DP2 2023-2024

Testing report

Acme Software Factory

Repository: https://github.com/rafcasceb/Acme-SF-D04

Student #1:

- Castillo Cebolla, Rafael rafcasceb@alum.us.es

Other members:

- Flores de Francisco, Daniel danflode@alum.us.es
- Heras Pérez, Raúl rauherper@alum.us.es
- Mellado Díaz, Luis luimeldia@alum.us.es
- Vento Conesa, Adriana adrvencon@alum.us.es

GROUP C1.049

Version 1.1

19-05-24

Content Table

Executive summary

This report will offer a detailed analysis of the testing procedure and results, including a section about functional testing and another one for performance testing.

We will follow a precise but accessible approach aiming to promote comprehension and assure a good final product.

Revision Table

Date	Version	Description of the changes	Sprint
10/05/2024	1.0	• Executive summary • Introduction • Functional testing	4
11/05/2024	1.0	• Performance testing • Conclusion • Bibliography	4
19/05/2024	1.1	• Remade after follow up	4

Introduction

This document will provide a detailed analysis of the testing procedure and results for the following features:

- Operations by managers on Projects.
- Operations by managers on User stories.

The content of a testing report is organized into two chapters:

- Functional testing: a listing with the test cases implemented, grouped by feature. For each test case, a succinct description plus a clear indication on how effective it was at detecting bugs are provided.

- Performance testing: it provides adequate charts, a 95%-confidence interval for the wall time taken by the project to serve the requests in the functional tests and a 95%-confidence hypothesis contrast.

Contents

Functional testing

Operations by manager on Projects

Test case 1: list-mine

For this command, we just selected the button for listing all projects for ten different managers.

For hacking, we considered accessing the URL by a wrong role. Trying to access it with a good role but a wrong user doesn't make sense.

It provided a coverage of 93.1 %, covering all instructions except a default assertion, which is logical. No bugs were detected.

Test case 2: show

For this command, we selected several projects of the listing of Manager 1 to see their details. Then we tried accessing the inexistent project of identifier -1.

For hacking, we tried accessing a project of Manger 1 with a wrong role and with Manager 2.

It provided a coverage of 96.2 %, covering all instructions except a default assertion, which is logical. No bugs were detected.

Test case 3: create

For this command, we have tried to create a new project. For each attribute we have checked the system rejects all different types of invalid data. Later, for each attribute, we have checked the system accepts all different types of valid data.

For hacking, the framework through web browser only supports to test GET hacking operations.

It provided a coverage of 92.6 %, covering all instructions except a default assertion, which is logical. No bugs were detected.

Test case 4: update

For this command, we have updated the project with identifier 153. For each attribute we have checked the system rejects all different types of invalid data. Later, for each attribute, we have checked the system accepts all different types of valid data.

For hacking, the framework through web browser only supports to test GET hacking operations.

It provided a coverage of 92.7 %. It covered all instructions but some logical exceptions: default assertions, and some combinations of the assertions for wrong user and null user story since the framework from the web browser doesn't allow to. No bugs were detected.

Test case 5: delete

For this command we tried deleting the project with identifier 149, which cannot be deleted since it has child audits, child contracts, child sponsorships, child training modules. Then we tried deleting the project with identifier 150, which cannot be deleted since it is published. Lastly, we correctly deleted the project with identifier 153.

For hacking, the framework through web browser only supports to test GET hacking operations.

It provided a coverage of 91.8 %. It covered all instructions but some logical exceptions: default assertions, and some combinations of the assertions for wrong user and null user story since the framework from the web browser doesn't allow to. No bugs were detected.

Test case 6: publish

For this command, we have tried to publish three different projects. First, we have tried to update the project with identifier 153, which cannot be published since it doesn't have any user story. Then, we tried with the project with identifier 149, which cannot be published since it has unpublished user stories. And, finally, we tried with the project with identifier 151. This project was valid for publishing, however, before correctly publishing it, we followed a similar approach to the update tests, since the publishing form also sends all attributes for them to be updated. With this project we also tried publishing it with fatal errors.

For hacking, the framework through web browser only supports to test GET hacking operations.

It provided a coverage of 93.9 %. It covered all instructions but some logical exceptions: default assertions, and some combinations of the assertions for wrong user and null user story since the framework from the web browser doesn't allow to. Besides, the attribute *fataErrorsPresent* which comes from a checkbox, never comes with errors, but the check is performed for security. No bugs were detected.

Operations by manager on User stories

Test case 1: list-mine

For this command, we just selected the button for listing all user stories for ten different managers.

For hacking, we considered accessing the URL by a wrong role. Trying to access it with a good role but a wrong user doesn't make sense.

It provided a coverage of 92.6 %, covering all instructions except a default assertion, which is logical. No bugs were detected.

Test case 2: list-for-project

localhost:8082/acme-sf-d04/manager/user-story/list-for-project?projectId=151

For this command, we clicked on the button to see the user stories of three different projects: project with identifier 149, which had multiple children user stories, project with identifier 151, which had one child user story, and project with identifier 153, which had none. Then we tried accessing the inexistent project of identifier -1.

For hacking, we tried accessing the same user story listing with a wrong role and with Manager 2.

It provided a coverage of 95.5 %, covering all instructions except a default assertion, which is logical. No bugs were detected.

Test case 3: show

For this command, we selected several user stories of the listing of Manager 1 to see their details. Then we tried accessing the inexistent project of identifier -1.

For hacking, we tried accessing a user story of Manager 1 with a wrong role and with Manager 2.

It provided a coverage of 96.5 %, covering all instructions but some logical exceptions: default assertions, and some combinations of the assertions for wrong user, since the framework from the web browser doesn't allow to. No bugs were detected.

Test case 4: create

For this command, we have tried to create a new user story. For each attribute we have checked the system rejects all different types of invalid data. Later, for each attribute, we have checked the system accepts all different types of valid data.

For hacking, the framework through web browser only supports to test GET hacking operations.

It provided a coverage of 92.9 %, covering all instructions except a default assertion, which is logical. No bugs were detected.

Test case 5: update

For this command, we have updated the user story with identifier 631. For each attribute we have checked the system rejects all different types of invalid data. Later, for each attribute, we have checked the system accepts all different types of valid data.

For hacking, the framework through web browser only supports to test GET hacking operations.

It provided a coverage of 92.5 %. It covered all instructions but some logical exceptions: default assertions, and some combinations of the assertions for wrong user and null user story since the framework from the web browser doesn't allow to. No bugs were detected.

Test case 6: delete

For this command we deleted the user story with identifier 631. There is no restriction to test.

For hacking, the framework through web browser only supports to test GET hacking operations.

It provided a coverage of 88.4 %. It covered all instructions but some logical exceptions: default assertions, and some combinations of the assertions for wrong user and null user story since the framework from the web browser doesn't allow to. No bugs were detected.

Test case 7: publish

For this command, we have tried to publish the user story with identifier 631. Before correctly publishing it, we followed a similar approach to the update tests, since the publishing form also sends all attributes for them to be updated.

For hacking, the framework through web browser only supports to test GET hacking operations.

It provided a coverage of 92.6 %. It covered all instructions but some logical exceptions: default assertions, and some combinations of the assertions for wrong user, null user story or published user story (a published user story cannot access the publishing function), since the framework from the web browser doesn't allow to. No bugs were detected.

Operations on ProjectUserStory intermediate table

Test case 1: create

For this command we tried linking projects to user stories. We checked that an association to a null project was rejected, that a published user story could link projects and that a published project could not be linked any further.

For hacking, we tried accessing the linking page of a user story of Manager 1 with a wrong role and with Manager 2.

It provided a coverage of 91.9 %. It covered all instructions but some logical exceptions: default assertions, and some combinations of the assertions for wrong user, null user story, published user story, or user story and project of different manager. All of these are not checked because the framework from the web browser doesn't allow to, but are necessary to manage hacking. It must be kept in mind that we are using the frontend form generated for the create service, so not all checks could be done in the authorization. No bugs were detected.

Test case 2: delete

For this command we tried unlinking projects to user stories. We checked that unlinking a null project was rejected, that a published user story could unlink projects, that deleting a project deleted the association and that a published project could not be unlinked any further.

For hacking, we tried accessing the unlinking page of a user story of Manager 1 with a wrong role and with Manager 2.

It provided a coverage of 91.8 %. It covered all instructions but some logical exceptions: default assertions, and some combinations of the assertions for wrong user, null user story or published user story since the framework from the web browser doesn't allow to. It must be kept in mind that we are using the frontend form generated for the delete service, so not all checks could be done in the authorization. No bugs were detected.

Performance testing

Let us present an analysis of the performance data obtained from the functional testing. Firstly, we will present the performance results of the tests and later we'll simulate a hypothesis contrast.

Performance data

These tests have been recorded in a computer with the following characteristics: Intel® Core™ i7-10750H CPU @2.60 GHz and 16 GB of RAM.

After the execution of the tests, the following graph has been generated, showing the average response time for each request path.

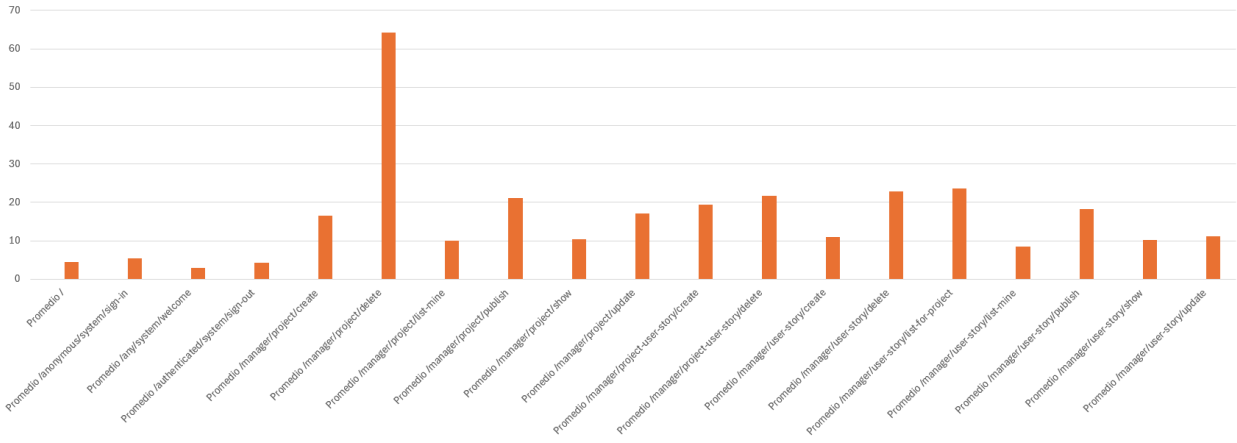

Image 1: Average response time per request path.

One feature is particularly highlighted above the others: the delete of a project. The entity Project has direct parent dependencies with five other entities: Audit, Contract, Sponsorship, TrainingModule and UserStory, which constraint its functionalities. A project cannot be deleted if it has a child of any of the first four previous entities, and in case of having a child user story, the intermediate table which links both instances should be deleted as well. Therefore, performing a delete of a project is not a simple task and must execute multiple queries and operations. Thus, it is logical that its response time is so elevated in comparison with the rest.

All the other features show a consistent and logical performance. Let us now calculate a confidence interval for the whole test suite.

Columna1	
Media	9,849108945
Error típico	0,393483132
Mediana	7,2065
Moda	7,292
Desviación estándar	11,61941765
Varianza de la muestra	135,0108665
Curtosis	52,40281144
Coeficiente de asimetría	5,477301617
Rango	164,8326
Mínimo	1,8198
Máximo	166,6524
Suma	8588,423
Cuenta	872
Nivel de confianza(95,0%)	0,772285931

	Lower limit	Upper limit
Confidence interval (ms):	9,07682301	10,6213949
Confidence interval (s):	0,00907682	0,01062139

Image 2: Data analysis summary and confidence level.

With this data analysis summary, we have computed the 95.0 % confidence interval of our data, which is, in milliseconds, [9.07682301, 10.6213949]. We can also see below the corresponding transformation to seconds.

In this project we don't have any performance requirement to which we can compare our confidence interval. However, in general terms, this could be considered an acceptable response time.

Hypothesis contrast

Since we don't have any to meet any performance requirement in this delivery, we are going to simulate a hypothesis contrast. The new data will be obtained my increasing a 10% the real testing data.

First, we generate the data analysis summary for both performance samples and compare the results.

Before				*After*		
Media	9,849108945			Media	10,83401984	
Error típico	0,393483132			Error típico	0,432831445	
Mediana	7,2065			Mediana	7,92715	
Moda	7,292			Moda	8,0212	
Desviación estándar	11,61941765			Desviación estándar	12,78135941	
Varianza de la muestra	135,0108665			Varianza de la muestra	163,3631485	
Curtosis	52,40281144			Curtosis	52,40281144	
Coeficiente de asimetría	5,477301617			Coeficiente de asimetría	5,477301617	
Rango	164,8326			Rango	181,31586	
Mínimo	1,8198			Mínimo	2,00178	
Máximo	166,6524			Máximo	183,31764	
Suma	8588,423			Suma	9447,2653	
Cuenta	872			Cuenta	872	
Nivel de confianza(95,0%)	0,772285931			Nivel de confianza(95,0%)	0,849514524	
	Lower limit	Upper limit			Lower limit	Upper limit
Confidence interval (ms):	9,076823014	10,62139488		Confidence interval (ms):	9,984505315	11,6835344
Confidence interval (s):	0,009076823	0,010621395		Confidence interval (s):	0,009984505	0,01168353

Image 3: Data analysis summary and confidence level for both samples.

The results have naturally increased, which could be considered a downgrade. However, comparing the confidence intervals intuitively is not an easy task. For this purpose, we will make use of a Z-Test. Behold its results:

Prueba z para medias de dos muestras		
	Before	*After*
Media	9,849108945	10,83401984
Varianza (conocida)	135,0108665	163,3631485
Observaciones	872	872
Diferencia hipotética de las medias	0	
z	-1,683738664	
P(Z<=z) una cola	0,046116093	
Valor crítico de z (una cola)	1,644853627	
Valor crítico de z (dos colas)	0,092232186	
Valor crítico de z (dos colas)	1,959963985	

Image 4: Z-Test results between the two performance samples.

A Z-Test is based on a value called alpha, which is computed as 1 minus the confidence level percentage. In this case, alpha will be 0.05. To understand the result of the Z-Test, we need to compare the first two-tail p value (*Valor crítico de z (dos colas)* in Spanish) to alpha. If the p value is below alpha, then we proceed to compare the averages and see if the new average has decreased.

In our case, however, the p value is 0.09223186, which is considerably higher than alpha, almost twice as much. This means that our supposed changes didn't result in any significant improvement. The sample times are different, but globally, they are considered the same.

Conclusions

This strict mechanism for formal testing has allowed us to exhaustively analyze our code in search for bugs in our code. We found two small details in an unbind method of a service which were not correctly functioning and proceeded to solve them. The final result of all tests is overwhelmingly positive, with an almost full instruction coverage (full within logic) and showing great performance results, with a great average response time.

Bibliography

Intentionally blank.