Security Interview Questions

1. What is XSS, and how does it pose a security risk in web applications?
2. Explain the concept of output encoding and its role in preventing XSS attacks.
3. How can a Content Security Policy (CSP) help mitigate XSS vulnerabilities?
4. Discuss the impact of XSS on user privacy and data integrity.
5. What are some best practices for developers to prevent XSS attacks in their applications?
6. What is CSRF, and how does it work as an attack vector?
7. Explain the role of anti-CSRF tokens in preventing CSRF attacks.
8. How does the SameSite cookie attribute contribute to CSRF protection?
9. Discuss scenarios where CSRF attacks can have severe consequences.
10. What are common methods to secure against CSRF attacks in web applications?
11. Why are IFrames a potential security risk, and how can they be used maliciously?
12. Describe techniques to prevent clickjacking and other IFrame-related attacks.
13. How does the X-Frame-Options header contribute to IFrame protection?
14. Differentiate between authentication and authorization in the context of web security.
15. Name and describe key security headers used to enhance web application security.
16. Explain how the Strict-Transport-Security (HSTS) header improves security.
17. Discuss security considerations when using client-side storage mechanisms like cookies and localStorage.
18. How can SameSite cookies and the HttpOnly flag enhance client-storage security?
19. Why is HTTPS important for securing communication between clients and servers?
20. Explain the role of SSL/TLS in establishing a secure connection.
21. How can the use of third-party dependencies introduce security vulnerabilities?
22. Discuss best practices for securing and monitoring dependencies in a web application.
23. What are common compliance standards and regulations related to web application security?
24. How can compliance with standards like GDPR and PCI DSS impact web application security?
25. Why is input validation crucial for preventing security vulnerabilities?
26. What is SSRF, and how can it be exploited by attackers?
27. Discuss methods to prevent SSRF attacks in a web application.

28. What is SSJI, and how does it pose a security risk?
29. How can developers prevent server-side JavaScript injection vulnerabilities?
30. How can these policies help control and restrict certain features in a web application?
31. Explain the purpose of Feature Policy and Permissions-Policy headers in web security.
32. What is SRI, and how does it contribute to the security of external resources?
33. Discuss the implementation and benefits of Subresource Integrity.