Introduction & Experience

1. Can you give a brief introduction about yourself?

2. How many web applications and APIs have you tested so far?

3. How would you rate your skills in web application and API testing on a scale of 1 to 10?

4. Which types of applications have you tested most—banking, e-commerce, SaaS, etc.?

5. Can you describe a challenging vulnerability you found and how you reported it?

SQL Injection (SQLi)

6. What is SQL Injection?

7. Can you give one test case for SQL Injection in a web application?

8. How do you test SQL Injection manually?

9. How can SQL Injection be tested in an automated way (e.g., SQLMap)?

10. What are common mitigation techniques for SQL Injection?

11. What is blind SQL Injection, and how is it different from regular SQLi?

12. How do you prevent SQL Injection in prepared statements?

Cross-Site Scripting (XSS)

13. What is Cross-Site Scripting (XSS)?

14. Can you provide some test cases for XSS (stored, reflected, DOM-based)?

15. How can XSS be mitigated in web applications?

16. What is the difference between stored, reflected, and DOM-based XSS?

17. How do Content Security Policy (CSP) headers help prevent XSS?

Remote & Local Vulnerabilities

18. What is Remote Code Execution (RCE), and how does it occur?

19. What is Local File Inclusion (LFI), and how can it be exploited?

20. What is Remote File Inclusion (RFI), and how can it be exploited?

21. What is a file upload vulnerability, and how do you test for it?

22. How can file upload vulnerabilities be mitigated?

23. What are path traversal vulnerabilities, and how are they different from LFI/RFI?

API Security

24. Can you explain API vulnerabilities like BOLA, BFLA, and BOPLA?

25. What is mass assignment? Can you provide an example?

26. What is API authentication vs. authorization?

27. What is rate limiting, and why is it important for API security?

28. What are common ways to test REST and SOAP APIs for security?

29. What are the differences between REST and SOAP APIs in terms of security?

Web Security Headers & Cookies

30. What are some important security headers used in web applications, and what are their purposes?

31. What are the important cookie attributes for security (HttpOnly, Secure, SameSite)?

32. How does CORS affect web application security?

33. How do you test CORS misconfigurations?

34. How can Clickjacking attacks be prevented using headers?

Other Web Vulnerabilities

35. What is SSRF (Server-Side Request Forgery), and how do you test for it?

36. What is CSRF (Cross-Site Request Forgery), and how can it be prevented?

37. What is insecure deserialization, and how can it lead to RCE?

38. How do you test for open redirect vulnerabilities?

39. What is HTTP parameter pollution (HPP), and how is it exploited?

40. How do you test for subdomain takeover vulnerabilities?

Cross / Advanced Questions

SQL Injection & API

41. How would SQLi in a web app differ from SQLi in an API endpoint?

42. Can a blind SQL Injection lead to data exfiltration in an API? How?

43. How can mass assignment issues in APIs lead to SQL Injection or privilege escalation?

XSS & Cookie/CORS

44. How can XSS be exploited to steal cookies even if HttpOnly is enabled?

45. Can a misconfigured CORS policy amplify XSS attacks? Explain with an example.

46. How does DOM-based XSS differ in impact between web apps and mobile hybrid apps?

File Upload & RCE

47. How can a file upload vulnerability lead to Remote Code Execution?

48. What are the differences in mitigating RCE via file upload versus LFI/RFI?

49. Can insecure deserialization combined with file upload lead to RCE? How?

API Security Cross Questions

50. How would you exploit a BOLA vulnerability differently in REST vs SOAP APIs?

51. How does rate-limiting help prevent brute force or BFLA attacks in APIs?

52. How can mass assignment in an API lead to BOLA or BOPLA vulnerabilities?

Web Headers, Cookies & XSS/CSRF

53. How do security headers like CSP, X-Frame-Options, and SameSite work together to prevent XSS and CSRF?

54. Can improperly configured cookies and CORS headers lead to session hijacking? Explain.

55. How would you combine CSRF and XSS in an attack scenario?

LFI/RFI & SSRF

56. How can LFI or RFI be used to perform SSRF attacks?

57. Can you chain LFI with file upload to achieve RCE? How?

58. What is the impact of LFI/RFI on internal network scanning and API endpoints?

Authentication & Authorization

59. How can BOLA in APIs lead to privilege escalation in web apps?

60. How would you test for horizontal vs vertical privilege escalation in a web app or API?

61. Can weak session management combined with XSS lead to account takeover?

Advanced Attack Chaining

62. Give an example of chaining vulnerabilities: SQLi → RCE → Privilege Escalation.

63. How can SSRF be used to bypass firewall rules and access internal APIs?

64. How can a misconfigured REST API allow attackers to exploit file upload or XSS vulnerabilities?

Testing & Automation

65. How would you prioritize testing for vulnerabilities when time is limited?

66. Can automated tools fully replace manual testing for XSS, SQLi, or API vulnerabilities? Why or why not?

67. How do you validate that mitigations (CSP, prepared statements, cookie attributes) are working properly?