A [3 + 2 + 3 + 2 marks]

1. Rewrite the following JavaScript code to prevent potential XSS when displaying user input.

```
document.write('<p>' + userInput
+ '</p>');
```

2. Using sound reasons, argue in favor or against the statement: Using XSS attacks, an attacker is able to wipe victim's hard disk.
3. A biometric authentication system has been configured to allow access only when user's biometric profile matches at least 99.9% with the profile in database. What challenges could the users face in such scenario?
4. How do hierarchies simplify management of role based access control.

B [2 + 3 + 2 + 3 marks]

1. Following code comes from the PHP backend of an app. Discuss what crucial step in missing?

```
$data = $_POST["comment"];
insert_in_database($data);
```

2. State with reasons whether the statement is correct: CSRF attacks can only be launched via POST requests.
3. In a database of user accounts, following row exists: (id=426, digest=ab4jp, salt=2287). A user tries to login with username 426 and password p3ach. How will the system check if user's credentials are correct.
4. Differentiate between authentication and authorization in an access control system? How frequently does each activity take place?

Group A

Q1

Use textContents safe sink

```
// First assign the <p> object to ‘element’
element.textContents = userInput
```

Q2

During XSS, attacker’s script runs within the browser, hence it is limited by what a web browser will allow. Accessing the files on hard disk is not, by default, allowed to javascript code.

Q3

Having such a high threshold means there will be very low false acceptances, but relatively higher false rejections. So genuine users will be rejected by the system whenever their biometric profile is slightly different, such as due to physical factors on body (wetness, wound, oily hands etc.).

Q4

We do not have to define all privileges for every single role. Rather, (mostly) defining privileges for leaf nodes in hierarchy tree will be sufficient. Parent roles will automatically receive all permissions that their child roles have.

Group B

Q1

Comment contents are being received from client side, hence data validation and sanitization is essential before pushing it to db. Make sure it includes no malicious scripts.

Q2

No, CSRF request can be sent via either GET or POST, whatever method server is using to receive requests from clients.

Q3

By evaluating the Boolean condition:

hash(p3ach | 2287) == ab4jp

Q4

Authentication is concerned with verification of user's credentials, while access control job is to enforce authorization rules which define what permissions a user has for each resource.

Authentication is a less frequent activity (one login per session). But access control mechanism is a continuous meditation between a user and system resources.