Project: Siemens EDA – SDET Technical Task – Task 4 - API testing
Tester: Nagy Raouf

ID	Title	Description	Steps to Reproduce	Expected Result	Actual Result	Severity
B-01	POST /api/v1/users does not return token and wrong status code	When creating a user with a valid payload, the API returns status 200 OK instead of 201 Created, and the response body does not include the expected token.	1. Send a POST request to /api/v1/users with a valid user payload. 2. Inspect the response status code and body. 3. Note the missing token and status code.	Status code should be 201 Created and response body should include a "token" property along with a success message.	Status code is 200 OK, and the response body contains the success message but does not include the "token" property.	Medium
B-02	POST /api/v1/users returns 401 instead of 400 for duplicate user registration	When trying to register a user with duplicate data, the API returns a 401 Unauthorized status instead of the expected 400 Bad Request with a duplicate user error message.	1. Send a POST request to /api/v1/users with data for a user already registered. 2. Check the response status and message.	Status code should be 400 Bad Request with a message indicating duplicate user error.	Status code is 401 Unauthorized instead of 400 Bad Request; response may or may not contain the duplicate user message.	Medium
B-03	POST /api/v1/users rejects invalid payload with name only but returns 401 Unauthorized	When registering a user with only a name (missing required fields), the API returns 401 Unauthorized instead of 400 Bad Request.	1. Send a POST request to /api/v1/users with a payload containing only the name field (missing other required fields). 2. Observe response status and body.	Status code should be 400 Bad Request, and the API should reject the request with an error.	Status code is 401 Unauthorized, indicating incorrect error handling for validation failure.	High
B-04	POST /api/v1/users rejects invalid payload with email only but returns 401 Unauthorized	When registering a user with only an email (missing other required fields), the API returns 401 Unauthorized instead of 400 Bad Request.	1. Send a POST request to /api/v1/users with a payload containing only the email field (missing other required fields). 2. Observe response status and body.	Status code should be 400 Bad Request, and the API should reject the request with an error.	Status code is 401 Unauthorized, indicating incorrect error handling for validation failure.	High
B-05	POST /api/v1/users rejects invalid payload with password only but returns 401 Unauthorized	When registering a user with only a password (missing other required fields), the API returns 401 Unauthorized instead of 400 Bad Request.	1. Send a POST request to /api/v1/users with a payload containing only the password field (missing other required fields). 2. Observe response status and body.	Status code should be 400 Bad Request, and the API should reject the request with an error.	Status code is 401 Unauthorized, indicating incorrect error handling for validation failure.	High
B-06	POST /api/v1/users accepts invalid email format and returns 200 OK	When registering a user with an invalid email format, the API incorrectly accepts the request and returns status 200 OK instead of rejecting it.	1. Send a POST request to /api/v1/users with a payload containing an invalid email format. 2. Observe the response status and body.	Status code should be 400 Bad Request, and the API should reject the request with an error about invalid email format.	Status code is 200 OK, and the request is accepted despite invalid email format.	High
B-07	POST /api/v1/users accepts empty payload and returns 200 OK	When registering a user with an empty request body, the API incorrectly accepts the request and returns status 200 OK instead of rejecting it.	1. Send a POST request to /api/v1/users with an empty request body. 2. Observe the response status and body.	Status code should be 400 Bad Request, and the API should reject the request with an error.	Status code is 200 OK, and the request is accepted despite empty payload.	High
B-08	POST /api/v1/auth returns 401 instead of 400 when password is missing	When authenticating a user without providing a password, the API returns 401 Unauthorized instead of 400 Bad Request.	1. Send a POST request to /api/v1/auth with only the email parameter and omit the password. 2. Observe the response status.	Status code should be 400 Bad Request, indicating missing required parameter.	Status code is 401 Unauthorized, indicating incorrect handling of validation failure.	Medium
B-09	GET /api/v1/users returns 403 instead of 401 when token is missing	When requesting user data without providing a token, the API returns 403 Forbidden instead of 401 Unauthorized.	1. Send a GET request to /api/v1/users without an Authorization header. 2. Observe the response status.	Status code should be 401 Unauthorized to indicate missing authentication token.	Status code is 403 Forbidden, indicating incorrect error handling for missing token.	Medium
B-10	GET /api/v1/users returns 403 instead of 401 when token is invalid	When requesting user data with an invalid token, the API returns 403 Forbidden instead of 401 Unauthorized.	1. Send a GET request to /api/v1/users with an Authorization header containing an invalid token. 2. Observe the response status.	Status code should be 401 Unauthorized to indicate invalid authentication credentials.	Status code is 403 Forbidden, indicating incorrect error handling for invalid token.	Medium
B-11	PATCH /api/v1/users returns 403 instead of 401 when token is missing	When updating user data without providing a token, the API returns 403 Forbidden instead of 401 Unauthorized.	1. Send a PATCH request to /api/v1/users without an Authorization header. 2. Observe the response status.	Status code should be 401 Unauthorized to indicate missing authentication token.	Status code is 403 Forbidden, indicating incorrect error handling for missing token.	Medium
B-12	PATCH /api/v1/users returns 403 instead of 401 when token is invalid	When updating user data with an invalid token, the API returns 403 Forbidden instead of 401 Unauthorized.	1. Send a PATCH request to /api/v1/users with an Authorization header containing an invalid token. 2. Observe the response status.	Status code should be 401 Unauthorized to indicate invalid authentication credentials.	Status code is 403 Forbidden, indicating incorrect error handling for invalid token.	Medium
B-13	PATCH /api/v1/users accepts invalid body and returns 200 OK	When updating user data with an invalid request body, the API incorrectly accepts the request and returns 200 OK instead of rejecting it.	1. Send a PATCH request to /api/v1/users with a valid Authorization token. 2. Use a request body containing invalid fields (e.g., { foobar: "invalid" }). 3. Observe the response.	Status code should be 400 Bad Request, and the API should reject the request with a validation error.	Status code is 200 OK, and the request is accepted despite invalid body fields.	High
B-14	DELETE /api/v1/users returns 403 instead of 401 when token is missing	When attempting to delete a user without providing a token, the API returns 403 Forbidden instead of 401 Unauthorized.	1. Send a DELETE request to /api/v1/users without including an Authorization header. 2. Observe the response status.	Status code should be 401 Unauthorized to indicate missing authentication token.	Status code is 403 Forbidden, indicating incorrect error handling for missing token.	Medium
B-15	DELETE /api/v1/users returns 403 instead of 401 when token is invalid	When attempting to delete a user with an invalid token, the API returns 403 Forbidden instead of 401 Unauthorized.	1. Send a DELETE request to /api/v1/users with an Authorization header containing an invalid token. 2. Observe the response status.	Status code should be 401 Unauthorized to indicate invalid authentication credentials.	Status code is 403 Forbidden, indicating incorrect error handling for invalid token.	Medium