

Politechnika Białostocka Bezpieczeństwo Aplikacji Internetowych	Prowadzący: dr inż. Maciej Brzozowski
Temat: PS-2 – Implementacja prawidłowej kontroli dostępu do danych. 1. Dominik Adrian Kruk 2. Mateusz Matocha	Ocena:

1. Specyfikacja środowiska i technologii:

Język programowania: Java EE version 1.8.171

Baza danych: Oracle Database 11g Express Edition Release 11.2.0.2.0 - 64bit
Production

Technologie: Spring 4.0; Thymeleaf 3.0.9; Hibernate 5.2; HTML 5;

System Operacyjny: Windows 10 Home Edition Wersja 10.0.17134 Kompilacja 17134

Program do zarządzania bazą danych: Oracle SQL Developer Version 17.3.0.271

Środowisko programistyczne(IDE): IntelliJ IDEA 2017.3.2 (Ultimate Edition)

Build #IU-173.4127.27, built on December 25, 2017

2. Wykonanie zadań:

1) Formularz logowania:

Login form

Login

Password

Login

- 2) Formularz wyświetlający wiadomości zapisane przez użytkowników:

Witamy w serwisie

Dodaj postUstawieniaReset

nowa 1

Wystawione przez: user11

EdytujZarządzajUsuń

nowa 2

Wystawione przez: user11

EdytujZarządzajUsuń

- 3) Zaimplementuj formularz umożliwiający dodawanie wiadomości przez zalogowanych użytkowników:

Dodaj nową wiadomość

Treść wiadomości

Nowa treść wiadomości

Dodaj

- 4) Zaimplementuj formularz umożliwiający usuwanie wiadomości poprzez ich twórców:

Nowa treść wiadomości

Wystawione przez: user1

EdytujZarządzajUsuń

- 5) Zaimplementuj formularz umożliwiający nadawanie bądź odbieranie uprawnień do modyfikacji innym użytkownikom przez właściciela wiadomości:

Edytuj uprawnienia dla:

Nowa treść wiadomości

Wybierz użytkownika

user3

Dodaj uprawnienie do edycji

Wybierz użytkownika

user2

Usuń uprawnienie do edycji

- 6) Zaimplementuj formularz umożliwiający modyfikację wiadomości poprzez ich twórców bądź też użytkowników, którzy mają do tego uprawnienia:

Edytuj Wiadomość

Treść wiadomości

Nowa treść wiadomości

Edytuj

Testy wykonane w postman:

- 1) Dodanie wpisu jako niezalogowany:

Request:

POST localhost:8082/addMessage Params Send Save

Authorization Headers (1) Body Pre-request Script Tests Cookies Code

form-data x-www-form-urlencoded raw binary

	Key	Value	Description	...	Bulk Edit
<input checked="" type="checkbox"/>	text	nowy text			
	New key	Value	Description		

Response(przekierowanie na stronę logowania):

Pretty Raw Preview

Napisz

-post

Login form

Login

username

Password

password

Login

- 2) Dodanie wiadomości przez zalogowanego użytkownika:

Request:

POST http://localhost:8082/addMessage Params Send Save

Authorization Headers Body Pre-request Script Tests Cookies Code

form-data x-www-form-urlencoded raw binary

	Key	Value	Description	...	Bulk Edit
<input checked="" type="checkbox"/>	text	editing message			

Response:

editing message
Wystawione przez: user1
[Edytuj](#) [Zarządzaj](#) [Usuń](#)

3) Edycja własniej wiadomości:

Request(ID poprzednio dodanej wiadomości):

POST http://localhost:8082/edit

Authorization Headers Body Pre-request Script Tests

form-data x-www-form-urlencoded raw binary

Key	Value	Description
<input checked="" type="checkbox"/> text	editing message nowa treść	
<input checked="" type="checkbox"/> id	252	
New key	Value	Description

Response:

editing message nowa treść
Wystawione przez: user1
[Edytuj](#) [Zarządzaj](#) [Usuń](#)

4) Edycja wpisu którego użytkownik nie jest moderatorem ani właścicielem:

Request:

POST http://localhost:8082/edit

Authorization Headers Body Pre-request Script Tests

form-data x-www-form-urlencoded raw binary

Key	Value	Description
<input checked="" type="checkbox"/> text	nie moja	
<input checked="" type="checkbox"/> id	250	

Response:

Wystawione przez: user3
Fourth message text Fourth message text Fourth message text Fourth message text Fourth message text
Wystawione przez: user4
nowa 1
Wystawione przez: user11
nowa 2
Wystawione przez: user11
First message text First message text First message text First message text
Wystawione przez: user1
[Edytuj](#) [Zarządzaj](#) [Usuń](#)
Second message text Second message text Second message text Second message text Second message text
Wystawione przez: user2

5) Nadawanie uprawnień do edycji przez właściciela:

Request(dla user2):

POST localhost:8082/manage

Authorization Headers (1) Body Pre-request Script Tests

form-data x-www-form-urlencoded raw binary

Key	Value	Description
<input checked="" type="checkbox"/> newPermission	2	
<input checked="" type="checkbox"/> id	252	

Response:

Pretty Raw Preview

Napisz

-post

Witaj, *user1*

Edytuj uprawnienia dla:

editing message nowa treść

Wybierz użytkownika

user3 ▼

Dodaj uprawnienie do edycji

Wybierz użytkownika

user2 ▼

Usuń uprawnienie do edycji

6) Nadawanie uprawnień nie przez właściciela:

Request:

POST localhost:8082/manage Params Send Save

Authorization Headers (1) Body Pre-request Script Tests Cookies Code

form-data x-www-form-urlencoded raw binary

	Key	Value	Description	...	Bulk Edit
<input checked="" type="checkbox"/>	newPermission	2			
<input checked="" type="checkbox"/>	id	250			

Response(z powodu braku uprawnień do wiadomości strona nie jest wygenerowana):

Pretty Raw Preview

```
{ "timestamp": 1528585891647, "status": 404, "error": "Not Found", "exception": "pl.edu.pb.wi.bai.message.MessageManageException", "message": "No message available", "path": "/manage" }
```

7) Nadawanie uprawnień do edycji przez moderatora:

Request(z user1 próbujemy nadać uprawnienia do wiadomości 2 dla user3):

POST localhost:8082/manage Params Send Save

Authorization Headers (1) Body Pre-request Script Tests Cookies Code

form-data x-www-form-urlencoded raw binary

	Key	Value	Description	...	Bulk Edit
<input checked="" type="checkbox"/>	newPermission	3			
<input checked="" type="checkbox"/>	id	2			

Response(brak uprawnień):

```
Pretty Raw Preview

{"timestamp":1528586068475,"status":404,"error":"Not Found","exception":"pl.edu.pb.wi.bai.message.MessageManageException","message":"No message available","path":"/manage"}
```

8) Odbieranie uprawnień przez właściciela:

Request(wiadomość z pkt.5):

POST localhost:8082/delete/ Params Send Save

Authorization Headers (1) Body Pre-request Script Tests Cookies Code

form-data x-www-form-urlencoded raw binary

	Key	Value	Description	*** Bulk Edit
<input checked="" type="checkbox"/>	deletePermission	2		X
<input checked="" type="checkbox"/>	id	252		

Response(możemy nadać uprawnienia do edycji, czyli zostały usunięte):

Edytuj uprawnienia dla:

editing message nowa treść

Wybierz użytkownika

user2 ▼

Dodaj uprawnienie do edycji

9) Usuwanie uprawnień nie przez właściciela:

Request:

POST localhost:8082/delete/ Params Send Save

Authorization Headers (1) Body Pre-request Script Tests Cookies Code

form-data x-www-form-urlencoded raw binary

	Key	Value	Description	*** Bulk Edit
<input checked="" type="checkbox"/>	deletePermission	3		X
<input checked="" type="checkbox"/>	id	2		

Response(błąd-brak uprawnień):

```
Pretty Raw Preview Save Response

{"timestamp":1528586427632,"status":404,"error":"Not Found","exception":"pl.edu.pb.wi.bai.message.MessageManageException","message":"No message available","path":"/delete/"}
```

10) Usuwanie uprawnień do edycji przez moderatora:

Request(zalogowany user1 jest moderatorem wiadomości id=2):

POST localhost:8082/delete/ Params Send Save

Authorization Headers (1) Body Pre-request Script Tests Cookies Code

form-data x-www-form-urlencoded raw binary

	Key	Value	Description	*** Bulk Edit
<input checked="" type="checkbox"/>	deletePermission	3		X
<input checked="" type="checkbox"/>	id	2		

Response:

```
Pretty Raw Preview Save Response

{"timestamp":1528586427632,"status":404,"error":"Not Found","exception":"pl.edu.pb.wi.bai.message.MessageManageException","message":"No message available","path":"/delete/"}
```

11) Usuwanie wpisu, którego nie jest się właścicielem:

Request:

GET ▾	localhost:8082/delete/2	Params	Send ▾	Save ▾
-------	-------------------------	--------	--------	--------

Response:

```
{"timestamp":1528586664169,"status":404,"error":"Not Found","exception":"pl.edu.pb.wi.bai.message.MessageManageException","message":"No message available","path":"/delete/2"}
```

12) Usuwanie przez właściciela wpisu:

Request:

GET ▾	localhost:8082/delete/252	Params	Send ▾	Save ▾
-------	---------------------------	--------	--------	--------

Response(przekierowanie na stronę z wiadomościami po poprawnym usunięciu):

[Napisz](#)

[-post](#)

Witaj, *user1* [Wyloguj się](#)

Witamy w serwisie

Ostatnio zalogowano 10-06-2018 01:03

[Dodaj post](#) [Ustawienia](#) [Reset](#)

First message text First message text First message text First message text First message text First message text

Wystawione przez: user1

[Edytuj](#) [Zarządzaj](#) [Usuń](#)

Second message text Second message text Second message text Second message text Second message text Second message text

Wystawione przez: user2