? EASY (Q1–Q10)

Q1. Web application security focuses on protecting:
A. Only servers
B. Only databases
C. Web applications and their data
D. Network cables

Q2. Which component handles user interaction in a web application?
A. Database
B. Web server
C. Client browser
D. Application server

Q3. Which security objective protects sensitive user data?
A. Availability
B. Confidentiality
C. Integrity
D. Authentication

Q4. Which is a common web application risk?
A. Hardware failure
B. Input validation flaws
C. Power outage
D. Disk crash

Q5. Which HTTP method is used to retrieve data?
A. POST
B. PUT
C. GET
D. DELETE

Q6. Burp Suite is mainly used for:
A. Network routing
B. Web application security testing
C. Malware creation
D. System administration

Q7. Which HTTP header maintains session state?
A. Host
B. User-Agent
C. Cookie
D. Referer

Q8. Which testing approach analyzes a running application?
A. Static analysis
B. Dynamic analysis
C. Code review
D. Compilation

Q9. Identifying assets, threats, and vulnerabilities is part of:
A. Incident response
B. Threat modeling
C. Penetration testing
D. Logging

Q10. Which Burp Suite tool intercepts HTTP traffic?
A. Scanner
B. Repeater
C. Proxy
D. Intruder

□ MEDIUM (Q11–Q25)

Q11. Input handling flaws can lead to:
A. SQL Injection
B. XSS
C. Command Injection
D. All of the above

Q12. Authentication issues primarily affect:
A. Availability
B. Confidentiality
C. Integrity
D. Authorization

Q13. Static application security testing (SAST) analyzes:
A. Running application
B. Network traffic
C. Source code
D. User behavior

Q14. Dynamic application security testing (DAST) analyzes:
A. Source code
B. Compiled binaries
C. Runtime behavior
D. Documentation

Q15. Which HTTP header identifies the requested domain?
A. Referer
B. Host
C. Cookie
D. Authorization

Q16. STRIDE threat model includes:
A. Spoofing
B. Tampering
C. Repudiation
D. All of the above

Q17. Which Burp Suite feature modifies and replays requests?
A. Scanner
B. Repeater
C. Intruder
D. Decoder

Q18. Authorization flaws allow attackers to:
A. Crash the system
B. Access restricted resources
C. Encrypt data
D. Patch vulnerabilities

Q19. HTTP response codes in the 4xx range indicate:
A. Server errors
B. Client errors
C. Redirection
D. Success

Q20. Manual security testing is best suited for:
A. Finding logic flaws
B. Large-scale scanning
C. Automation
D. Performance testing

Q21. Which Burp tool performs automated attacks?
A. Repeater
B. Proxy
C. Intruder
D. Comparer

Q22. Threat actors are:
A. Security tools
B. Vulnerabilities
C. Individuals or entities causing threats
D. Security policies

Q23. Which HTTP method modifies existing resources?
A. GET
B. POST
C. PUT
D. HEAD

Q24. Security-related HTTP headers help prevent:
A. SQL Injection
B. Browser-based attacks
C. Hardware failures
D. Network congestion

Q25. Web vulnerability impact analysis helps in:
A. Performance tuning
B. Risk prioritization
C. UI design
D. Code formatting

🟥 HARD (Q26–Q40)

Q26. Which web application component is most vulnerable to injection attacks?
A. Client browser
B. Application layer
C. Web server OS
D. Network firewall

Q27. Black-box testing means:
A. Full source code access
B. No internal knowledge
C. Partial code access
D. Only documentation access

Q28. White-box testing provides:
A. No access
B. Network-level access
C. Full source code visibility
D. Runtime-only access

Q29. Improper session management can result in:
A. Session hijacking
B. Authentication bypass
C. Account takeover
D. All of the above

Q30. Burp Scanner limitations include:
A. False positives
B. Lack of logic testing
C. Automation dependency
D. All of the above

Q31. DOM-based XSS occurs when:
A. Server reflects input
B. Client-side JavaScript processes data
C. Database stores payload
D. Network injects scripts

Q32. HTTP OPTIONS method can expose:
A. Database structure
B. Supported HTTP methods
C. User credentials
D. Encryption keys

Q33. Threat modeling helps to:
A. Eliminate all threats
B. Identify and prioritize risks
C. Fix vulnerabilities automatically
D. Encrypt applications

Q34. Which Burp feature extends functionality via plugins?
A. Comparer
B. Extender
C. Decoder
D. Intruder

Q35. Application-layer vulnerabilities are difficult to detect because:
A. They require source code
B. They depend on business logic
C. They occur at network layer
D. They are always encrypted

Q36. Automated scanners are weak at detecting:
A. SQL Injection
B. XSS
C. Business logic flaws
D. Misconfigurations

Q37. Which HTTP header prevents clickjacking?
A. X-Frame-Options
B. Content-Type
C. Host
D. Referer

Q38. Risk rating in threat modeling is based on:
A. Asset value only
B. Threat likelihood and impact
C. Vulnerability count
D. Code size

Q39. Which testing approach simulates real attackers?
A. White-box
B. Gray-box
C. Black-box
D. Static testing

Q40. Burp Suite is most effective when combined with:
A. Antivirus
B. Manual testing
C. Firewalls
D. Compilers