70 Application Security Engineer Interview Questions to Ask Candidates

Questions

1. Can you explain the concept of Cross-Site Scripting (XSS) and how you would prevent it in a web application?

2. What is the difference between authentication and authorization? How would you implement them securely in an application?

3. Describe the OWASP Top 10 and why it's important for application security.

4. How would you approach securing an API endpoint? What considerations would you keep in mind?

5. Explain the concept of 'Least Privilege' and how you would apply it in application design.

6. What tools or techniques do you use for static code analysis? How do they improve application security?

7. How would you handle sensitive data storage in an application? What encryption methods would you recommend?

8. Can you describe a time when you identified and mitigated a security vulnerability in an application?

9. What is your approach to security testing in a CI/CD pipeline?

10. How do you stay updated with the latest application security threats and mitigation techniques?

11. How do you conduct a security review of a new application feature?

12. What steps would you take if you discovered a vulnerability in a live application?

13. How do you educate your team about security best practices?

14. How do you prioritize security tasks in a development project?

15. What experience do you have with incident response planning?

16. Can you explain the importance of security in the software development lifecycle (SDLC)?

17. How do you integrate security practices into an agile development environment?

18. Explain the concept of threat modeling and how you apply it to software development.

19. What strategies do you use to prevent SQL injection attacks?

20. Can you discuss the implications of using third-party libraries in terms of security?

21. How would you secure data in transit between microservices?

22. Describe how you would implement a security incident and event management (SIEM) system.

23. What methods do you use to ensure secure coding practices are followed by the development team?

24. How would you conduct a security audit for a new application?

25. Discuss the concept of zero trust architecture and its relevance in application security.

26. What is your approach to handling security patches and updates in a large-scale application?

27. How do you evaluate the security posture of a cloud-based application?

28. What measures would you take to protect against distributed denial-of-service (DDoS) attacks?

29. How do you assess the security risks of deploying an application in a containerized environment?

30. Can you describe the importance of logging and monitoring in application security?

31. What steps would you take to ensure compliance with data protection regulations like GDPR in an application?

32. How would you start a threat modeling process for a new application?

33. How do you ensure that threat modeling remains an integral part of the development lifecycle?

34. What steps would you take if a serious threat is identified during the threat modeling process?

35. Can you explain how you would use threat modeling to improve application security over time?

36. How would you approach conducting a vulnerability assessment on a complex web application?

37. What tools do you prefer for automated vulnerability scanning, and why?

38. Can you explain the difference between authenticated and unauthenticated vulnerability scans?

39. How do you prioritize vulnerabilities found during an assessment?

40. What steps would you take to validate a potential SQL injection vulnerability?

41. How would you assess the security of a mobile application?

42. Can you describe a time when you discovered a critical vulnerability that automated tools missed?

43. What strategies do you use to minimize false positives in vulnerability reports?

44. How do you approach assessing the security of APIs?

45. Imagine you are in the middle of a project and discover a significant security flaw. How do you communicate this to your team and management?

46. You're tasked with securing an application that's already in production. What steps would you take to prioritize and address security vulnerabilities?

47. A development team insists on using a third-party library despite your concerns about its security. How would you handle this situation?

48. If a new security vulnerability is announced that affects a library you use, what process do you follow to address this in your application?

49. Imagine a colleague implements a feature that could potentially expose sensitive user data. How would you approach discussing this with them?

50. You are reviewing code and notice patterns that could lead to security issues. What feedback would you provide to the developer?

51. How do you handle pushback from developers when implementing security measures they see as too restrictive or cumbersome?

52. During a security assessment, you find vulnerabilities that are difficult to fix due to legacy code. What approach would you take?

53. If a new threat emerges that could affect your application, how would you evaluate its impact and communicate it to the project team?

54. You have limited time to train a new team about application security practices. What key topics would you prioritize in your training?

55. undefined

56. undefined

57. undefined

58. undefined

59. undefined

60. undefined

61. undefined

62. undefined

63. undefined