Qubika Sports Club Management System - Defect Report

Defect Ticket ID: QBK-17529

[Security Vulnerability]: Authentication Token is exposed in Login Response

Reporter: Joshua Acciarri
Date: 30/07/2025
Environment: QA Env (URL: https://club-administration.qa.qubika.com/#/auth/login)
Found on: Firefox 140.0 (Windows 11)
Credentials: Email: *test.qubika@qubika.com* | Password: *12345678*

Description:

After successfully logging in, the API response directly exposes the **J**WT **access token in plaintext** within the browser's developer tools (Network tab). This means that anyone who gains access to this response **could steal the token** and use it to log in as an admin or impersonate the user. This presents a critical security risk, especially if the token has extended validity and no IP binding.

Severity: **S1** (Critical) – Security breach risk, could lead to unauthorized account access.

Priority: P1 (High) – Must be fixed to ensure system integrity.

Expected Result:

Authentication tokens should never be directly exposed in frontend-accessible responses. They should be handled via secure HttpOnly cookies or server-managed sessions

Actual Result:

The token is visible in the response payload, making it vulnerable to theft and misuse.

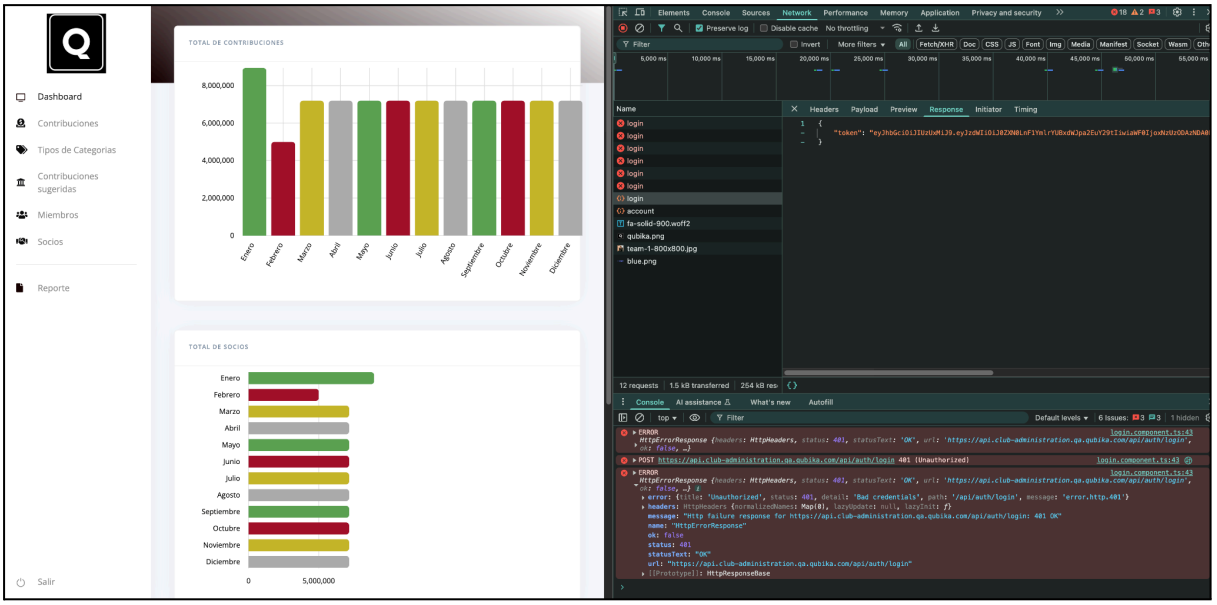
Steps to Reproduce:

1. Navigate to https://club-administration.qa.qubika.com

2. Login with valid credentials e.g. Email: test.qubika@qubika.com , Password: 12345678.
3. Open Developer Tools > Network tab.
4. Observe the POST request to /auth/login.
5. Review the JSON response containing the access token

Attachments:

Application after logging in with valid credentials, Network tab on Dev tools opened.



Response on Swagger with same payload