Test Plan Report

**Team**

* Dima Sabina Andreea
* Gramadă Florin Alexandru
* Magadan Alexandru
* Panaintescu Florentina
* Prodan Petru

This test plan defines the overall testing approach to verify the functionality, performance, usability, and security of the Trendyol application. ,,Trendyol**"** application is a leading e-commerce platform that allows users to explore, purchase, and manage a wide range of products, including fashion, electronics, and household items.

The primary goal is to identify and eliminate defects , ensuring that the platform operates efficiently across various devices and environments. Through a structured testing process, we aim to enhance the application’s reliability and user satisfaction while maintaining business requirements and industry standards.

**Objectives**

* Verify that all features of the Trendyol application function as intended
* Validate the performance and scalability of the application under various load conditions.
* Confirm the security of user data and transactions.
* Identify and report any defects or issues for resolution.

**Test Approach**

* *Manual Testing :* for exploratory testing and ad-hoc scenarios.
* ​*Automated Testing :*for regression testing, performance testing and repetitive test cases.
* *Tools :*Selenium, Postman etc.

**Test Deliverables**

* Test cases and test scripts.
* Test summary report with metrics and recommendations.

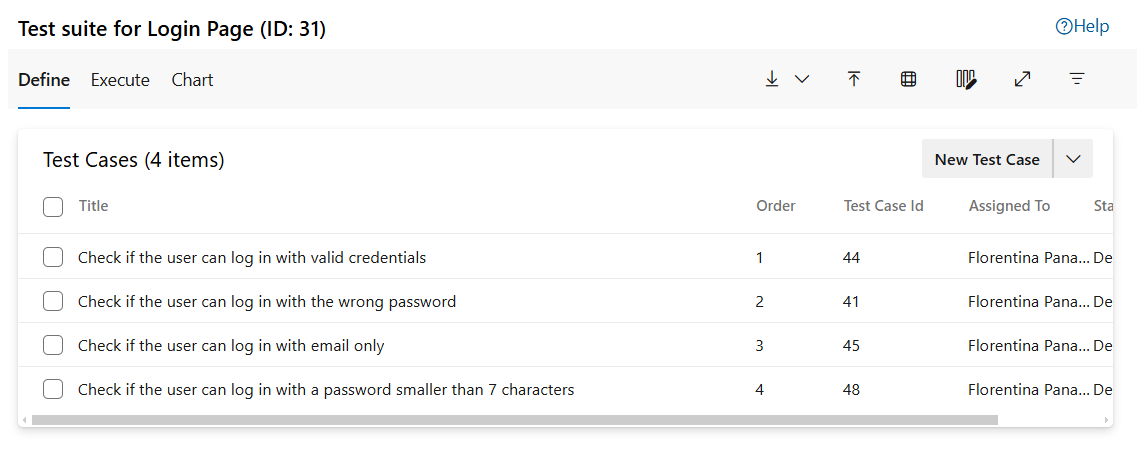
This test plan ensures that the Trendyol application is robust, user-friendly, and meets functional and non-functional requirements. Regular testing cycles and issue tracking will enhance the app’s reliability.

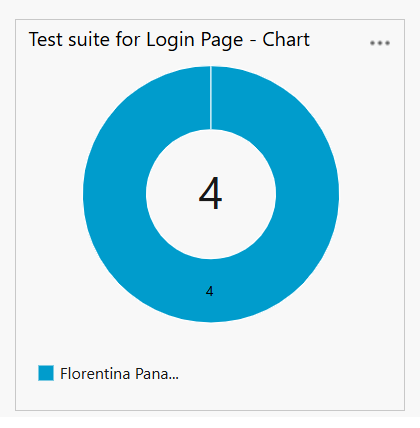
**Test Account**

user: acc.tst010101@gmail.com  
pass: testtest1

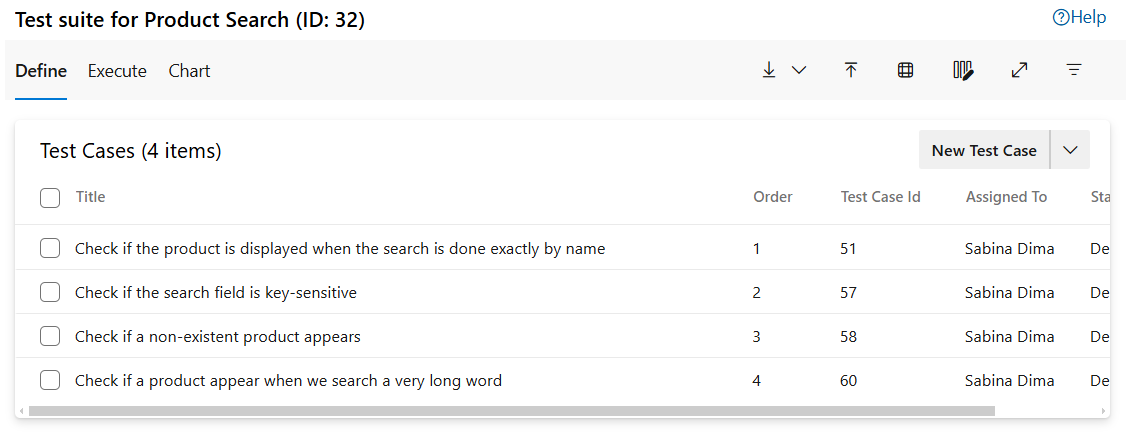
**Test Cases –** Manual Testing

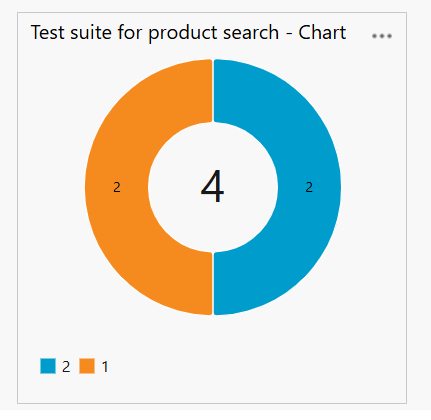
* **Panaintescu Florentina**



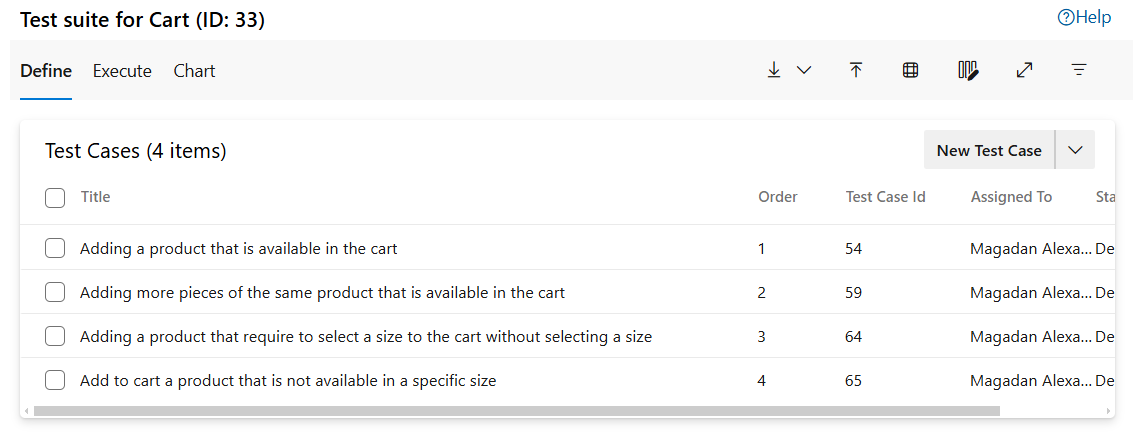


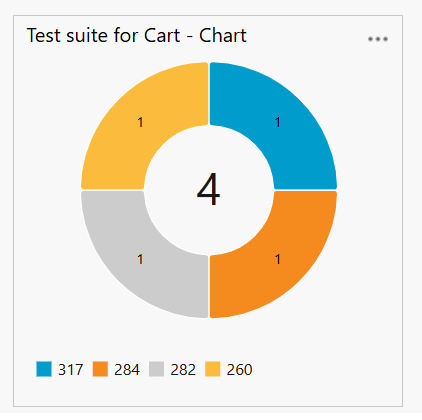
* **Dima Sabina Andreea**



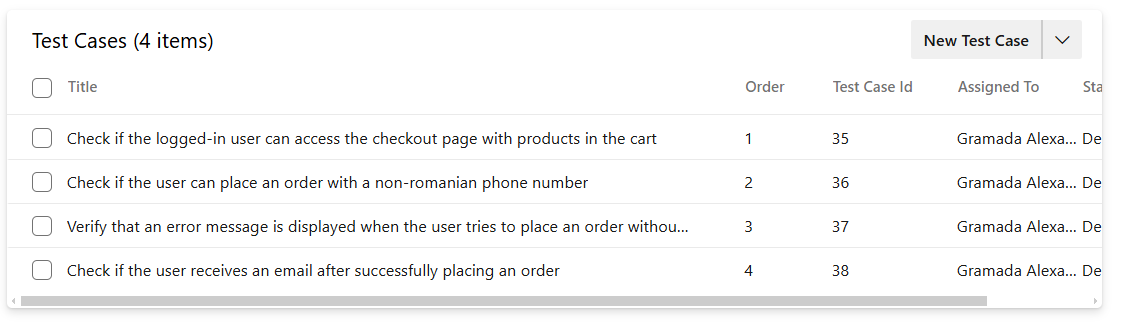


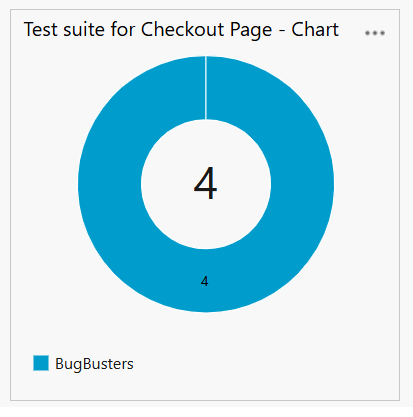
* **Magadan Alexandru**



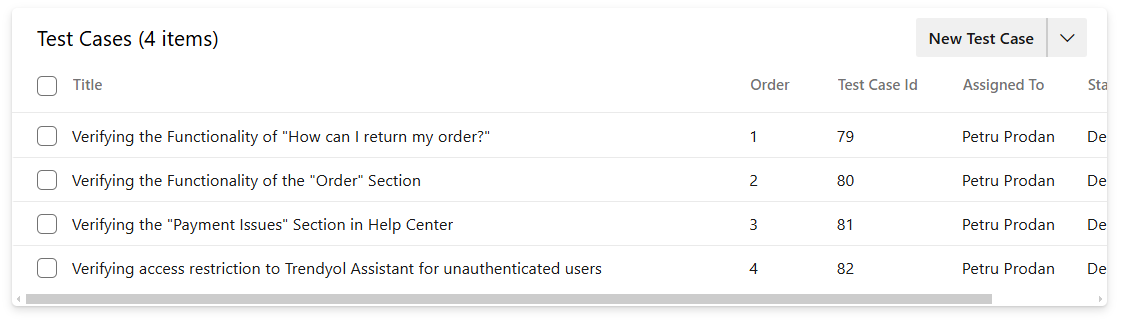


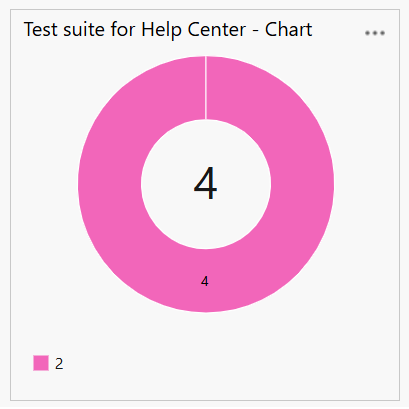
* **Gramadă Florin Alexandru**





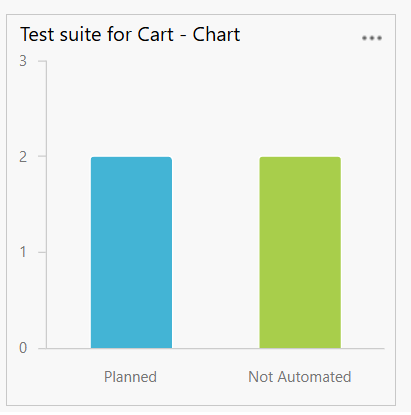
* **Prodan Petru**



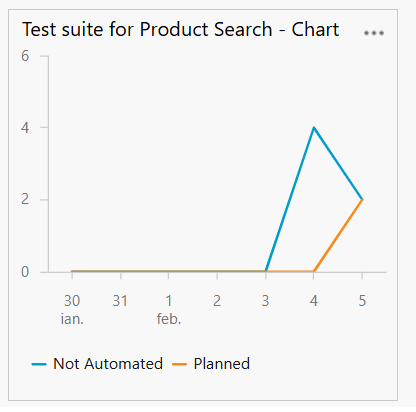


**Test Cases –** Automated Testing

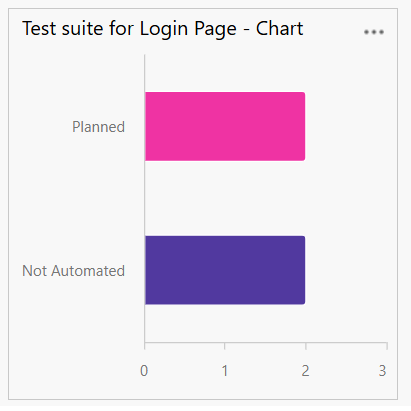
* **Magadan Alexandru**



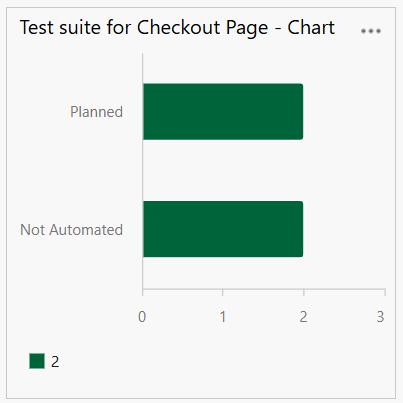
* **Dima Sabina Andreea**



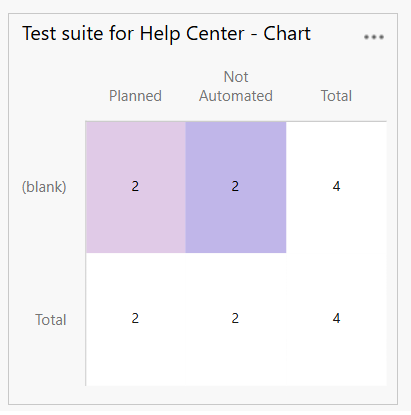
* **Panaintescu Florentina**



* **Gramadă Florin Alexandru**



* **Prodan Petru**



**Security of the application**

Some of the vulnerabilities from OWASP Top 10 for the application Trendyol could be:

1. Broken Access Control

If users can access other accounts' information by modifying a URL or using insecure requests.

If administrators do not have clear restrictions on actions that regular users can perform.

2. Cryptographic Failures

If sensitive data, such as credit card information, passwords, or user addresses, is not properly encrypted.

If Trendyol allows data transmission without HTTPS or stores passwords without hashing and salting.

3. Vulnerable and Outdated Components

If the site uses outdated plugins, frameworks, or libraries with known vulnerabilities.

Dependency on third-party software (e.g., payment gateways) that may have security breaches.

4. Identification and Authentication Failures

If Trendyol allows weak passwords or does not implement two-factor authentication (2FA) for seller/admin accounts.

If an attacker can brute-force passwords due to the absence of rate-limiting mechanisms.

5. Software and Data Integrity Failures

If website updates are automated and not verified before deployment.

If the product delivery system and financial transactions are vulnerable to manipulation.

6. Security Logging and Monitoring Failures

If Trendyol does not detect unauthorized access attempts or suspicious activity in real time.

If attacks on the system go unnoticed for long periods.

7. Server-Side Request Forgery (SSRF)

If an attacker can force the server to access internal resources or make unauthorized requests to internal APIs.