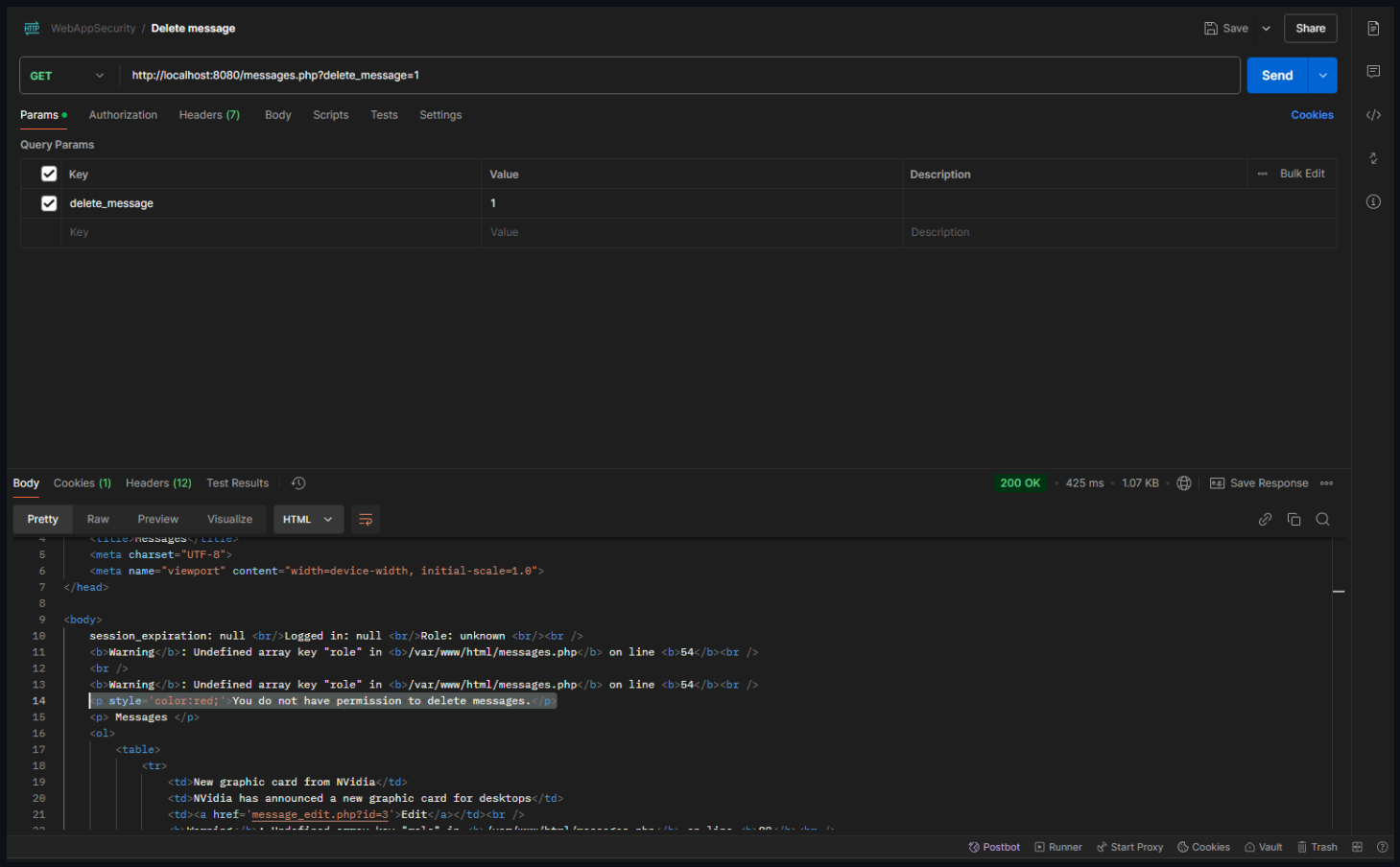
Web Applications Security

Kamil Gabrysiewicz	Index: 95400	Grupa: 2.1
Wtorek 11:45-13:15	Semestr 2	Laboratorium 6

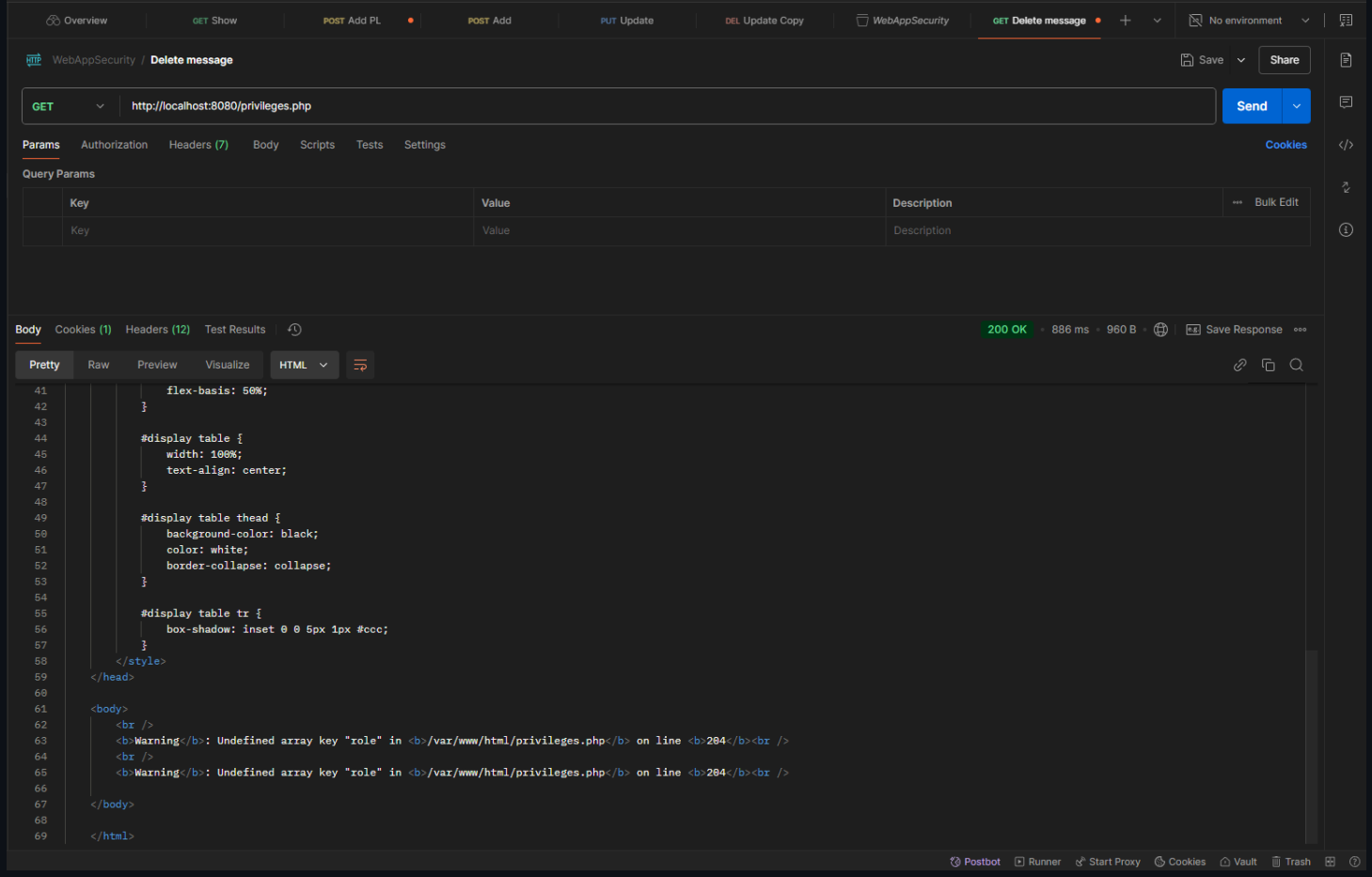
Task 6.1.

Verify whether verification of authorizations to all functions is carried out correctly. Send fabricated requests to functions without being logged in. If any irregularities are detected, improve the security measures and re-verify their correct operation. Tip. To fabricate requests, you can change the method of sending requests from forms to "get" during testing. If you don't want to do this, use a request inspection and creation program. It may be Fidler (https://www.telerik.com/fiddler).

Gladly in last laboratory I slightly overdone my app and all features of protection against fabricated request have been added. Attempt of deleteing message that doesn't belong to us will lead to message of "You do not have permission to delete message".



Attempt of accessing the view that isnt made for unprivileged, unlogged user will wont work and view won't be even rendered for attacker.



Task 6.2.

Implement the ability to view and edit your own messages in the application. Add a "my messages" page. Use the existing function to edit messages. Only modify the access control code there. Users with appropriate permissions and the message creator are to be authorized to edit messages.

Logging is a user "test" with role user"

Main page

Register new user

login
email
password
repeat password
Create account

Log in

login test
password test
Log in

Code 696219
Verify

Change Password

Login
Current Password
New Password
Repeat New Password
Change Password

Index
Messages
Add New Message

View messages.php will display all undeleted public messages for all user. The *My messages* hyperlink is only available for logged in users and leads to messages posted by that particular user. *Edit* and *Delete* button are no longer available in messages.php view and were moved to *My Messages* view.

session_expiration: 1732681474
Logged in: 1
Role: user

Messages

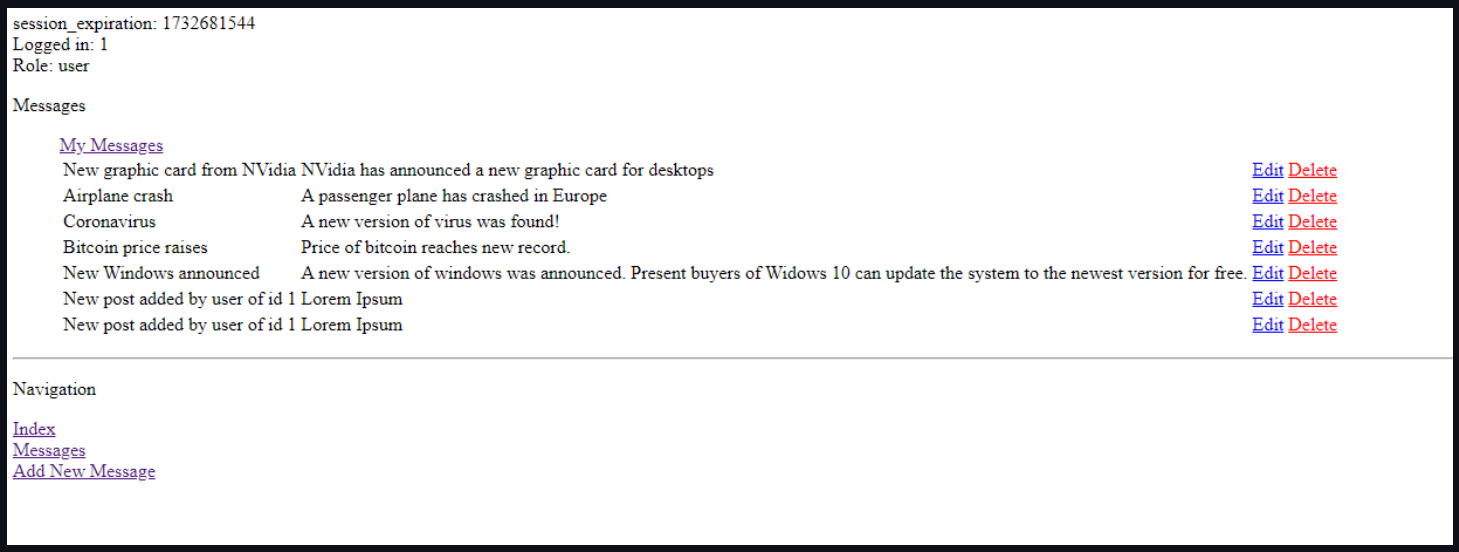
My Messages

New graphic card from NVidia	NVidia has announced a new graphic card for desktops
Airplane crash	A passenger plane has crashed in Europe
Coronavirus	A new version of virus was found!
Bitcoin price raises	Price of bitcoin reaches new record.
New Windows announced	A new version of windows was announced. Present buyers of Widows 10 can update the system to the newest version for free.
New post added by user of id 1	Lorem Ipsum
New post added by user of id 1	Lorem Ipsum

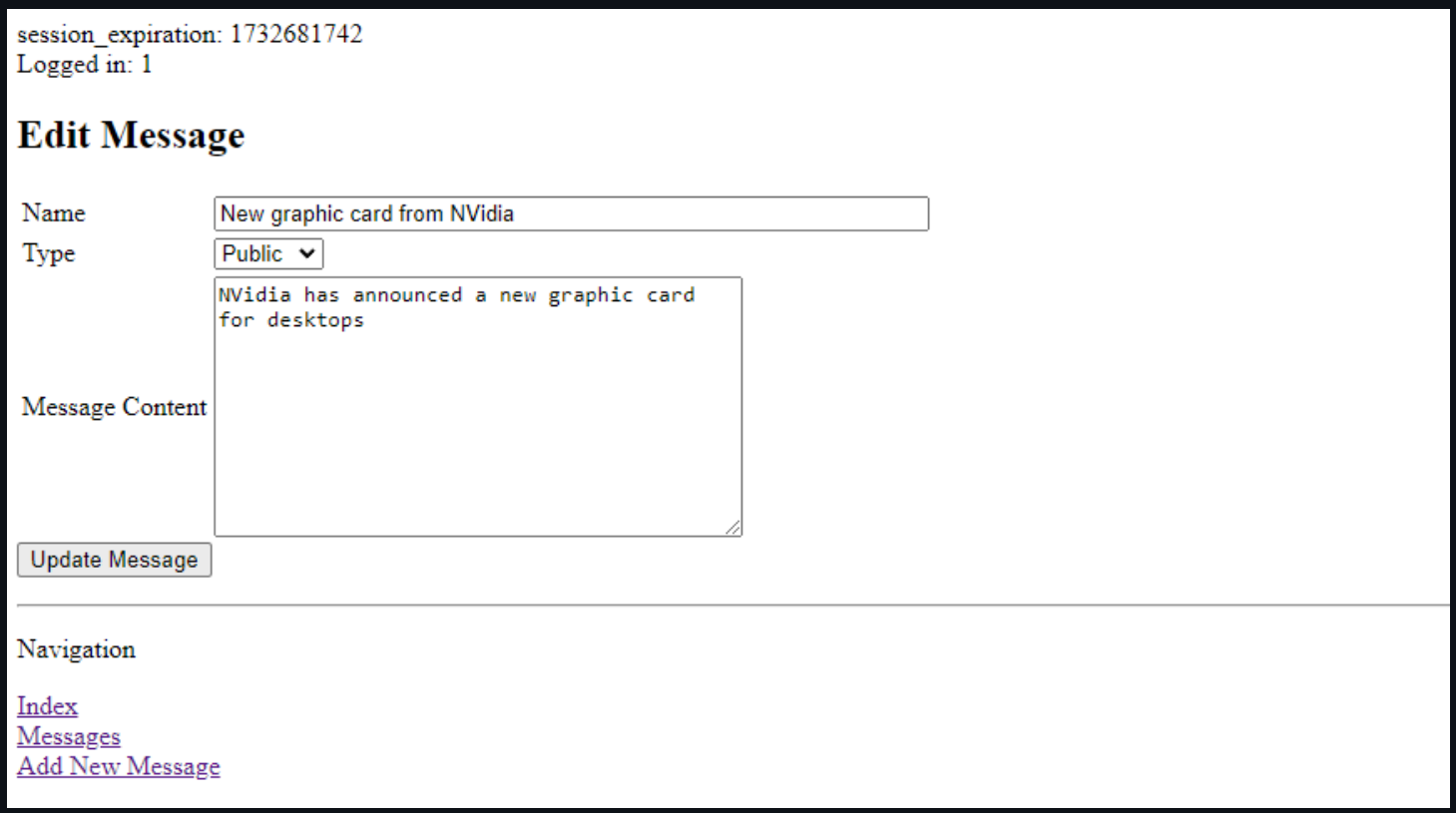
Navigation

Index
Messages
Add New Message

In *My Messages* user can see, edit and delete his own messages



Edit for user that owns a message



Successfull delete of user's own message

session_expiration: 1732681779
Logged in: 1
Role: user

Message deleted successfully.

Messages

My Messages

Airplane crash	A passenger plane has crashed in Europe
Coronavirus	A new version of virus was found!
Bitcoin price raises	Price of bitcoin reaches new record.
New Windows announced	A new version of windows was announced. Present buyers of Widows 10 can update the system to the newest version for free.
New post added by user of id 1	Lorem Ipsum
New post added by user of id 1	Lorem Ipsum

Navigation

Index
Messages
Add New Message

Now to show more security features I will login as new "test2" user with default role "user"

Main page

Register new user

login
email
password
repeat password
Create account

Log in

login test2
password test2
Log in

Code 275503
Verify

Change Password

Login
Current Password
New Password
Repeat New Password
Change Password

Index
Messages
Add New Message

I quickly created new message as user test2, which can be seen in overall messages view

session_expiration: 1732681844
Logged in: 1
Role: user

Messages

My Messages

Airplane crash	A passenger plane has crashed in Europe
Coronavirus	A new version of virus was found!
Bitcoin price raises	Price of bitcoin reaches new record.
New Windows announced	A new version of windows was announced. Present buyers of Widows 10 can update the system to the newest version for free.
New post added by user of id 1	Lorem Ipsum
New post added by user of id 1	Lorem Ipsum
New post added by user test2	Post made by user test2

Navigation

Index
Messages
Add New Message

View of *My Messages* for user test2

session_expiration: 1732681855
Logged in: 1
Role: user

Messages

My Messages

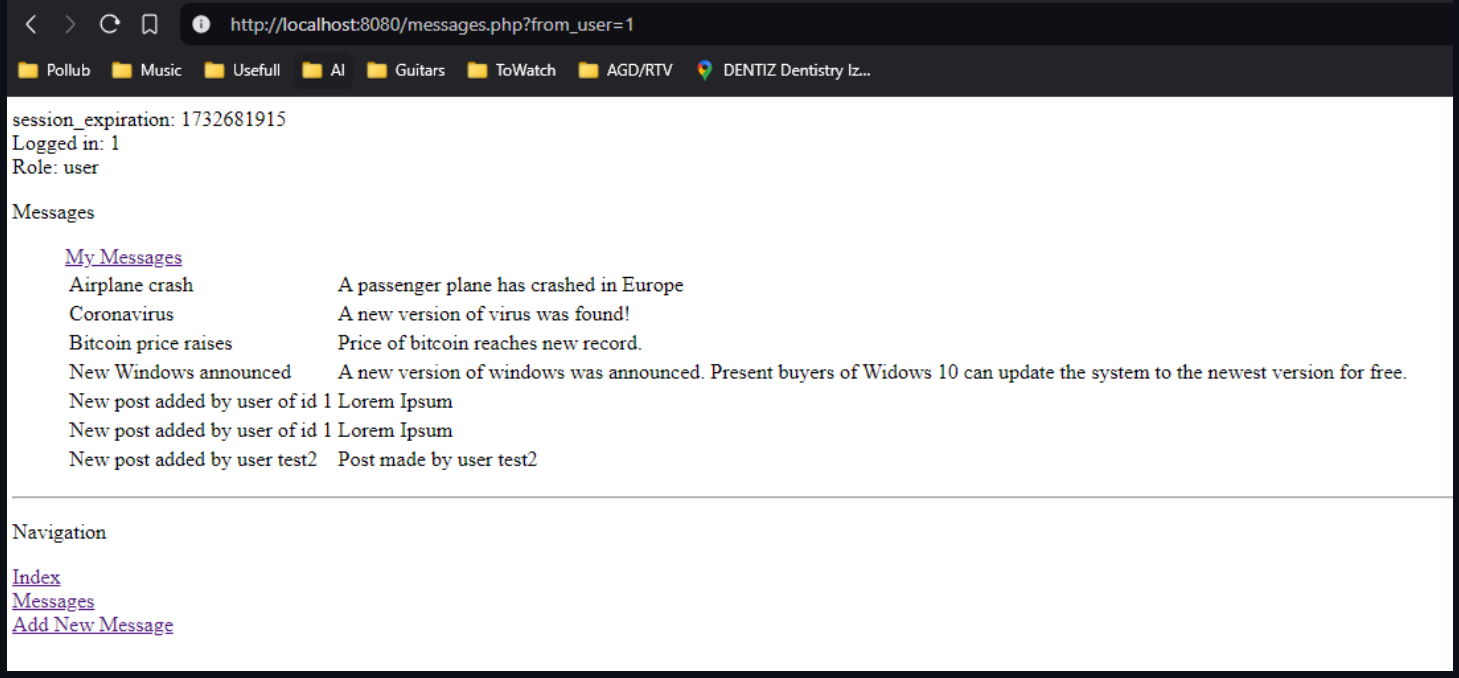
New post added by user test2 Post made by user test2 Edit Delete

---

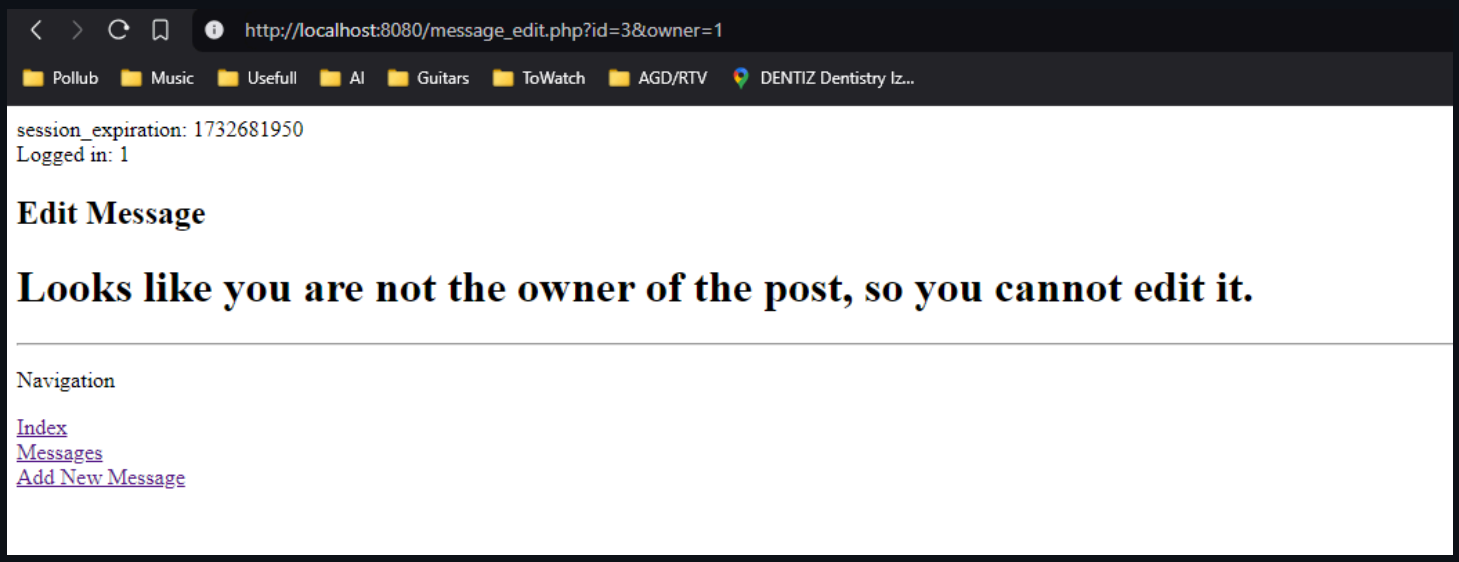
Navigation

Index
Messages
Add New Message

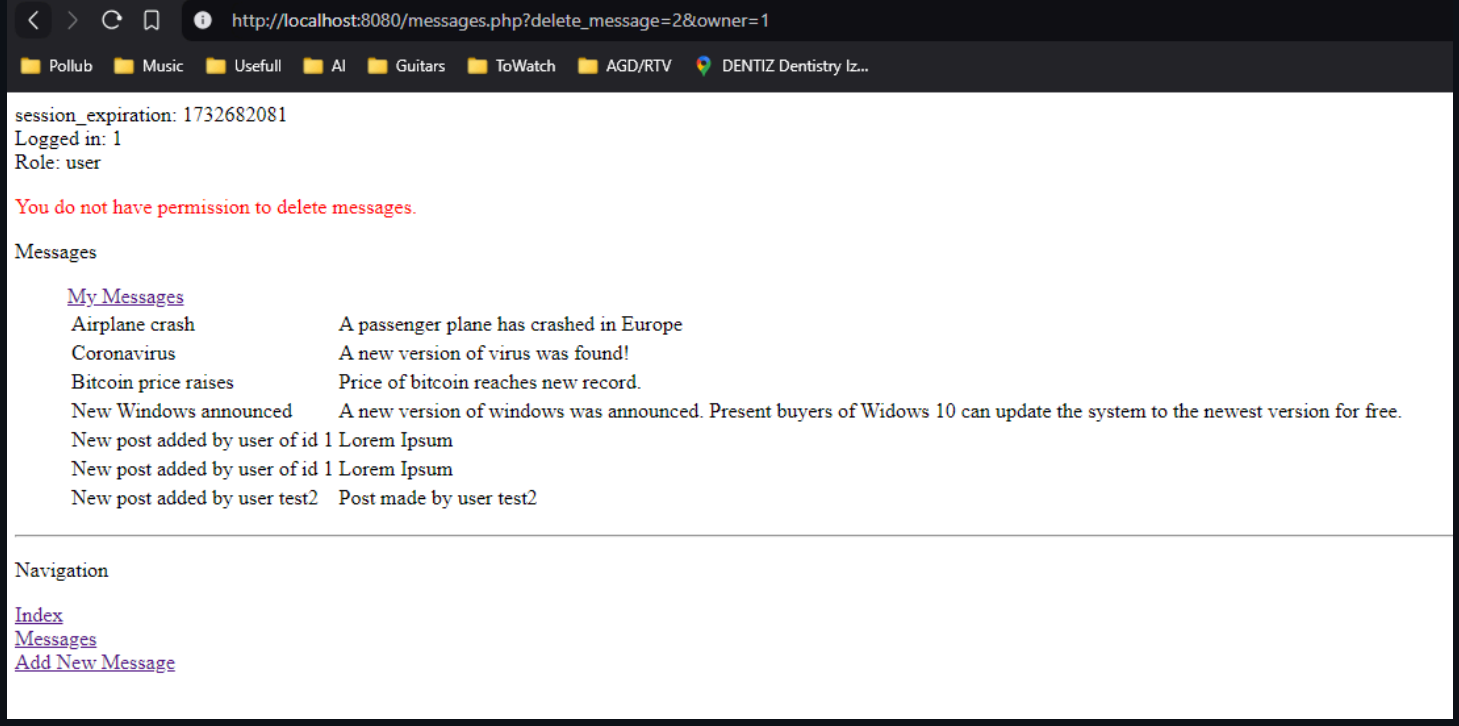
IN this example we can see how "test2" tries to access "My Messagess" view for "test" user, but because he isnt logged in as him, he sees just default "Messages.php" view that is available for all users



User "test2" tries to access edit form for message of id 3 that belongs to user of id 1 (test user)



User "test2" tries to delete message of id 2 that belongs to user of id 1 (test user) via url



Final view for admin or moderator that allows to see and access both edit and delete from "Messages.php" view