Practice Questions

1. Explain the structure of an HTTP request and response. How do headers, status codes, and message bodies contribute to web communication?
2. Discuss the role of cookies in web applications. How can cookies be exploited, and what measures can be taken to secure them?
3. Describe different types of HTTP status codes and their significance in web security. Provide examples for each category.
4. Compare and contrast different encoding schemes used in web applications, such as URL encoding, HTML encoding, Unicode encoding, Base64 encoding, and Hex encoding.
5. Explain the Base64 encoding technique and its applications. Convert the word "Cat" into its Base64 representation.
6. Explain the Hex encoding technique and its applications. Convert the word "Cat" into its Hex representation.
7. Explain the process of web application enumeration. How do attackers and security professionals use web spidering to analyze applications?
8. Describe the various security vulnerabilities associated with web applications. Discuss how input validation can prevent these vulnerabilities.
9. What are the key differences between server-side and client-side functionality in web applications? Explain how each contributes to security risks.
10. What is cross-site scripting (XSS)? Discuss the different types of XSS attacks and their prevention mechanisms.
11. Explain SQL injection attacks. How do attackers exploit SQL vulnerabilities, and what best practices can be used to prevent them?
12. Discuss the importance of session management in web security. How can weak session management lead to security breaches?
13. Define the CIA triad (Confidentiality, Integrity, and Availability). How does each principle contribute to securing web applications?
14. What is the STRIDE threat model? Explain each category and how it helps in identifying potential security threats.
15. What is Attack Surface Reduction (ASR)? Discuss different strategies used to minimize the attack surface in web applications.
16. Explain the concept of authentication and authorization in web security. How do these mechanisms protect user data?

17. Describe the role of JavaScript in web security. How can JavaScript be exploited by attackers, and what security measures should developers implement?
18. Discuss the significance of logging and monitoring in web security. How do access logs, error logs, and security logs help in threat detection?
19. Explain how hidden form fields can be manipulated by attackers. What security best practices should be followed to prevent such attacks?
20. Describe how an attacker can exploit insecure URL parameters. What techniques can be used to protect web applications from parameter tampering?
21. What is non-repudiation in web security? Provide real-world examples where non-repudiation is crucial.
22. Explain the rules of thumb for reducing the attack surfaces. Discuss the different ways of categorizing threats.
23. Explain the different types of authentication methods and compare their security levels.
24. Describe the working of two-factor authentication (2FA) and explain how it enhances security compared to single-factor authentication.
25. Discuss the different categorization of Web Application Authentication, with example?
26. Discuss the pros and cons of using password-based authentication for web applications. Suggest ways to make it more secure.
27. Explain the advantages and disadvantages of implementing SSO in enterprise applications. How can it be made more secure?
28. What are the common password attacks (e.g., brute-force, dictionary, phishing)? Discuss ways to mitigate these attacks.
29. Analyze the impact of session fixation on authentication security. How can developers prevent it?
30. What are common implementation flaws in authentication mechanisms? Provide examples and explain how they can be fixed.
31. How does OAuth 2.0 enhance authentication security? Explain its working with an example.
32. Discuss why password complexity requirements alone are not enough for security. What additional security measures should be implemented?
33. Define the network inspection commands with example
34. A security analyst wants to perform a deep vulnerability scan on a company's web server by using Advanced Scan in Nessus. Which type of Nessus scan should they use, and how does it differ from a basic network scan?

35. Your organization suspects unauthorized devices are connected to the internal network. You are assigned to perform a basic network scan using Nessus to identify active hosts and their open ports.
    a) Describe the steps you would take to perform this scan using Nessus.
    b) What information will the Nessus report provide?
36. What are the categorizations of threats in Nessus? How is it prioritized?
37. A cybersecurity analyst wants to monitor HTTP traffic to detect potential unauthorized login attempts on a company's website.
    a) How would they configure Wireshark to capture only HTTP traffic?
    b) What specific packet details should they analyze for suspicious activity?
38. A company is concerned about open ports exposing their database server (192.168.1.10) to potential attacks. What Nmap command should be used to check for open ports and running services on this server?
39. Explain the role of Wireshark in Network Security.
40. During a vulnerability assessment, you are capturing thousands of packets. Why are filters important in Wireshark, and what is the difference between display filters and capture filters?
41. A cybersecurity team is planning to conduct a vulnerability assessment on their corporate network. How does Nmap help in this process, and why is it a preferred tool for network scanning?
42. How would you use Nmap to detect open ports and identify the running services on **IP 192.168.1.10**? How would you scan an entire subnet (192.168.1.0/24) to identify all live hosts, in a range of IP addresses.