security and privacy, and propose mitigation strategies. 7Marks

ii. Discuss the various types of HTTP request and response methods commonly used in web applications. Explain the significance of each method and how they contribute to different operations like data retrieval, modification, and interaction with the server. 7Marks

OR

i. What are vulnerable and outdated components in the context of web applications? How can they be identified and managed? 7Marks

ii. A blog comment section allows users to submit JavaScript code, which gets executed in other users' browsers. Describe vulnerability associated with it. How might attackers use it? Propose a mitigation technique. 7Marks

Question 3 Answer the following questions:

i. Explain Vulnerability Assessment process and different types of vulnerability assessments. 7Marks

ii. A web application allows users to reset their passwords by entering their email addresses. However, there is no verification mechanism, and attackers use automated tools to identify valid email accounts associated with the application. Analyze the risks of this approach and recommend a secure workflow for password reset functionality. 7Marks

(P.T.O)

OR

i. Explain detailed process of investigating Email Addresses using OSINT. 7Marks

ii. An attacker uses a brute-force tool to target the login page of a company's web application, exploiting weak passwords. The application does not have account lockout policies or monitoring in place. Analyze how these weaknesses can be exploited and suggest a comprehensive strategy to strengthen authentication mechanisms. 7Marks

Questions 4 Answer the following questions:

i. Explain the differences between Local File Inclusion (LFI) and Remote File Inclusion (RFI) vulnerabilities. How can attackers exploit these vulnerabilities, and what strategies can be employed to prevent them? 7Marks

ii. Explain how clickjacking works and discuss the security implications of such attacks on sensitive web applications. 7Marks

OR

i. An online store offers a discount code for new users, but due to a flaw in the business logic, returning customers can use the code repeatedly. Analyse the risks of business logic flaws in this scenario and suggest strategies to detect and prevent such issues during development. 7Marks

ii. A login page is exploited by injecting admin'-- into the username field. Describe vulnerability associated with it and outline preventive measures. 7Marks

Questions 5: Attempt any Seven out of Twelve. 14Marks

1. Difference between web applications and cloud applications.
2. Explain how XSS vulnerabilities can compromise session security.
3. How can API integrations compromise a web application if not securely implemented?
4. What does the "what you have" category of authentication represents?
5. Give any 4 differences between CVSS v2 and CVSS v3.
6. What is the difference between passive and active footprinting?
7. Why is assessing firmware vulnerabilities in IoT devices critical for network security?
8. How does excessive error message exposure aid attackers in crafting injection attacks?
9. Why is a lack of session expiration a critical flaw in penetration testing?
10. What is black box, grey box and white box penetration testing?
11. What is -Pn scan in Nmap and why do we use it?
12. What is the purpose of the Repeater in Burp Suite?