Integration, test and validation processes in the Privacy Flag context

Infocom World 2017, Athens

Prof. Yannis Stamatiou
CTI / University of Patras – Business Administration Dept.

PRIVACY FLAG

Co-funded by the European Union

Co-funded by the Swiss Confederation

Privacy Flag Project Enabling Crowd-sourcing based privacy protection for smartphone applications, websites and Internet of Things deployments

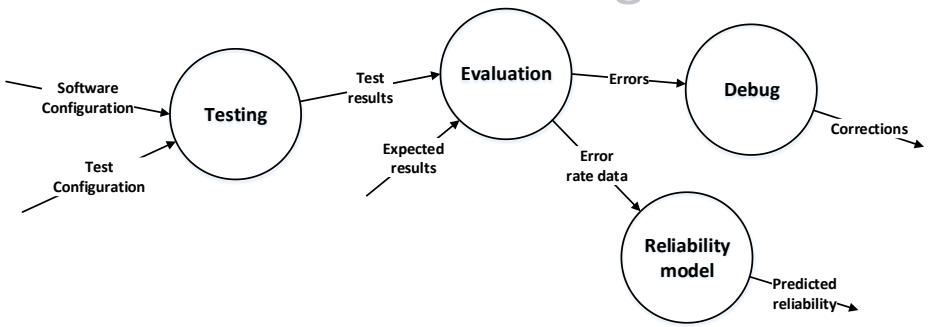
Modules that are currently integrated, fine-tuned, and running

- Security and privacy enablers
- Crowd sourcing monitoring of privacy risks with distributed agents
- Browser add-ons
- Smartphone application
- Observatory, Early Warning System, and Database Server
- Website and backend management platform

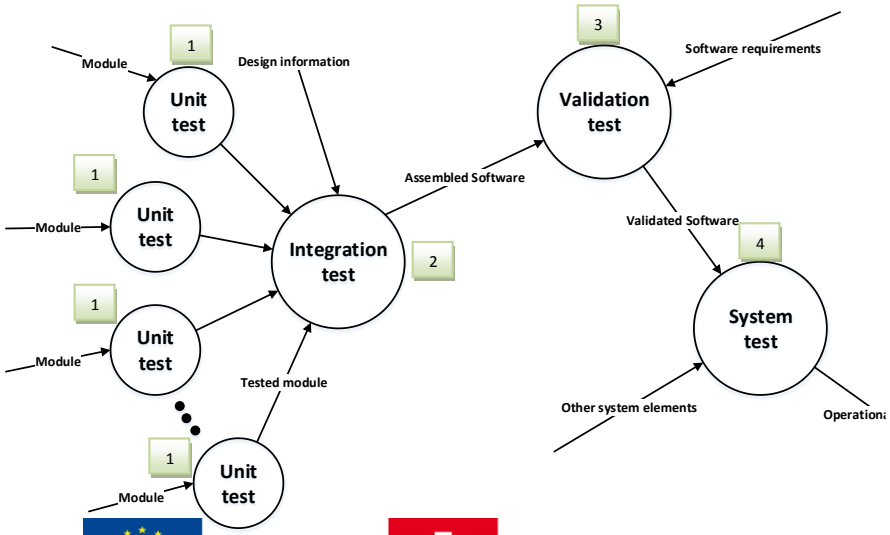
Co-funded by the European Union
Co-funded by the Swiss Confederation

The integration and testing methodology

Module level testing



System level testing/integration



1. Individual unit testing.
2. Integration of individual units to implement the Privacy Flag platform.
3. Validation test of the integrated platform against the requirements.
4. First round of integrated platform testing.
5. Feedback to developers and implementation of corrective measures – quick individual unit testing against reported problems.
6. Integration of new individual unit modules.
7. Second round of final platform testing.
8. Pilot operation and testing with a group of real users.

Co-funded by the European Union
Co-funded by the Swiss Confederation

The use case testing template

Part A: ***Use case identification***

Use Case ID:			
Use Case Name:			
Created By:		Last Updated By:	
Date Created:		Date Last Updated:	

Part B: ***Use case definition***

Actors:	
Description:	
Trigger:	
Preconditions:	
Postconditions:	
Normal Flow:	
Alternative Flows:	
Exceptions:	
Includes:	
Special Requirements:	
Legal Considerations:	
Assumptions:	
Notes and Issues:	

Co-funded by the European Union

Co-funded by the Swiss Confederation

What was expected from partners

Example use case: Website and backend management platform

PRIVACY FLAG

Use Case ID:	DNET_05		
Use Case Name:	**Privacy Flag backend users authorization**		
Created By:	Nenad Gligoric	Last Updated By:	Nenad Gligoric
Date Created:	2/05/2016	Date Last Updated:	2/05/2016

Actors:	Registered user
Description:	A user should be able to access only resources which he is authorized to access after starting the sessions.
Trigger:	The user opens backend of the website.
Preconditions:	The user is registered into the platform.
Postconditions:	
Normal Flow:	The number of concurrent users starts a session and system responds as expected and allows access only to authorized resources.
Alternative Flows:	
Exceptions:	
Includes:	
Special Requirements:	
Legal Considerations:	
Assumptions:	
Notes and Issues:	

1) **Identify** your tests in D5.1 (partner acronym – test number, e.g. DNET – 05).

2) **Set up** test case according to specs, i.e. simulate the Actor(s), the Trigger, and Preconditions according to Description.

3) **Run** the test and compare run flow and results against the Normal (expected) flow.

4) If applicable and necessary, please **take into account** (and fill in) the rest of the fields.

5) **Provide** a written report (for all assigned tests) to CTI on the execution of the test case, findings, results, and corrective actions (if necessary).

Co-funded by the European Union

Co-funded by the Swiss Confederation

What was expected from partners

Example use case: Database (Case 1)

Use Case ID:	CTI_DB_1		
Use Case Name:	Execution of sample queries		
Created By:	Yannis Stamatiou	Last Updated By:	Yannis Stamatiou
Date Created:	7/3/2016	Date Last Updated:	7/3/2016
Actors:	Distributed agents and users (through questionnaires).		
Description:	This test will evaluate the ability of the database to correctly execute sample queries on sample data.		
Trigger:	A connection from an agent or users.		
Preconditions:	The query arrives, intact, to the database		
Postconditions:	The results of the query match the expected results, as reflected by the database scheme and sample contents.		
Normal Flow:	The results are promptly returned and are as expected based on the stored values.		
Alternative Flows:			
Exceptions:	Query results are faulty or query results are not returned at all.		
Includes:			
Special Requirements:	The database is up and running.		
Legal Considerations:			
Assumptions:	The database server is correctly set-up and configured while the database contents are correct.		
Notes and Issues:			

Co-funded by the European Union

Co-funded by the Swiss Confederation

What was expected from partners

Example use case: Database (Case 2)

Use Case ID:	CTI_DB_2		
Use Case Name:	Data confidentiality		
Created By:	Yannis Stamatiou	Last Updated By:	Yannis Stamatiou
Date Created:	7/3/2016	Date Last Updated:	7/3/2016
Actors:	Data exchanged with other platform modules.		
Description:	Test whether the connection with the DB is secure, i.e. data encryption and authentication mechanisms are implemented and enabled.		
Trigger:	Initiation of communication between the DB and another module (e.g. Distributed Agents).		
Preconditions:	The database and platform modules are correctly configured for communication.		
Postconditions:	Data is exchanged between the database and any connecting module in encrypted format.		
Normal Flow:	Data is properly encrypted.		
Alternative Flows:			
Exceptions:	Data is not in encrypted format.		
Includes:			
Special Requirements:	The involved modules and the database are correctly set-up and configured.		
Legal Considerations:			
Assumptions:	All modules are in an appropriate operating condition.		
Notes and Issues:			

Co-funded by the European Union

Co-funded by the Swiss Confederation

Observatory, Database, and Server

Use case 4	Result	Test description
Verification Check: This is a stress test for the server according to which the testing team will find the threshold point at which the response time of the server drops significantly. This will test only the ability of the server to sustain an acceptable connection rate without taking into account the database response times (this will be a separate test for the database module).	Succeeded	The “paessler” tool (https://www.paessler.com/tools/webstress) was used to perform a stress test on the server that hosts the databases for the smartphone application and the browser add-on, as well as the whole backend system in order to provide Quality of Service (QoS) to PF services.

Co-funded by the European Union
Co-funded by the Swiss Confederation

Observatory, Database, and Server

Use case 5	Result	Test description
Verification Check: This will test whether all data connections between the actors and the database are suitably encrypted, i.e. whether the SSL protocol is activated with the correct connection parameters (e.g. encryption algorithm used and key sizes).	On-going	This test checks whether the server opens, correctly an SSL/TLS connection when service requests are accepted.

Use case 6	Result	Test description
Verification Check: This test will evaluate the ability of the database to correctly execute sample queries on sample data.	Succeeded	The mysqlslap tool was used for stress-testing the database for the correct and fast execution of thousands of connection requests. This tool emulates a variable client workload on a MySQL server and reports the timing of each stage. It works as if multiple clients were accessing the server.

Co-funded by the European Union
Co-funded by the Swiss Confederation

Observatory, Database, and Server

Use case 7	Result	Test description
Verification Check: Test whether the connection with the DB is secure, i.e. data encryption and authentication mechanisms are implemented and enabled.	On-going	This test checks whether the data are correctly encrypted upon their transmission to and from the database.

Co-funded by the European Union
Co-funded by the Swiss Confederation

Testing configuration

With respect to the configuration on which the rest of the tests are implemented, the server on which the database resides has the following characteristics:

- *Memory: 4GB*
- *Processors: (1 processor with 4 cores)*
- *Hard disk: 200GB*

We see that the current configuration is limited. However, the results of the database (DB_1) and server workload (SE_1) tests were satisfactory and demonstrate that the database and the server can sustain heavy workloads which amount to 5000, approximately, connection requests per second which is far beyond the expected workload for the PF platform.

Co-funded by the European Union
Co-funded by the Swiss Confederation

Simulations

PRIVACY FLAG

We simulated the simultaneous use of the server in the following scenarios:

1. Privacy Flag Observatory, i.e. each user should visit the website http://150.140.193.133:2080/privacy/addon/new_metrics.php which includes the PF Threat Observatory.

2. Use of PF add-on, i.e., each user runs the GET call http://150.140.193.133:3000/addon/questionnaire_eng since, whenever the add-on is loaded, this GET call is used in order to display the UPRAAM questionnaire to them. After that, other GET and POST calls are used as well but we simply test how many users may use simultaneously the add-on without any error.

3. Use of PF smartphone application, i.e., each user runs the GET call http://150.140.193.133:3000/smartphone/questionnaire since, whenever the app is loaded, this GET call is used in order to display the UPRAAM questionnaire to them. After that, other GET and POST calls are used as well but we simply test how many users may open simultaneously the smartphone app without any error.

Co-funded by the European Union
Co-funded by the Swiss Confederation

Results

PRIVACY FLAG

The results were the following:

PF Observatory

- *Average Click Time 3.319 ms, 32.795 Clicks, 711 Errors*
- *Total Number of Clicks: 32.795 (711 Errors)*
- *Average Click Time of all URLs: 3.247 ms*

PF Add-on

- *Average Click Time 85 ms, 38.724 Clicks, 5 Errors*
- *Total Number of Clicks: 38.724 (5 Errors)*
- *Average Click Time of all URLs: 85 ms*

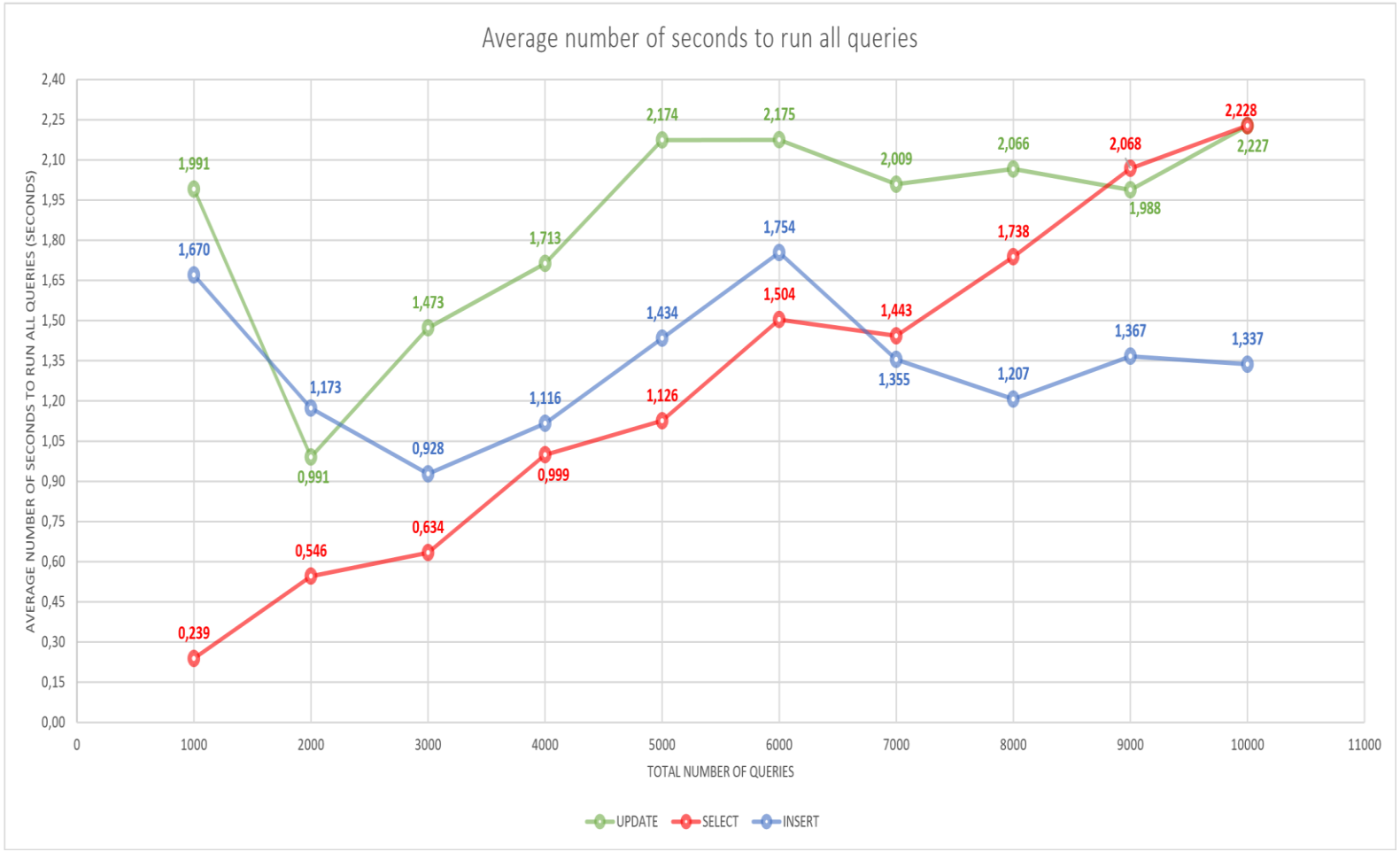
PF Smartphone Application

- *Average Click Time 57 ms, 47.047 Clicks, 0 Errors*
- *Total Number of Clicks: 47.047 (0 Errors)*
- *Average Click Time of all URLs: 57 ms*

Co-funded by the European Union
Co-funded by the Swiss Confederation

PRIVACY FLAG

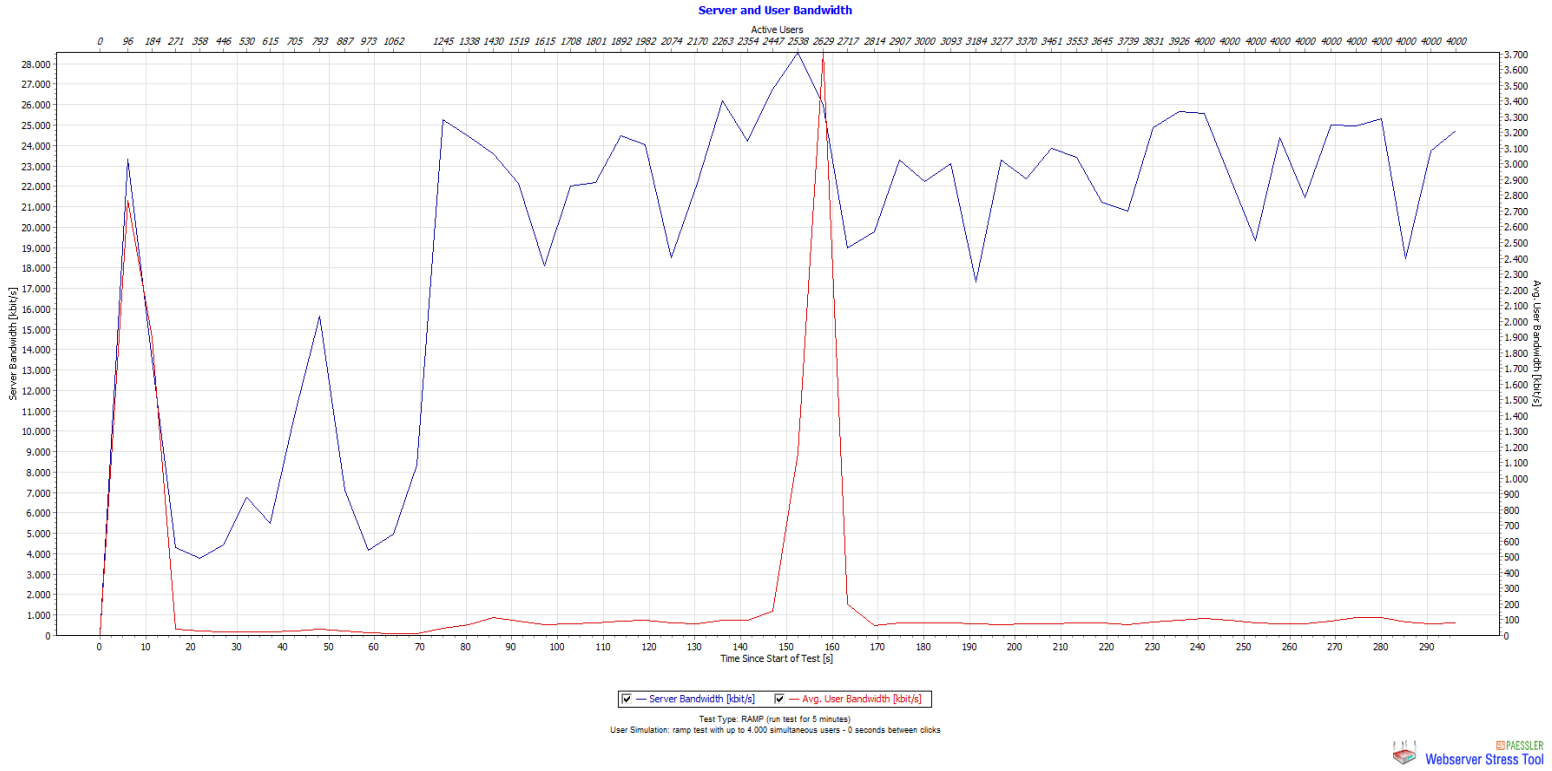
Some indicative test results for the Database and Server



Co-funded by the European Union

Co-funded by the Swiss Confederation

Some indicative test results for the Observatory



Co-funded by the European Union

Co-funded by the Swiss Confederation

Smartphone application

Use Case: SA_01 – App version 2		
Test description	Test Result	Action
Difference in API when posting package name	Failed	Fixed
UPRAAM questions not loaded correctly	Failed	Fixed
Server error	Failed	Fixed
Error when posting using username instead of user_name	Failed	Fixed
Final test	Success	

Use Case: SA_02 – App version 2		
Test description	Test Result	Action
Difference in API when posting package name	Failed	Fixed
UPRAAM questions not loaded correctly	Failed	Fixed
Server error	Failed	Fixed
Error when posting using username instead of user_name	Failed	Fixed
Server is down due to error messages	Failed	Fixed
Server is up and down due to wrong script update	Failed	Fixed
JSON body not created correctly, specs and implementation not the same, all fields updated to be in alphanumeric order	Failed	Fixed
Server is down	Failed	Fixed
Final test	Success	

Co-funded by the European Union

Co-funded by the Swiss Confederation

Smartphone application

Use Case: SA_01 – App version 3		
Test description	Test Result	Action
Final test	Success	

Use Case: SA_02 – App version 3		
Test description	Test Result	Action
When used in Android version lower than 6, user is able to send his own evaluation for an app but not the permissions (as only exist in version 6 and above). **JSON body was not created correctly and in app permissions fields none value was sent**	Failed	Fixed
Server is down	Failed	Fixed
Final test	Success	

Co-funded by the European Union

Co-funded by the Swiss Confederation

Browser Add-On

PRIVACY FLAG

Use Case: BA_01		
Test description	Test Result	Action
Check API status failed, server was not reachable, internet security restrictions	Failed	Fixed
Check API status failed, server was down, due to inactivity server was shutdown	Failed	Fixed
Wrong fields when posting url, not including full url address	Failed	Fixed
Wrong message when error state	Failed	Fixed
UPRAAM questions not retrieved correctly	Failed	Fixed
Final test	Success	

Use Case: BA_02		
Test description	Test Result	Action
Check API status failed, server was not reachable, internet security restrictions	Failed	Fixed
Check API status failed, server was down, due to inactivity server was shutdown	Failed	Fixed
Wrong fields when posting url, not including full url address	Failed	Fixed
Wrong message when error state	Failed	Fixed
Wrong JSON body from add-on to server	Failed	Fixed
Server down due to error calls	Failed	Fixed
Final test	Success	

Co-funded by the European Union

Co-funded by the Swiss Confederation

PRIVACY FLAG

Security and Privacy enablers

Use case #	Result	Test description
PE_02: Verify that the created system just picks relay nodes inside of an EU country	Succeeded	In a comprehensive testrun that contains of fetching 1000 websites, it was ensured that just relay nodes in EU countries were chosen.
PE_03: Verify that a usable quality of service is given	Succeeded	In a comprehensive testrun that contains of 1000 website fetching processes while measuring the fetching time, it was shown that the average loading time for more than half of the fetched websites decreased and the general standard deviation with the EU routing extension is way lower than before. See the graphs in D4.2 for more details.
PE_01: Verify that the IP changes after activating the enabler	Skipped	Since the plans changed and it was agreed that the privacy enabler will _not_ be used for the whole communication, there is no on/off switch. Additionally, the secure communication technique is not deployed in the browser add-on yet.
PE_04: Verify that there are no connection leaks	Skipped	Since the plans changed and it was agreed that the privacy enabler will _not_ be used for the whole communication, there are course leaks in the regular browsing that is not handled via our proxy.

Co-funded by the European Union
Co-funded by the Swiss Confederation

PRIVACY FLAG

Website and backend management platform

Use case #1	Result	Test description
User starts an action on the privacy flag webpage and system responds as expected. The test is executed using Google Chrome Page Load which measures loading of all pages. Measurement is done Page is loaded in less then 10s.	Succeeded	Verified that the load page was under < 5s for all pages (average 4.23s).

Use case #2	Result	Test description
The number of authenticated users is performing actions in the Privacy Flag backend and system runs without an error for the Wordpress backend.	Succeeded	Verified that the load page for the Wordpress backend was efficient for multiple logged in users
The number of authenticated users is performing actions in the Privacy Flag backend and system runs without an error for the custom coded backend.	On-going	At this moment custom backend is still not in its final phase of implementation.

Co-funded by the European Union

Co-funded by the Swiss Confederation

Website and backend management platform

Use case #3	Result	Test description
A user logs in the backend and should be able to access only resources which he is authorized to access after starting the session. This is tested by tring to opening url direclty without loging in and tring to use functionalities which only loged in user could access.	On-going	At this moment, custom backend is still not in its final phase of implementation.

Use case #4	Result	Test description
A user should be able to access the table with a ranking list of assessed websites and smartphone application. The data is pulled from the database and the table should be filled in with latest assessments.	On-going	At this moment, the table is deployed but the data in the backend are not ready to be presented to the end users.

Co-funded by the European Union
Co-funded by the Swiss Confederation


velti
DUNAV NET
Archimede Solutions SARL
University of BRISTOL
Istituto Italiano per la Privacy e la Valorizzazione dei Dati
National and Kapodistrian University of Athens
UNIVERSITÉ DU LUXEMBOURG
CTI "DIOPHANTUS" computer technology institute & press
OTE
MANDAT INTERNATIONAL
HWCommunications Cyber Security and Resilience
LULEÅ UNIVERSITY OF TECHNOLOGY
MY DATA
PRIVACY FLAG
Co-funded by the European Union
Co-funded by the Swiss Confederation