“Майже В МММ”

Marie Maimeskul
Michael Kobelev
Vadym Kochmar
Maryna Tiutiun

System testing

Terms of reference

Nover25, 2019

API testing

Testing API endpoints

1. **api/startSession:**

Passed:	**false**
Problems found:	Return data doesn't match TOR API (fixed - M. Kobelev)

2. **api/login:**

Passed:	**false**
Problems found:	Missing session tokens (fixed - V. Kochmar) Tokens generation used incorrect logic - generated similar tokens (fixed - M. Kobelev)

3. **api/balance:**

Passed:	**true**
Problems found:	None

4. **api/changePin:**

Passed:	**false**
Problems found:	Available only for CreditCard (fixed - M. Kobelev) Accept data doesn't match TOR API (fixed - M. Kobelev) Return data doesn't match TOR API (fixed - M. Kobelev)

5. **api/withdraw:**

Passed:	**false**
Problems found:	Endpoint split into different endpoints for different types of Card

6. **api/confirmWithdraw:**

Passed:	**false**
Problems found:	Missing Transaction model (fixed - M. Tiutiun) Didn't withdraw money from account (fixed - M. Kobelev)

7. **api/cardExists:**

Passed:	**true**
Problems found:	None

8. **api/transfer:**

Passed:	**true**
Problems found:	None

Edgecase analysis

1. **Section 1. Authorization, authentication.**

Use case	Passed	Notes
Try empty pin	**false**	Assignees: M. Kobelev, M. Tiutiun
Try incorrect pin	**true**	
Try empty card number	**true**	
Try to work with ATM, when server is shut down	**true**	

2. **Section 2. Interface**

Use case	Passed	Notes
Try waiting for 30 secs	true	
Clicking on screen	true	
Clicking other (not supposed to be clicked) buttons	true	

3. **Section 3.1 Views. Change pin**

Use case	Passed	Notes
Entering different PINs	true	
Leaving fields for PINs empty	false	Assignees: M. Kobelev, M. Tiutiun
Cancelling, when entered PINs	true	

4. **Section 3.2 Views. Withdraw cash**

Use case	Passed	Notes
Entering invalid sum	true	
Clicking other buttons	true	
Withdrawing exactly the sum on account	true	

5. **Section 3.3 Views. Balance**

Use case	Passed	Notes
Clicking other buttons	true	
Balance for credit card	true	

6. **Section 3.4 Views. Transfer**

Use case	Passed	Notes
Try to transfer to not existing account	true	
Try to transfer from credit card, when no money left.	true	
Try to transfer more that there's on account	true	

Security testing

Using OWASP checklist:

https://www.owasp.org/index.php/OWASP_Secure_Coding_Practices_Checklist

Section	Passed	Not passed	Critical issues
Input validation	10	6	
Output encoding	1	5	
Authentication and Password Management	27	7	1) Ensure that only cryptographically strong one-way salted hashes of passwords are stored and that the table/file that stores the passwords and keys is write-able only by the application. 2) Use only HTTP POST requests to transmit authentication credentials 3) Enforce password complexity requirements established by policy or regulation 4) Enforce account disabling after an established number of invalid login attempts
Session Management	5	18	
Database Security	7	5	1) Close the connection as soon as possible 2) The application should connect to the database with different credentials for every trust distinction (e.g., user, read-only user, guest, administrators)