Sample Report:

Introduction:

This report outlines the results of the QA testing performed on the Manual Testing,Performance Testing (Using Jmeter),Automation,Authentication & Security modules of the application. The aim of this testing was to ensure that the application is secure and user-friendly, and that it meets the expected standards for Authentication & Security.

Test Environment:

Operating System: Windows 10

Browser: Chrome Version 95.0.4638.54

JMeter version: 5.4.1

Test Server Configuration: Windows Server 2019, 4 CPU Cores, 16GB RAM, 500GB HDD

Application Server Configuration: Linux, 4 CPU Cores, 8GB RAM, 256GB SSD

Test Tool: Selenium WebDriver,Performance Testing (Using Jmeter)

Test Scenarios:

Manual Testing(test case report):

I’ve completed wrote Signup,LoginLogout,Forgot Password,Reset Password,2FA Security Method Unavailable,Security Settings modules test cases.I wrote 101 test cae and found a bug which I report my manual testing sheet.and all expected results were met

Performance Testing:

I’ve completed performance test on frequently used https://exchange-tradex.nftarttoken.xyz/.  
Test executed for the below mentioned scenario in server 172.67.133.117

100 concurrent requests with 0 loop count; AVG TPS for total sample is ~ 0 And total concurrent API requested: 100.

200 concurrent requests with 0 loop count; AVG TPS for total sample is ~ 0 And total concurrent API requested: 200.

While executing 300 concurrent requests, most of the requests ‘failed to respond’ and error rate is almost 99.0%

Summary: Server can not handle at least concurrent 200 API calls with most of the error rate at 99%.

Signup:

I verify that a new user can successfully create an account with valid credentials.

I verify that an error message is displayed when the user attempts to sign up with invalid credentials.

I verify that the user is redirected to the login page after successful signup.

Login:

I verify that a registered user can successfully login with valid credentials.

I verify that an error message is displayed when the user attempts to login with invalid credentials.

I verify that the user is redirected to the dashboard after successful login.

Logout:

I verify that the user can successfully logout from the application.

I verify that the user is redirected to the login page after successful logout.

Forgot Password:

I verify that the user can successfully reset their password through the "Forgot Password" functionality.

I verify that an error message is displayed when the user enters an incorrect email address for password reset.

I verify that the user receives a password reset email with the correct instructions.

Reset Password:

I verify that the user can successfully reset their password with the correct verification code.

I verify that an error message is displayed when the user enters an incorrect verification code.

I verify that the user is redirected to the login page after successful password reset.

2FA Security Method Unavailable?

I verify that the user is informed when 2FA security method is available and the appropriate working.

Security Settings:

I verify that the user can access their security settings page.

I verify that the user can update their security settings, including enabling or disabling 2FA security method.

I verify that the updated security settings are saved and reflected on the security settings page.

Summary:

Overall, the QA testing of the Authentication & Security modules was successful, and all expected results were met. The application is secure and user-friendly, and meets the expected standards for Authentication & Security. However, we recommend that the development team should continuously monitor and test the application to ensure that it remains secure and error-free.