قائمة الاسئلة

امتحان نهاية الفصل الدراسي الثاني - للعام الجامعي 1446 هـ - الموافق -2025/2024م-كلية الحاسوب وتكنولوجيا المعلومات :: تصميم برم

د.محمد محمد صالح الجودة

1) Which testing method analyzes source code without executing the program?
   1) - a) Dynamic Analysis (DAST)
   2) + b) Static Code Analysis (SAST)
   3) - c) Penetration Testing
   4) - d) Chaos Engineering
2) Which tool is used for dynamic application security testing (DAST)?
   1) - a) SonarQube
   2) - b) Checkmarx
   3) + c) OWASP ZAP
   4) - d) Metasploit
3) What is a key benefit of integrating security testing into the SDLC?
   1) - a) Delays deployment timelines
   2) - b) Increases remediation costs
   3) + c) Identifies vulnerabilities early
   4) - d) Reduces user trust
4) During secure code reviews, _____ checks ensure cryptographic functions use strong algorithms.
   1) - a) Input Validation
   2) - b) Authentication
   3) + c) Cryptography
   4) - d) Error Handling
5) The _____ phase of the SDLC involves defining security requirements and threat modeling.
   1) - a) Design
   2) + b) Requirements
   3) - c) Development
   4) - d) Deployment
6) _____ is a tool commonly used for network penetration testing.
   1) - a) Checkmarx
   2) + b) Nmap
   3) - c) SonarQube
   4) - d) OWASP ZAP
7) A future trend in security testing involves _____-driven analysis using AI and machine learning.
   1) - a) Compliance
   2) + b) AI
   3) - c) Containerized
   4) - d) Immersive
8) Which process answers the question, "What are you allowed to access?"
   1) - a) Authentication
   2) + b) Authorization
   3) - c) Tokenization
   4) - d) Encryption
9) Which MFA factor involves using a smartphone app to generate time-based codes?
   1) - a) Something You Know
   2) + b) Something You Have
   3) - c) Something You Are
   4) - d) Somewhere You Are
10) What is the primary purpose of salting passwords before hashing?

1) - a) Speed up authentication
2) - b) Reduce storage requirements
3) + c) Prevent rainbow table attacks
4) - d) Simplify password recovery

11) In RBAC, permissions are assigned to _____, not individual users.
1) - a) Tokens
2) + b) Roles
3) - c) Sessions
4) - d) Scopes

12) The _____ part of a JWT contains metadata like the hashing algorithm.
1) + a) Header
2) - b) Payload
3) - c) Signature
4) - d) Claims

13) _____ is a tool used for simulating heavy server load during authentication testing.
1) - a) Postman
2) - b) OWASP ZAP
3) + c) JMeter
4) - d) Burp Suite

14) A _____ token in OAuth 2.0 allows clients to obtain new access tokens without user interaction.
1) - a) Session
2) + b) Refresh
3) - c) Bearer
4) - d) Access

15) What tool is used for static application security testing (SAST)?
1) - a) OWASP ZAP
2) - b) Burp Suite
3) + c) SonarQube
4) - d) JMeter

16) Which vulnerability is mitigated by implementing anti-CSRF tokens?
1) - a) Cross-Site Scripting (XSS)
2) + b) Cross-Site Request Forgery (CSRF)
3) - c) Insecure Deserialization
4) - d) Buffer Overflow

17) What is the primary purpose of input validation?
1) - a) Ensure data is displayed safely
2) - b) Prevent unauthorized access to logs
3) + c) Restrict data to expected formats and values
4) - d) Encrypt sensitive information

18) The _____ library is recommended for secure cryptographic operations.
1) + a) OpenSSL
2) - b) DOMPurify
3) - c) Hibernate
4) - d) OWASP ZAP

19) _____ tools like OWASP Dependency-Check identify vulnerabilities in third-party components.
1) - a) Static Analysis
2) - b) Dynamic Analysis
3) + c) Dependency Analysis
4) - d) Penetration Testing

20) The _____ phase of secure development involves static and dynamic security testing.
1) - a) Design
2) - b) Development
3) + c) Testing
4) - d) Deployment

21) _____ frameworks like Hibernate help mitigate SQL Injection risks.
1) - a) Authentication
2) + b) ORM
3) - c) CSP
4) - d) SAST

22) Which principle advocates granting minimal access rights necessary to perform tasks?
1) - a) Defense in Depth
2) - b) Open Design
3) + c) Principle of Least Privilege
4) - d) Fail Securely

23) Which strategy employs multiple layers of security controls?
1) - a) Open Design
2) + b) Defense in Depth
3) - c) Fail Securely
4) - d) Secure Factory Pattern

24) What does the Open Design principle emphasize?
1) - a) Security through obscurity
2) - b) Proprietary algorithms for confidentiality
3) + c) Transparency and public scrutiny of security mechanisms
4) - d) Defaulting to granting access during errors

25) Which secure design pattern ensures objects are created with proper security configurations?
1) - a) Singleton Pattern
2) - b) Proxy Pattern
3) + c) Secure Factory Pattern
4) - d) Layered Design

26) The _____ principle avoids relying on design secrecy for security.
1) - a) Defense in Depth
2) + b) Open Design
3) - c) Least Privilege
4) - d) Fail Securely

27) The _____ layer enforces access controls and secure business rules.
1) + a) Business Logic
2) - b) Presentation
3) - c) Data Access
4) - d) Infrastructure

28) The _____ strategy includes firewalls, encryption, and secure coding practices.
1) + a) Defense in Depth
2) - b) Fail Securely
3) - c) Open Design
4) - d) Secure Factory

29) The _____ pattern controls access to sensitive resources.
1) + a) Proxy
2) - b)Singleton
3) - c) Secure Factory

4) - d) Layered

30) Which STRIDE category involves unauthorized impersonation of users or components?
1) - a) Tampering
2) - b) Information Disclosure
3) - c) Repudiation
4) + d) Spoofing

31) Which tool is specifically designed for creating visual system models and automating threat identification using STRIDE?
1) - a) OWASP ZAP
2) - b) Burp Suite
3) - c) OWASP Dependency-Check
4) + d) Microsoft Threat Modeling Tool

32) What mitigation strategy addresses "Repudiation" threats in an e-commerce system?
1) - a) Multi-Factor Authentication
2) - b) End-to-End Encryption
3) - c) Rate Limiting
4) + d) Secure Audit Logging

33) Which future trend focuses on modeling threats in cloud-native environments?
1) - a) AI-Driven Threat Analysis
2) - b) Privacy-Centric Modeling
3) + c) Distributed Architecture Security
4) - d) Physical Security Integration

34) The _____ framework categorizes threats into six types, including Spoofing and Tampering.
1) - a) MITRE ATT&CK
2) - b) PASTA
3) - c) DREAD
4) + d) STRIDE

35) To mitigate _____ threats, implement end-to-end encryption and digital signatures.
1) - a) Spoofing
2) - b) Elevation of Privilege
3) - c) Information Disclosure
4) + d) Tampering

36) The _____ phase of threat modeling involves creating Data Flow Diagrams (DFDs).
1) + a) Create DFD
2) - b) Map Threats
3) - c) Identify Assets
4) - d) Develop Mitigations

37) A challenge in threat modeling is _____, such as overlooking insider threats.
1) - a) Incomplete Asset Identification
2) - b)Overlooking Emerging Threats
3) - c) Ineffective Mitigations
4) + d) Neglecting Human Factors

38) Which phase of SDL involves defining measurable security objectives and KPIs?
1) + a) Requirements and Security Planning
2) - b) Secure Implementation
3) - c) Deployment and Maintenance
4) - d) Security Testing and Verification

39) Which tool is used for static code analysis to identify vulnerabilities early?
1) - a) OWASP ZAP

2) - b) Burp Suite
3) + c) SonarQube
4) - d) Microsoft Threat Modeling Tool

40) What methodology is used during the Design phase to categorize threats like Spoofing and Tampering?
1) - a) DREAD
2) - b) PASTA
3) + c) STRIDE
4) - d) MITRE ATT&CK

41) Which activity is part of the Security Testing and Verification phase?
1) + a) Conducting penetration testing
2) - b) Defining security requirements
3) - c) Implementing secure deployment practices
4) - d) Creating Data Flow Diagrams (DFDs)

42) The _____ tool creates visual threat models using Data Flow Diagrams (DFDs).
1) - a) OWASP ZAP
2) - b) SonarQube
3) - c) Burp Suite
4) + d) Microsoft Threat Modeling Tool

43) _____ is an example of a secure coding practice to prevent SQL injection.
1) - a) Input validation
2) - b) Rate limiting
3) + c) Parameterized queries
4) - d) HSTS headers

44) The _____ phase includes activities like risk assessment and mitigation planning.
1) + a) Design
2) - b) Requirements
3) - c) Security Testing
4) - d) Deployment

45) _____ ensures rapid response to security incidents through predefined protocols.
1) - a) Continuous Monitoring
2) + b) Incident Response Planning
3) - c) Fuzz Testing
4) - d) Threat Modeling

46) Which component of the CIA triad ensures data remains unaltered?
1) - a) Confidentiality
2) + b) Authentication
3) - c) Availability
4) - d) Integrity

47) Which principle restricts users to the minimum access necessary?
1) - a) Defense in Depth
2) - b) Fail Securely
3) - c) Open Design
4) + d)Least Privilege

48) What vulnerability was exploited in the Equifax breach?
1) - a) Heartbleed
2) + b) Apache Struts
3) - c) EternalBlue
4) - d) Shellshock

49) The _____ vulnerability allows attackers to overwrite adjacent memory.

1) + a)Buffer Overflow
2) - b) SQL Injection
3) - c) XSS
4) - d) CSRF

50) A banking app uses JWT tokens (Lecture 6) and bcrypt (Lecture 5). Which OWASP Top 10 items (Lecture 1) do these mitigate?
1) + a) Broken Authentication & Sensitive Data Exposure
2) - b) Injection & Security Misconfiguration
3) - c) XSS & Insecure Deserialization
4) - d) Insufficient Logging & XML External Entities

51) During SDLC's Design phase (Lecture 2), which combination of STRIDE (Lecture 3) and CIA triad (Lecture 1) addresses tampering of audit logs?
1) + a) STRIDE: Tampering → CIA: Integrity
2) - b) STRIDE: Repudiation → CIA: Availability
3) - c) STRIDE: Spoofing → CIA: Confidentiality
4) - d) STRIDE: Elevation of Privilege → CIA: Availability

52) Which toolset pairing best demonstrates Defense in Depth (Lecture 4) for a cloud API?
1) - a) SAST (SonarQube) + DAST (OWASP ZAP)
2) + b) OAuth 2.0 (Lecture 6) + Web Application Firewall (Lecture 4)
3) - c) Threat Modeling (STRIDE) + Parameterized Queries (Lecture 5)
4) - d) Bcrypt (Lecture 5) + SIEM (Lecture 2)

53) A system using "Secure Factory Pattern" (Lecture 4) and "Parameterized Queries" (Lecture 5) primarily mitigates:
1) - a) XSS & Buffer Overflows
2) + b) SQLi & Insecure Deserialization
3) - c) CSRF & Broken Access Control
4) - d) DoS & Information Disclosure

54) In the Equifax breach (Lecture 1), which SDLC phases (Lecture 2) were MOST neglected?
1) - a) Requirements & Design
2) - b) Testing & Deployment
3) + c) Deployment & Maintenance
4) - d) Implementation & Testing

55) Which combination aligns with the Open Design principle (Lecture 4)?
1) - a) Proprietary encryption + Security through obscurity
2) - b) Secret algorithms + Immutable logging
3) - c) Hidden API endpoints + OAuth 2.0
4) + d) AES-256 + Public STRIDE threat models

56) A healthcare app uses RBAC (Lecture 6) and the Principle of Least Privilege (Lecture 4). Which STRIDE threat (Lecture 3) is mitigated?
1) - a) Spoofing
2) - b) Information Disclosure
3) - c) Repudiation
4) + d)Elevation of Privilege

57) Which testing strategy combines SAST (Lecture 8), DAST (Lecture 8), and STRIDE (Lecture 3)?
1) + a) Use SonarQube + OWASP ZAP + Threat Modeling
2) - b) Implement bcrypt + JWT + OAuth
3) - c) Deploy WAF + SIEM + Honeypots
4) - d) Require MFA + HSTS + CSP

58) Which vulnerability chain is possible if Fail Securely (Lecture 4) is ignored during authentication (Lecture

6)?

1) - a) XSS → Session Hijacking
2) - b) SQLi → Data Corruption
3) + c) Authentication Bypass → Elevation of Privilege
4) - d) Buffer Overflow → RCE