Unit-IV

1. **What is the primary purpose of HTTPS in web communication?**
   a. High performance
   b. Data encryption
   c. Content compression
   d. Caching

2. **Which of the following is a common techniqu to prevent Cross-Site Scripting (XSS) attacks**
   a. Cross-Origin Resource Sharing (CORS)
   b. Content Security Policy (CSP)
   c. Secure Sockets Layer (SSL)
   d. Session Cookies

3. **What does CSRF stand for in the context of web security?**
   a. Cross-Site Request Forgery
   b. Cross-Site Scripting Fraud
   c. Cross-Site Resource Falsification
   d. Counter-Strike Rapid Firewall

4. **Which HTTP response status code indicates a successful request in the 2xx range?**
   a. 200 OK
   b. 404 Not Found
   c. 500 Internal Server Error
   d. 302 Found

5. **What is the purpose of a CAPTCHA in web security?**
   a. Data encryption
   b. User authentication
   c. Prevention of automated bots
   d. Cross-site scripting protection

6. **Which of the following is not a common authentication factor?**
   a. Something you know
   b. Something you have
   c. Something you are
   d. Something you want

7. **What is the primary purpose of a WAF (Web Application Firewall) in web security?**
   a. Network monitoring
   b. Malware detection
   c. Intrusion prevention for web applications
   d. DNS filtering

8. **Which HTTP method is considered unsafe and should not be used for sensitive operations due to its idempotent nature?**
   a. GET
   b. POST
   c. DELETE
   d. PUT

9. **What is the purpose of a nonce in web security protocols like OAuth?**
   a. Cryptographic hashing
   b. Random number generation
   c. Data encryption
   d. Session management

10. **Which security mechanism helps protect against SQL injection attacks in web applications?**
a. Secure Sockets Layer (SSL)
b. Content Security Policy (CSP)
c. Input validation
d. Cross-Origin Resource Sharing (CORS)

11. **What is the primary purpose of SSL in web communication?**
a. Data compression
b. Data encryption
c. Session tracking
d. DNS resolution

12. **Which protocol does SSL typically operate over to provide a secure communication channel?**
a. HTTP
b. TCP
c. UDP
d. FTP

13. **Which layer of the OSI model does SSL/TLS operate in?**
a. Application layer
b. Transport layer
c. Network layer
d. Data link layer

14. **What is the successor of SSL and the current standard for secure communication on the web?**
a. TLS (Transport Layer Security)
b. HTTP/2
c. IPsec (Internet Protocol Security)
d. SSH (Secure Shell)

15. **Which type of cryptographic key is used in the SSL handshake process to establish a secure connection?**
a. Public key
b. Private key
c. Session key
d. Master key

16. **Which SSL/TLS handshake step involves the server sending its digital certificate to the client?**
a. Key exchange
b. Server hello
c. Certificate verify
d. Client hello

17. **In SSL/TLS, what is the purpose of the Certificate Authority (CA)?**
a. Encrypting data
b. Verifying server identity
c. Managing session keys
d. Handling DNS resolution

18. **Which cipher suite is considered more secure in SSL/TLS?**
a. DES (Data Encryption Standard)
b. RC4 (Rivest Cipher 4)
c. AES (Advanced Encryption Standard)
d. 3DES (Triple Data Encryption Standard)

19. **What is the purpose of the SSL/TLS record layer?**
a. Key exchange
b. Compression
c. Encryption and integrity
d. Session resumption

20. **Which HTTP status code indicates that the communication is over a secure SSL/TLS connection?**
a. 200 OK
b. 301 Moved Permanently
c. 403 Forbidden
d. 404 Not Found

21. **What is the primary purpose of TLS in communication over the internet?**
a. Data Compression
b. Data encryption
c. IP address resolution
d. Session tracking

22. **Which version of TLS is the successor to SSL 3.0?**
a. TLS 1.0
b. TLS 1.1
c. TLS 1.2
d. TLS 1.3

23. **In the TLS handshake process, which message type does the client send to the server to initiate the key exchange?**
a. Client hello
b. Server hello
c. Certificate
d. Finished

24. **Which protocol layer does TLS operate on in the OSI model?**
a. Application layer
b. Transport layer
c. Network ILayer
d. Data link layer

25. **What is the purpose of the 'change cipher spec' message in the TLS handshake?**
a. To indicate the end of the handshake
b. To change the encryption algorithm
c. To request a new session key
d. To verify the server's digital certificate

26. **Which cryptographic algorithm is commonly used for key exchange in TLS?**
a. RSA
b. AES
c. DES
d. HMAC

27. **What is the purpose of the 'finished' message in the TLS handshake?**
a. To confirm the server's identity
b. To exchange session keys
c. To verify the integrity of the handshake
d. To request data compression

28. **In TLS, what is the purpose of the Hello Retry Request (HRR) message?**
    a. Request a new session key
    b. Request a digital certificate from the client
    c. Indicate a change in the encryption algorithm
    d. Request the client to renegotiate the handshake

29. **Which version of TLS introduced the concept of 'forward secrecy'?**
    a. TLS 1.0 b. TLS 1.1
    c. TLS 1.2 d. TLS 1.3

30. **What is the purpose of the TLS record layer in the TLS protocol?**
    a. Key exchange
    b. Compression
    c. Encryption and integrity
    d. Session resumption

31. **What is the primary goal of Secure Electronic Transactions (SET)?**
    a. Secure data storage
    b. Secure online communication
    c. Secure financial transaction
    d. Secure social media interactions

32. **Which organisation developed the SET protocol to enhance the security of electronic payments?**
    a. World Wide Web Consortium (W3C)
    b. Internet Engineering Task Force (IETF)
    c. Mastercard and visa
    d. Electronic Frontier Foundation (EFF)

33. **In SET, what is the primary function of the Certificate Authority (CA)?**
    a. Encryption of transaction data
    b. Generation of digital signatures
    c. Issuing digital certificates
    d. Handling payment authorisation

34. **What cryptographic technique is commonly used in SET to ensure the confidentiality and integrity of transaction data?**
    a. RSA encryption
    b. SHA-256 hashing
    c. Triple DES (3DES)
    d. Elliptic Curve Cryptography (ECC)

35. **What SET component is responsible for verifying the identity of the parties involved in an electronic transaction?**
    a. Payment gateway
    b. Digital wallet
    c. Secure Socket Layer (SSL)
    d. Digital certificate

36. **In SET, what is the purpose of the payment gateway?**
    a. Encrypting transaction data
    b. Facilitating communication between parties
    c. Issuing digital certificates
    d. Authorising payment transactions

37. **What is the role of the digital wallet in the SET protocol?**
    a. Encrypting credit card numbers
    b. Storing digital certificates
    c. Facilitating payment authorisation
    d. Verifying merchant identities

38. **What SET message is used to request payment authorisation from the cardholder's bank?**
    a. Authorisation request
    b. Payment acknowledgement
    c. Payment confirmation
    d. Payment response

39. **Which SET entity ensures the confidentiality of the cardholder's payment information during a transaction?**
    a. Acquiring bank
    b. Issuing bank
    c. Merchant
    d. Payment gateway

40. **What security feature in SET allows the cardholder to dispute an unauthorised transaction and receive a refund?**
    a. Digital signature
    b. Chargeback protection
    c. Payment confirmation
    d. Authentication token