? EASY (Q1–Q10)

Q1. In web security, data extraction refers to:
A. Backing up databases
B. Retrieving sensitive data by exploiting vulnerabilities
C. Encrypting application data
D. Compressing server logs

Q2. Which component usually stores sensitive application data?
A. Client browser
B. Network router
C. Database
D. Firewall

Q3. Data extraction attacks mainly affect:
A. Availability
B. Confidentiality
C. Performance
D. Usability

Q4. Which vulnerability is commonly used for data extraction?
A. SQL Injection
B. Clickjacking
C. CSRF
D. CAPTCHA bypass

Q5. Hidden parameters are often discovered by:
A. Packet loss
B. Manual parameter tampering
C. System reboot
D. Encryption

Q6. Information disclosure occurs when:
A. Data is encrypted
B. Error messages reveal sensitive details
C. Logs are deleted
D. Access is denied

Q7. HTTP responses can reveal:
A. Server banners
B. Error messages
C. Status codes
D. All of the above

Q8. Which HTTP method is typically used to retrieve data?
A. POST
B. PUT
C. GET
D. DELETE

Q9. Data extraction is usually the result of:
A. Secure configuration
B. Misconfiguration or vulnerabilities
C. Strong encryption
D. Input validation

Q10. Which analysis involves observing traffic without interaction?
A. Active analysis
B. Passive analysis
C. Exploitation
D. Injection

□ MEDIUM (Q11–Q25)

Q11. Sensitive data exposure can occur due to:
A. Improper access control
B. Verbose error handling
C. Insecure APIs
D. All of the above

Q12. Hidden endpoints are often discovered during:
A. Deployment
B. Advanced reconnaissance
C. Encryption
D. Authentication

Q13. Which technique combines multiple vulnerabilities?
A. Chained exploitation
B. Brute force
C. Sniffing
D. Flooding

Q14. Business logic flaws differ from technical flaws because they:
A. Are network-based
B. Exploit application workflow
C. Depend on encryption
D. Require malware

Q15. Which HTTP method may pose risk if improperly exposed?
A. GET
B. POST
C. PUT
D. All of the above

Q16. Insecure direct object reference (IDOR) allows:
A. Data deletion
B. Unauthorized data access
C. Server crash
D. Malware upload

Q17. Advanced identification techniques rely heavily on:
A. Source code access
B. Response analysis
C. Encryption algorithms
D. Antivirus tools

Q18. Which layer is most responsible for enforcing access control?
A. Client layer
B. Network layer
C. Application server
D. Database storage

Q19. HTTP status code 500 usually indicates:
A. Client error
B. Authentication failure
C. Server error
D. Redirection

Q20. Improper HTTP method handling can lead to:
A. Data manipulation
B. Unauthorized access
C. Logic bypass
D. All of the above

Q21. Advanced exploitation often targets:
A. Network cables
B. Application logic
C. Power supply
D. Hardware chips

Q22. Passive analysis is preferred when:
A. Avoiding detection
B. Exploiting vulnerabilities
C. Modifying data
D. Performing DoS

Q23. Which tool is commonly used to analyze HTTP responses?
A. Burp Suite
B. Wireshark
C. Nessus
D. Hashcat

Q24. Data extraction via XSS mainly targets:
A. Server memory
B. User-side data
C. Network bandwidth
D. Disk storage

Q25. Which misconfiguration exposes unnecessary data?
A. Disabled logging
B. Debug mode enabled
C. Strong encryption
D. Role-based access

🟥 HARD (Q26–Q40)

Q26. Chained vulnerabilities increase risk because they:
A. Are easier to detect
B. Combine multiple weaknesses for higher impact
C. Only affect availability
D. Require insider access

Q27. Which HTTP method should be disabled if not required?
A. GET
B. POST
C. OPTIONS
D. All non-essential methods

Q28. Improper access control is a root cause of:
A. Data extraction
B. Logic flaws
C. Privilege escalation
D. All of the above

Q29. Response-based identification focuses on:
A. Network packets only
B. Server behavior and messages
C. Client UI design
D. Authentication tokens only

Q30. Insecure APIs increase data extraction risk due to:
A. Lack of encryption
B. Excessive data exposure
C. Poor authentication
D. All of the above

Q31. GET requests should not be used for sensitive data because they:
A. Are slower
B. Appear in URLs and logs
C. Require authentication
D. Are encrypted

Q32. Active analysis differs from passive analysis because it:
A. Does not interact with the system
B. Sends crafted requests
C. Only observes traffic
D. Avoids detection

Q33. Which vulnerability enables attackers to bypass workflow restrictions?
A. Logic flaw
B. SQL Injection
C. XSS
D. Buffer overflow

Q34. Improper error handling contributes to:
A. Data leakage
B. Information disclosure
C. Attack surface expansion
D. All of the above

Q35. Which security control best limits data extraction?
A. Encryption only
B. Proper authorization checks
C. Network bandwidth control
D. UI validation

Q36. HTTP/1.1 introduced which security-relevant feature?
A. Stateless connections
B. Persistent connections
C. No headers
D. No methods

Q37. Application-level data extraction is harder to detect because:
A. It uses malware
B. It mimics legitimate requests
C. It crashes servers
D. It blocks logs

Q38. Which analysis best identifies business logic abuse?
A. Automated scanning
B. Manual testing
C. Network sniffing
D. Static code compilation

Q39. Excessive data in API responses indicates:
A. Secure design
B. Over-fetching vulnerability
C. Encryption failure
D. Network issue

Q40. The most effective mitigation against data extraction is:
A. Firewall rules
B. Secure coding and access control
C. Antivirus
D. Obfuscation only