CBS 402 Preliminary Examination

Name:_____ Rating:_____

Section:_____

TEST I. Matching Type (No Erasure)

___1. Considered the most common type of authentication
___2. A password attacks that includes phishing and shoulder surfing
___3. An engine where your JavaScript run
___4. uses an event-driven, non-blocking I/O model, making it lightweight and efficient for data-intensive real-time applications
___5. makes it easy to share and reuse code, and it has a large and active community
___6. It is designed to make creating web servers and web applications easier
___7. Is the process of checking if the data entered by the user into a form or API request meets certain criteria
___8. This helps prevent security attacks like SQL injection, cross-site scripting (XSS), or script injection
___9. This is the slowest yet most thorough method.
___10. make password attacks easier by creating a large pre-generated data set of candidate digests.
___11. can significantly reduce the amount of time needed to break a password
___12. consists of a random string that is used in hash algorithms
___13. can be used to create a one-time password (OTP)
___14. contains an integrated circuit chip that can hold information
___15. A front-end framework that provides a built-in mechanism for validating forms.

A. Data Sanitation
B. Express
C. Rainbow table
D. Password
E. Smart Card
F. Validator.js
G. Data Validation
H. Social Engineering
I. V8
J. Password mask
K. Salt
L. Password library
M. Brute Force
N. Token
O. JS engine
P. Node.js
Q. Angular
R. NPM

TEST II. Multiple Choice (NO ERASURE)

___1. Which of these is NOT a reason why users create weak passwords?
A. Most sites force users to create weak passwords even though they do not want to
B. Having multiple passwords makes it hard to remember all of them.
C. A security policy requires a password to be changed regularly.
D. A lengthy and complex password can be difficult to memorize.

___2. A TOTP token code is valid _____.
A. only while the user presses SEND
B. until an event occurs
C. for as long as it appears on the device
D. for up to 24 hours

___3. Which human characteristic is NOT used for biometric identification?
A. Retina
B. Weight
C. face
D. finger

___4. When users combine letters, numbers, and punctuation (character sets), they do it in a pattern.
A. Replacing
B. Changing
C. appending
D. Modifying

___5. An analysis of one theft of 32 million user passwords founds that an occurrence of the password is evident. which of the following password has the highest number of occurrence?
A. 12345678
B. 123456
C. 12345
D. 123456789

___6. These attacks used every possible combination of letters, numbers, and characters are used to create candidate digests that are then matched against those in the stolen digest file.
A. Dictionary
B. Password collection
C. hybrid
D. Brute Force

___7. Which of the following is NOT a types of parameter for brute force attack
A. Language
B. Spelling
C. Skip
D. pattern

___8. In access control terminologies, It is a specific resource, such as a file or a hardware device.
A. Object
B. Operation
C. Subject
D. Identification

___9. This role has the duty to determine the level of security needed for the data
A. Custodian C. subject
B. Owner D. end-user

___10. This role, has the duty to follow all the organization's security guidelines
A. End user C. Custodian
B. Admin D. Owner

___11. This role has the duty to review all the security settings and maintain record of access
A. Custodian C. Owner
B. End-user D. admin

___12. An access control model that is least restrictive.
A. Mandatory Access Control C. Role Based Access Control
B. Rule Based Access Control D. Discretionary Access Control

___13. sometimes called Non-Discretionary Access Control.
A. Mandatory Access Control C. Role Based Access Control
B. Rule Based Access Control D. Discretionary Access Control

___14. This helps reduce the attack surface by eliminating unnecessary privileges that could provide an avenue for an attacker.
A. high privilege C. least privilege
B. common privilege D. data privilege

___15. uses a person's unique physical characteristics for authentication
A. Standard biometric C. Cognitive Biometric
B. Static Biometric D. Dynamic Biometric

___16. Which of the following is not a validation framework
A. Express-validator C. mysql2-validator
B. Laravel validation D. angular

___17. Which of the following is NOT a data sanitation framework
A. sanitize-html C. sanitize-js
B. sqlstring D. sanitizer

___18. Which of the following is NOT a common NPM command
A. npm init C. npm remove
B. nom install D. npm list

___19. Which of the following is NOT a feature of express.js
A. Routing C. template
B. Middleware D. controller

___20. Which of the following is the most restrictive access control model?
A. Mandatory Access Control C. Role Based Access Control
B. Rule Based Access Control D. Discretionary Access Control

TEST III. Enumeration

(5) Types of Data Validation

_____ _____
_____ _____
_____

(5) Types of Data Sanitation

_____ _____
_____ _____
_____

(5) password complexity

_____
_____
_____
_____
_____