Week 9 Practice questions with Solutions

1] In role-based access control systems_ [MCQ]

1. Users can switch between roles.
2. Users have only a single role.
3. Users have to log in with a new name if they want a new role.
4. Users need permission to log in each time from an administrator.

Answer: Option 1.

Solution: It is possible for a single user to have more than one role, and permission needs to be granted only once.

2] 'Google docs' allows you to share a document with others as "Editor", "Commenter" or "Viewer". What kind of access control system is this? [MCQ]

1. Attribute based access control
2. Role-based access control
3. Discretionary access control
4. Mandatory access control

Answer: Option 2.

Solution: Google docs with the help of Role-based access control provides certain level of access and forms the hierarchy as Editor> Commenter> Viewer.

3] The principle of least privilege recommends that: [MCQ]

1. All users should be able to access the entire system.
2. Users should never be allowed to install software on their own.
3. Users access to system resources should be restricted to the minimum they need to do their work.
4. System administrators can always do whatever they want.

Answer: Option 3.

Solution: Option 1 is the opposite of least privilege. Option 2 is unnecessary. You can allow someone to install software if they need to. Option 4 is unnecessary as even admins should have limits on what they are allowed to do. For example, in data centers generally admin users cannot read data because it is encrypted, but they may be able to delete data since they have access to the system. So they have the administrative power they need, but still cannot read files.

4] Cookies are used to: [MSQ]

1. store session information
2. store values that the server needs to know about the client connection
3. store photographs and documents
4. store values that the client needs to know about the server

Answer: Option 1 and 2.

Solution: Storing large amounts of data like photos is generally not a good idea. Though it could be possible in principle, generally cookies are limited to about 4KB in size, not suitable for documents. Cookies are sent from the client to the server - it does not really make sense to store information that the client needs to know.

5] Sessions are used primarily to: [MCQ]

1. Give the server information about what the client was doing previously.
2. Limit the amount of time a user can connect to a system.
3. Allow the government to intercept communications.
4. None of the above

Answer: Option 1.

Solution: Sessions are used primarily to give the server information about what the client was doing previously. While it may be used sometimes to limit the amount of time a user can connect to a system, it is not the primary use.

6] Secret keys are used by the server while generating cookies to ensure that: [MCQ]

1. The cookie cannot be used on any other server.
2. The user cannot modify the content of the cookie.
3. The server cannot modify the cookie.
4. The user can be logged out if needed.

Answer: Option 2.

Solution: Secret keys are used by the server while generating cookies to ensure that the user cannot modify the content of the cookie. All the others have nothing to do with keeping the cookie secret.

7] HTTPS provides security for_ [MCQ]

1. the entire application.
2. the client.
3. the server.
4. the connection.

Answer: Option 4.

Solution: In case of HTTPS, only the connection is secure.

8] Logging is typically used to_ [MCQ]

1. detect unusual activity on the server.
2. block unauthorized access.
3. enforce HTTPS connections.
4. convert HTTP to HTTPS.

Answer: Option 1.

Solution: Logging is used to detect unusual activity on the server. Others have nothing to do with logging.

9] Time series databases are optimized for queries such as: [MSQ]

1. Most common search terms used on a website.
2. Number of visitors to a website in the last month.
3. Time of day when traffic on a site is maximum.
4. Relationship between customers and orders.

Answer: Option 2 and 3.

Solution: Time series databases are optimized for queries such as number of visitors to a website in the last month or time of day when traffic on a site is maximum. Others don't have any direct relationship with time series.

10] Which of the following is/are true for HTTPS? [MSQ]

1. HTTPS guarantees that no one can ever read the messages you send on a link.
2. HTTPS reduces the likelihood of someone being able to intercept what is on the link itself.
3. When you connect to Gmail and enter your password, the password will be sent over the HTTPS link as plain text and will be visible at the server.
4. All of the above

Answer: Option 2 and 3.

Solution: HTTPS only reduces the likelihood of someone being able to intercept what is on the link itself. If the messages are stored later, or are decrypted and then visible to others, then it can still be seen by others. Initially, the password is sent over the HTTPS link as a plain text and there is nothing to prevent the password from being seen at the server - only after the server has verified the password will it set cookies.

11] Consider two statements on HTTP methods given below: [MCQ]

Statement 1: In a HTTP GET request, all parameters of the request can be logged as part of the URL. Statement 2: In a HTTP POST request, all parameters of the request can be logged as part of the URL.

1. Both statement 1 and statement 2 are correct.
2. Both statement 1 and statement 2 are incorrect.
3. Statement 1 is correct, statement 2 is incorrect.
4. Statement 2 is correct, statement 1 is incorrect.

Answer: Option 3.

Solution: GET pushes all parameters through the URL itself, so it will be logged as part of the URL whereas POST sends the data in the request body, not in the URL.

12] Which of the following statements is true? [MCQ]

1. HTTP basic authentication is the best way of securing a web application.
2. In HTTP basic authentication, the username and password are sent to the server in a secure manner.
3. There are many security issues with HTTP basic and there are better auth mechanisms.
4. All of the above

Answer: Option 3.

Solution: HTTP basic authentication is certainly not the best way of securing a web application as there are many security issues with HTTP basic and there are better auth mechanisms. HTTP basic authentication are encoded with base64 encoding, which is not a form of encryption and can easily be reversed to get back the password.