MASTER TEST PLAN

1. TEST PLAN IDENTIFIER ET-STP01.0
2. REFERENCES

None Identified.

1. INTRODUCTION

This is the Test Plan for user log in page at exness.com project. This plan will address only those items and elements that are related to the authentication procedure.

The primary focus of this plan is to ensure that the login page provides the process of determining whether someone or something is who or what it declares itself to be. Authentication technology via login page provides access control for the site by checking to see if a user's credentials match the credentials in a database of authorized users or in a data authentication server.

The project will have functional test cases and non-functional security test cases. The details for each types are addressed in the approach section.

1. TEST ITEMS

The following is a list, by version and release, of the items to be tested:

1. User login page at <https://www.exness.com/>, Version 5.4
2. SOFTWARE RISK ISSUES

There are several parts of the project that are not within the control of the login page but have direct impacts on the process and must be checked as well.

1. The ability to close or restart the browser (or main page of site) in the middle of the process is a critical factor to application reliability
2. FEATURES TO BE TESTED
3. New user registration process
4. Sing in a user after registration process
5. FEATURES NOT TO BE TESTED

A. Tools & Services function

1. Help Center function
2. Search function
3. APPROACH
   1. Testing types

Functional Test Cases:

|  |  |  |
| --- | --- | --- |
| Sr. No. | Functional Test Cases | Type- Negative/ Positive Test Case |
| 1 | Verify if a user will be able to login with a valid email and valid password. | Positive |
| 2 | Verify if a user cannot login with a valid email and an invalid password. | Negative |
| 3 | Verify if a user cannot login with an invalid email and a valid password. | Negative |
| 4 | Verify if a user cannot login with an invalid email and an invalid password. | Negative |
| 5 | Verify the ‘Forgot Password’ functionality. | Positive |
| 6 | Verify the messages for invalid login. | Positive |
| 7 | Verify if the data in password field is either visible as bullet signs. | Positive |
| 8 | Verify if a user is able to login with a new password after he/she has changed the password. | Positive |
| 9 | Verify if the login page allows to log in simultaneously with different credentials in a different browser. | Positive |
| 10 | Verify if the ‘Enter’ key of the keyboard is working correctly on the login page. | Positive |
|  |  |  |

Non-functional Security Test Cases:

|  |  |  |
| --- | --- | --- |
|  | Verify the time taken to log in with a valid email and password. | Performance & Positive Testing |
|  | Verify if the font, text color, and color coding of the Login page is as per the standard. | UI Testing & Positive Testing |
|  | Verify the login page and all its controls in different browsers | Browser Compatibility & Positive Testing. |
|  | Verify if a user cannot enter the characters more than the specified range in each field (email and Password). | Negative |
|  | Verify the timeout functionality of the login session. | Positive |
|  | Verify if a user should not be allowed to log in with different credentials from the same browser at the same time. | Negative |
|  | Verify the Login page against SQL injection attack. | Negative |
|  |  |  |

* 1. Test Tools

1. Python based automation tests
2. Google chrome web browser
3. Mozilla Firefox web browser
   1. Meetings

The test team will meet once every two weeks to evaluate progress to date and to identify error trends and problems as early as possible. The test team leader will meet with development and the project manager once every two weeks as well. These two meetings will be scheduled on different weeks. Additional meetings can be called as required for emergency situations.

* 1. Measures and Metrics

The following information will be collected by the test team during all testing phases. This information will be provided on a biweekly basis to the test manager and to the project team.

1. Defects by module and severity.

2. Defect Origin (Requirement, Design, Code)

3. Time spent on defect investigation by defect, for Critical & Major only. All Minor defects can be totaled together.

4. A Number of times a program submitted to the test team as ready for the test.

5. Defects located at higher levels that should have been caught at lower levels of testing.

1. ITEM PASS/FAIL CRITERIA

The test process will be completed when all tests from the approach section are finished as expected.

1. SUSPENSION CRITERIA AND RESUMPTION REQUIREMENTS
2. Log in page at exness.com project is not available

The testing process will be delayed until at least in one web browser the login page is available and elements are visible.

1. TEST DELIVERABLES

Acceptance test plan

Screen prototypes

Defect/Incident reports and summaries

Test logs and turnover reports

1. TAFFING AND TRAINING NEEDS

It is preferred that there will be at least one (1) full-time tester assigned to the project for the acceptance testing phases of the project.

Tester(s) will not need to be trained.

1. RESPONSIBILITIES

|  |  |  |  |
| --- | --- | --- | --- |
|  | PM | Dev Team | Test Team |
| Acceptance test Documentation & Execution | X |  | X |
| System Design Reviews | X | X | X |
| Detail Design Reviews | X | X | X |
| Test procedures and rules | X | X | X |
| Screen & Report prototype reviews |  | X | X |
| Change Control and regression testing |  | X | X |
|  |  |  |  |

1. PLANNING RISKS AND CONTINGENCIES
2. Limited QA staff

The Test team currently has two positions unfilled. As a result of this staff shortage there may be delays in getting staff to review appropriate

documents and to participate in the Acceptance test process.

1. APPROVALS

|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |