**Chapter 11 – Application Security - Answers**

1. Which of the following is not a way for programmers to bypass normal security controls while developing their software?
   1. A back door
   2. A trap door
   3. A maintenance hook
   4. A Trojan horse
2. Which of the following statements pertaining to software testing approaches is correct?
   1. A bottom-up approach allows interface errors to be detected earlier.
   2. A top-down approach allows errors in critical modules to be detected earlier.
   3. The test plan and results should be retained as part of the system's permanent documentation.
   4. Black box testing is predicated on a close examination of procedural detail.
3. In a DBMS, what does cardinality refers to?
   1. The number of rows in a relation.
   2. The number of columns in a relation.
   3. The number of tables in a database.
   4. The number of relations in a database.
4. With regard to databases, which of the following has characteristics of ease of reusing code and analysis and reduced maintenance?
   1. Object-Oriented Data Bases (OODB)
   2. Object-Relational Data Bases (ORDB)
   3. Relational Data Bases
   4. Data base management systems (DBMS)
5. Which of the following would be the most serious risk where a systems development life cycle methodology is inadequate?
   1. The project will be completed late.
   2. The project will exceed the cost estimates.
   3. The project will be incompatible with existing systems.
   4. The project will fail to meet business and user needs.
6. Which of the following types of testing is used to determine if program changes have introduced errors that did not exist before?
   1. Code comparison
   2. Integration testing
   3. Regession testing
   4. Unit testing
7. Which of the following is often the greatest failing of distributed system management solutions?
   1. scalability
   2. security
   3. heterogeneity
   4. synchronization
8. Which of the following test makes sure the modified or new system includes appropriate access controls and does not introduce any security holes that might compromise other systems?
   1. Recovery testing
   2. Security testing
   3. Stress/volume testing
   4. Interface testing
9. Which of the following are placeholders for literal values in a Structured Query Language (SQL) query being sent to the database on a server?
   1. Bind variables
   2. Assimilation variables
   3. Reduction variables
   4. Resolution variables
10. Which of the following is not used as a cost estimating technique during the project planning stage?
    1. Delphi technique
    2. Expert judgment
    3. Program Evaluation Review Technique (PERT) charts
    4. Function points (FP)
11. Operations Security seeks to primarily protect against which of the following?
    1. object reuse
    2. facility disaster
    3. compromising emanations
    4. asset threats
12. Who can best determine if security controls are adequate in a computer-based application system?
    1. system auditor
    2. system owner
    3. system manager
    4. system developer
13. Which of the following is commonly used for retrofitting multilevel security to a database management system?
    1. trusted front-end
    2. trusted back-end
    3. controller
    4. kernel
14. At which of the following phases of a software development life cycle are security and access controls normally designed?
    1. Coding
    2. Product design
    3. Software plans and requirements
    4. Detailed design
15. The primary reason for enabling software audit trails is which of the following?
    1. Improve system efficiency.
    2. Improve response time for users.
    3. Establish responsibility and accountability.
    4. Provide useful information to track down processing errors.
16. In a Web page, why does compiled code pose more risk than interpreted code?
    1. Because malicious code can be embedded in the compiled code and can be difficult to detect.
    2. Because the browser can safely execute all interpreted applets.
    3. Because compilers are not reliable.
    4. It does not. Interpreted code poses more risk than compiled code.
17. Which of the following is a not a control preventing an unauthorized change in a production environment?
    1. Deny programmer access to production data.
    2. Require change requests to include information about dates, descriptions, cost analysis and anticipated effects.
    3. Run a source comparison program between control and current source periodically.
    4. Establish procedures for emergency changes.
18. Which of the following phases of a software development life cycle normally incorporates the security specifications, determines access controls and evaluates encryption options?
    1. Detailed design
    2. Implementation
    3. Product design
    4. Software plans and requirements
19. Which of the following statements pertaining to software testing is incorrect?
    1. Unit testing should be addressed when the modules are being designed.
    2. Test data should be part of the specifications.
    3. Testing should be performed with live data to cover all possible situations.
    4. Test data generators can be used to systematically generate random test data that can be used to test programs.
20. Which of the following is used to create and delete views and relations within tables?
    1. SQL Data Definition Language
    2. SQL Data Manipulation Language
    3. SQL Data Relational Language
    4. SQL Data Identification Language
21. A system file that has been patched numerous times becomes infected with a virus. The anti-virus software warns that disinfecting the file may damage it. What course of action should be taken?
    1. Replace the file with the original version from master media
    2. Proceed with automated disinfection
    3. Research the virus to see if it is benign
    4. Restore an uninfected version of the patched file from backup media
22. Java is not:
    1. Object-oriented
    2. Distributed
    3. Compiled
    4. Multithreaded
23. Which of the following phases of a system development life-cycle is most concerned with authenticating users and processes to ensure appropriate access control decisions?
    1. Development/acquisition
    2. Implementation
    3. Operation/Maintenance
    4. Initiation
24. Which model, based on the premise that the quality of a software product is a direct function of the quality of its associated software development and maintenance processes, introduced five levels with which the maturity of an organization involved in the software process is evaluated?
    1. The Total Quality Model (TQM)
    2. The IDEAL Model
    3. The Software Capability Maturity Model
    4. The Spiral Model
25. A security evaluation report and an accreditation statement are produced in which of the following phases of the system development life cycle?
    1. requirements definition phase
    2. design phase
    3. development phase
    4. testing phase
26. What is one disadvantage of content-dependent protection of information?
    1. It increases processing overhead.
    2. It requires additional password entry.
    3. It exposes the system to data locking.
    4. It limits the user's individual address space.
27. Which of the following is a communication mechanism that enables direct conversation between two applications?
    1. DDE
    2. OLE
    3. ODBC
    4. DCOM
28. A persistent collection of interrelated data items can be defined as which of the following?
    1. database
    2. database management system
    3. database security
    4. database shadowing
29. Which of the following refers to the work product satisfying the real-world requirements and concepts?
    1. validation
    2. verification
    3. concurrence
    4. accuracy
30. Which of the following does not address Database Management Systems (DBMS) Security?
    1. Perturbation
    2. Cell suppression
    3. Padded cells
    4. Partitioning
31. Operation security requires the implementation of physical security to control which of the following?
    1. unauthorized personnel access
    2. incoming hardware
    3. contingency conditions
    4. evacuation procedures
32. Which of the following would be the best reason for separating the test and development environments?
    1. To restrict access to systems under test.
    2. To control the stability of the test environment.
    3. To segregate user and development staff.
    4. To secure access to systems under development.
33. Which of the following is a primary purpose for conducting parallel testing?
    1. To enable comprehensive unit and system testing.
    2. To ensure the new system meets all user requirements.
    3. To determine if the system is more cost-effective.
    4. To validate new changes to a system.
34. In regards to relational database operations, which of the following is used to create a plan and fix or resolve the plan?
    1. Bind
    2. Assimilation
    3. Reduction
    4. Resolution
35. Risk reduction in a system development life-cycle should be applied:
    1. Mostly to the initiation phase.
    2. Mostly to the development phase.
    3. Mostly to the disposal phase.
    4. Equally to all phases.
36. Which virus category has the capability of changing its own code, making it harder to detect by anti-virus software?
    1. Stealth viruses
    2. Polymorphic viruses
    3. Trojan horses
    4. Logic bombs
37. Risk analysis is MOST useful when applied during which phase of the system development process?
    1. Project initiation
    2. Requirements definition
    3. System construction
    4. Implementation planing
38. At what stage of the applications development process should the security department become involved?
    1. Prior to the implementation
    2. Prior to systems testing
    3. During unit testing
    4. During requirements development
39. Which of the following represents the best programming?
    1. Low cohesion, low coupling
    2. Low cohesion, high coupling
    3. High cohesion, low coupling
    4. High cohesion, high coupling
40. Which of the following can be defined as a unique identifier in the table that unambiguously points to an individual tuple or record in the table?
    1. primary key
    2. candidate key
    3. secondary key
    4. foreign key
41. Which of the following would MOST likely ensure that a system development project meets business objectives?
    1. Development and tests are run by different individuals
    2. User involvement in system specification and acceptance
    3. Development of a project plan identifying all development activities
    4. Strict deadlines and budgets
42. Why would a database be denormalized?
    1. To ensure data integrity
    2. To increase processing efficiency
    3. To prevent duplication of data
    4. To save storage space
43. Which of the following is not a defined maturity level within the Software Capability Maturity Model?
    1. Repeatable
    2. Defined
    3. Managed
    4. Oriented
44. In an on-line transaction processing system, which of the following actions should be taken when erroneous or invalid transactions are detected?
    1. The transactions should be dropped from processing.
    2. The transactions should be processed after the program makes adjustments.
    3. The transactions should be written to a report and reviewed.
    4. The transactions should be corrected and reprocessed.
45. Which of the following represents a relation, which is the basis of a relational database?
    1. One-dimensional table
    2. Two-dimensional table
    3. Three-dimensional table
    4. Four-dimensional table
46. What can be defined as an attribute that is a unique identifier within a given table?
    1. A primary key
    2. A foreign key
    3. A secondary key
    4. A candidate key
47. Which of the following is an advantage in using a bottom-up versus a top-down approach to software testing?
    1. Interface errors are detected earlier.
    2. Errors in critical modules are detected earlier.
    3. Confidence in the system is achieved earlier.
    4. Major functions and processing are tested earlier.
48. Which of the following represents the rows of the table in a relational database?
    1. attributes
    2. records or tuples
    3. record retention
    4. relation
49. What is called the act of obtaining information of a higher sensitivity by combining information from lower levels of sensitivity?
    1. Polyinstantiation
    2. Inference
    3. Aggregation
    4. Data mining
50. What is called the number of columns in a table?
    1. Schema
    2. Relation
    3. Degree
    4. Cardinality
51. A department manager has read access to the salaries of the employees in his/her department but not to the salaries of employees in other departments. A database security mechanism that enforces this policy would typically be said to provide which of the following?
    1. content-dependent access control
    2. context-dependent access control
    3. least privileges access control
    4. ownership-based access control
52. Development staff should:
    1. Implement systems.
    2. Support production data.
    3. Perform unit testing.
    4. Perform acceptance testing.
53. During which phase of an IT system life cycle are security requirements developed?
    1. Operation
    2. Initiation
    3. Development
    4. Implementation
54. A TCP SYN attack:
    1. requires a synchronized effort by multiple attackers.
    2. takes advantage of the way a TCP session is established.
    3. may result in elevation of privileges.
    4. is not something system users would notice.
55. Which of the following phases of a software development life cycle normally addresses reasonable care and due diligence?
    1. Implementation
    2. System feasibility
    3. Product design
    4. Software plans and requirements
56. Buffer overflow and boundary condition errors are subsets of which of the following?
    1. Race condition errors.
    2. Access validation errors.
    3. Exceptional condition handling errors.
    4. Input validation errors.
57. What is the main purpose of undertaking a parallel run of a new system?
    1. Resolve any errors in the program and file interfaces
    2. Verify that the system provides required business functionality
    3. Validate the operation of the new system against its predecessor
    4. Provide a backup for the old system
58. Which of the following best explains why computerized information systems frequently fail to meet the needs of users?
    1. Inadequate quality assurance (QA) tools.
    2. Constantly changing user needs.
    3. Inadequate user participation in defining the system's requirements.
    4. Inadequate project management.
59. Which of the following is an advantage of prototyping?
    1. Prototype systems can provide significant time and cost savings.
    2. Change control is often less complicated with prototype systems.
    3. It ensures that functions or extras are not added to the intended system.
    4. Strong internal controls are easier to implement.
60. Which of the following database implementations would be best defined as interconnected platforms running independent copies of software with independent copies of data?
    1. Decentralized
    2. Centralized
    3. Interoperable or cooperative
    4. Dispersed
61. Sensitivity labels are an example of:
    1. Preventive controls
    2. Detective controls
    3. Compensating controls
    4. Corrective controls
62. Which of the following evaluates the product against the specification?
    1. verification
    2. validation
    3. concurrence
    4. accuracy
63. Which of the following statements relating to Distributed Computing Environment (DCE) is FALSE?
    1. It is a layer of software that sits on the top of the network layer and provides services to the applications above it.
    2. It uses a Universal Unique Identifier (UUID) to uniquely identify users, resources and components.
    3. It provides the same functionality as DCOM, but is more proprietary.
    4. It is a set of management services with a communication layer based on RPC.
64. Complex applications involving multimedia, computer aided design, video, graphics, and expert systems are more suited to which of the following?
    1. Object-Oriented Data Bases (OODB)
    2. Object-Relational Data Bases
    3. Relational Data Bases
    4. Data base management systems (DBMS)
65. Which of the following is a characteristic of a decision support system (DSS)?
    1. DSS is aimed at solving highly structured problems.
    2. DSS emphasizes flexibility in the decision making approach of users.
    3. DSS supports only structured decision-making tasks.
    4. DSS combines the use of models with non-traditional data access and retrieval functions.
66. The object-relational and object-oriented models are better suited to managing complex data such as required for which of the following?
    1. computer-aided develop and imaging.
    2. computer-aided duplexing and imaging.
    3. computer-aided processing and imaging.
    4. computer-aided design and imaging.
67. What are edit controls?
    1. Preventive controls
    2. Detective controls
    3. Corrective controls
    4. Compensating controls
68. Which of the following files should the security administrator be restricted to READ only access?
    1. Security parameters
    2. User passwords
    3. User profiles
    4. System log
69. In SQL where is the actual data stored?
    1. Views
    2. Tables
    3. Schemas and sub-schemas
    4. Index-sequential tables
70. What is RAD?
    1. A development methodology
    2. A project management technique
    3. A measure of system complexity
    4. Risk-assessment diagramming
71. What can be defined as the verification that performance and security requirements have been met?
    1. Accreditation
    2. Certification
    3. Assurance
    4. Acceptance
72. Which of the following has the objective to control and manage data from a central location?
    1. Databases
    2. Data dictionaries
    3. Data access methods
    4. Data storage
73. Which expert system operating mode allows determining if a given hypothesis is valid?
    1. Vertical chaining
    2. Lateral chaining
    3. Forward chaining
    4. Backward chaining
74. Which of the following is based on the premise that the quality of a software product is a direct function of the quality of its associated software development and maintenance processes?
    1. The Software Capability Maturity Model (CMM)
    2. The Spiral Model
    3. The Waterfall Model
    4. Expert Systems Model
75. Which of the following is an advantage of using a high-level programming language?
    1. It decreases the total amount of code written
    2. It allows programmers to define syntax
    3. It requires programmer-controlled storage management
    4. It enforces coding standards
76. Which of the following is best defined as a circumstance in which a collection of information items is required to be classified at a higher security level than any of the individual items that comprise it?
    1. Aggregation
    2. Inference
    3. Clustering
    4. Collision
77. Matches between which of the following are important because they represent references from one relation to another and establish the connections among these relations?
    1. foreign key to primary key
    2. foreign key to candidate key
    3. candidate key to primary key
    4. primary key to secondary key
78. Which of the following best describes the purpose of debugging programs?
    1. To generate random data that can be used to test programs before implementing them.
    2. To ensure that program coding flaws are detected and corrected.
    3. To protect, during the programming phase, valid changes from being overwritten by other changes.
    4. To compare source code versions before transferring to the test environment
79. Which of the following can be defined as the process of rerunning a portion of the test scenario or test plan to ensure that changes or corrections have not introduced new errors?
    1. Unit testing
    2. Pilot testing
    3. Regression testing
    4. Parallel testing
80. A computer program in which malicious or harmful code is contained inside apparently harmless programming or data in such as way that it can get control and do damage is a:
    1. virus
    2. worm
    3. Trojan horse
    4. trap door
81. Which of the following would not correspond to the number of primary keys found in a table in a relational database?
    1. Degree
    2. Number of tuples
    3. Cardinality
    4. Number of rows
82. Which of the following phases of a system development life-cycle is most concerned with establishing a sound policy as the foundation for design?
    1. Development/acquisition
    2. Implementation
    3. Initiation
    4. Maintenance
83. What is used to hide data from unauthorized users by allowing a relation in a database to contain multiple tuples with the same primary keys with each instance distinguished by a security level?
    1. Data mining
    2. Polyinstantiation
    3. Cell suppression
    4. Noise and perturbation
84. Which of the following characteristics pertaining to databases is not true?
    1. A data model should exist and all entities should have a significant name.
    2. Justifications must exist for normalized data.
    3. No NULLs should be allowed for primary keys.
    4. All relations must have a specific cardinality
85. Which of the following is not an element of a relational database model?
    1. Data structures called tables or relations
    2. Integrity rules on allowable values and value combinations within the tables
    3. Operators on data within tables
    4. Security structures called referential validation within tables
86. Which software development model is actually a meta-model that incorporates a number of the software development models?
    1. The Waterfall model
    2. The modified Waterfall model
    3. The Spiral model
    4. The Critical Path Model (CPM)
87. Which question is NOT true concerning Application Control?
    1. It limits end users use of applications in such a way that only particular screens are visible.
    2. Only specific records can be requested choice
    3. Particular uses of the application can be recorded for audit purposes
    4. Is non-transparent to the endpoint applications so changes are needed to the applications involved
88. Which of the following translates source code one command at a time for execution on a computer?
    1. A translator
    2. An interpreter
    3. A compiler
    4. An assembler
89. Which of the following defines the software that maintains and provides access to the database?
    1. database management system (DBMS)
    2. relational database management system (RDBMS)
    3. database identification system (DBIS)
    4. Interface Definition Language system (IDLS)
90. A 'Pseudo flaw' is which of the following?
    1. An apparent loophole deliberately implanted in an operating system program as a trap for intruders
    2. An omission when generating Psuedo-code
    3. Used for testing for bounds violations in application programming
    4. A normally generated page fault causing the system to halt.
91. Which of the following refers to the number of rows in a relation?
    1. cardinality
    2. degree
    3. depth
    4. breadth
92. Which of the following can be defined as an attribute that is a unique identifier within a given table?
    1. primary key
    2. candidate key
    3. foreign key
    4. secondary key
93. In which of the following phases of system development life cycle (SDLC) is contingency planning most important?
    1. Initiation
    2. Development/acquisition
    3. Implementation
    4. Operation/maintenance
94. Which of the following would best describe the difference between white-box testing and black-box testing?
    1. White-box testing is performed by an independent programmer team.
    2. Black-box testing uses the bottom-up approach.
    3. White-box testing examines the program internal logical structure.
    4. Black-box testing involves the business units
95. The description of the database is called a schema, and the schema is defined by which of the following?
    1. Data Encapsulation Language (DEL).
    2. Data Connection Language (DCL).
    3. Data Definition Language (DDL).
    4. Data Identification Language (DIL).
96. Which of the following is an important part of database design that ensures that attributes in a table depend only on the primary key?
    1. Normalization
    2. Assimilation
    3. Reduction
    4. Compaction
97. Which of the following is used in database information security to hide information?
    1. Inheritance
    2. Polyinstantiation
    3. Polymorphism
    4. Delegation
98. Which of the following is the marriage of object-oriented and relational technologies combining the attributes of both?
    1. object-relational database
    2. object-oriented database
    3. object-linking database
    4. object-management database
99. Which of the following refers to the number of columns in a relation?
    1. degree
    2. cardinality
    3. depth
    4. breadth
100. Why do buffer overflows happen?
     1. Because buffers can only hold so much data
     2. Because input data is not checked for appropriate length at time of input
     3. Because they are an easy weakness to exploit
     4. Because of insufficient system memory