PHP ASSESSMENT:

The question

- Explain how you would implement user authentication using this User class.

The answer

We need to give the user access to enter the email and password, next check if the email and password are existing in database in our case, we need to check the user email and password that the user entered and compare it with the password in our database

If the user credentials (email and password) are correct we need to create a session by give it many variables, this session contain the user id, user name and give it a Boolean variable like logging to be true.

Now for the pages what need the user to be logged in we need to check if the session logged in variable is true or false

If the user logout we can just delete that session.

The question

- Write an optimized query that fetches 50 most recent records of active users and explain your indexing strategy.

The answer

First lest descript the sentence to fetch the data from database

1 – fetch 50 records means use

LIMIT 50

2 – most recent records

ORDER BY created_at DESC

3 – of the active users

WHERE status = "active"

4 – also we need to select the records that we need to fetch

SELECT id, name, email

So, the query will be like the bellow

```sql
SELECT
      id, name, email
FROM
      Users
WHERE
      Status = "active"
ORDER BY
      Created_at DESC
LIMIT
      50;
```

JAVASCRIPT ASSESSMENT:

The question

- How would you handle errors in this case? Provide examples.

The answer

- We can handle the errors depends on the response status code because its an API like 200 ok and 500 server error
  We can use the response.status to check the errors to handle them

The question

- Secure our application from SQL injection XSS and CSRF

The answer

- First secure our application from SQL injections that's by preparing the statements and never pass parameters directly to the SQL string (query)
- Second XSS protection what by sanitize the entries (inputs values) before send them to the database
- For SCRF we can set up a token (sessions or cookies) in our application for each user when interacting with the application, and use these tokens in actions and forms