1. A user can be associated with

a. zero roles

b. one role

c. multiple roles

d. all of the above

e. none of the above

2. A/an \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ is when an attacker uses a pre-computed database of words and their

hash values in an attempt to crack hashed passwords that they have gained access to.

a. cross-site scripting attack

b. dictionary attack

c. rainbow table attack

d. SQL injection attack

3. An interface that’s used to authenticate users so they can access web resources that have been

restricted is called a

a. realm

b. constraint

c. role

d. none of the above

4. By default, Tomcat stores usernames, passwords, and roles in the

a. the web.xml file

b. the server.xml file

c. a database

d. the tomcat-users.xml file

5. Educating your users about password strength and the dangers of giving out information to

unknown persons can help prevent

a. dictionary attacks

b. rainbow table attacks

c. social engineering attacks

d. cross-site scripting attacks

6. For more serious web applications, the \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ provides a way to access usernames,

passwords, and roles that have been stored in a relational database.

a. JDBCRealm

b. UserDatabaseRealm

c. DataSourceRealm

d. none of the above

7. For simple web applications, the \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ provides a quick and easy way to implement

a realm.

a. JDBCRealm

b. UserDatabaseRealm

c. DataSourceRealm

d. none of the above

8. Since this type of authentication does not automatically encrypt the username and password before

sending them to the server, it is typically used over a secure connection.

a. basic authentication

b. form-based authentication

c. digest authentication

d. both a and b

e. none of the above

9

9. The \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ provides a way to use connection pooling to access usernames,

passwords, and roles that have been stored in a database.

a. JDBCRealm

b. UserDatabaseRealm

c. DataSourceRealm

d. none of the above

10. The security realm provides the authorized

a. usernames and passwords

b. usernames and roles

c. usernames, passwords, and roles

d. passwords and roles

11. To restrict access to a web resource, you add a \_\_\_\_\_\_\_\_\_\_\_\_\_\_ element to the web.xml file.

a. security-constraint

b. auth-constraint

c. security-role

d. web-resource-collection

12. To salt a password, you append the salt value to the original password \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

hashing it.

a. before

b. after

c. while

d. instead of

13. When an application uses basic authentication,

a. the username and password are encrypted before being sent to the server

b. a dialog box automatically prompts the user for a username and password

c. the usernames and passwords are stored in the tomcat-users.xml file

d. the web.xml file provides the path for the login page

14. Which of the following is not included in a security constraint?

a. the URL pattern for the restricted resources

b. the authorized roles for accessing the restricted resources

c. the authorized usernames for accessing the restricted resources

d. all of the above

e. none of the above

15. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ are when an attacker attempts to gain unauthorized access to a system by

tricking users rather than exploiting technical flaws.

a. Cross-site scripting attacks

b. SQL injection attacks

c. Social engineering attacks

d. none of the above

16. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ encrypts data against a key, which can be used to decrypt the data at a later

date when it needs to be read by a user.

a. One-way hashing

b. Reversible encryption

c. Salting

d. none of the above

17. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ prevents rainbow table attacks.

a. Reversible encryption

b. Salting

c. One-way hashing

d. none of the above

10

18. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ is useful for encrypting things such as passwords, where there is no need for

anyone to read the original value of the password.

a. One-way hashing

b. Reversible encryption

c. Salting

d. none of the above