Test Case 1: Successful login

* Endpoint:<https://pay2.foodics.dev/cp_internal/login>
* Request Data:

{

"email": "merchant@foodics.com",

"password": "123456",

"token": "Lyz22cfYKMetFhKQybx5HAmVimF1i0xO"

}

Expected Behavior:

* Make a POST request to the login endpoint with the provided data.
* Verify that the response contains a successful login status code (e.g., 200 OK).
* Validate the response to ensure it contains the necessary information, such as user details or an access token.

Test Case 2: Unauthorized Access to 'whoami'

* Endpoint: <https://pay2.foodics.dev/cp_internal/whoami>
* Expected Behavior:
  + Make a GET request to the 'whoami' endpoint without authenticating.
  + Verify that the response contains an unauthorized access status code (e.g., 401 Unauthorized).
  + Ensure that the response message indicates that authentication is required.

Test Case 3: Get User Details After Successful Login

* Endpoint: https://pay2.foodics.dev/cp\_internal/whoami
* Request Data:

{

"email": "merchant@foodics.com",

"password": "123456",

"token": "Lyz22cfYKMetFhKQybx5HAmVimF1i0xO"

}

Expected Behavior:

* Perform a successful login by making a POST request to the login endpoint with the provided data.
* Capture the authentication token from the login response.
* Make a GET request to the 'whoami' endpoint, providing the captured token in the request header.
* Verify that the response contains a successful status code (e.g., 200 OK).
* Validate the response to ensure it contains user details, and the user is authorized to access 'whoami'.