

Gabrysiewicz Update README.md

553cbe1 · 3 minutes ago

109 lines (89 loc) · 4.85 KB

PreviewCodeBlame

Raw

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 Fiddler (<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 deleting message that doesn't belong to us will lead to message of "You do not have permission to delete message".

WebAppSecurity / Delete message

SaveShare

GET

http://localhost:8080/messages.php?delete_message=1

Send

Params

Authorization

Headers (7)

Body

Scripts

Tests

Settings

Cookies

Query Params

<input checked="" type="checkbox"/>	Key	Value	Description	Bulk Edit
<input checked="" type="checkbox"/>	delete_message	1		
	Key	Value	Description	

Body

Cookies (1)

Headers (12)

Test Results

200 OK425 ms1.07 KB

Save Response

Pretty

Raw

Preview

Visualize

HTML

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

<title>messages</title>

<meta charset="UTF-8">

<meta name="viewport" content="width=device-width, initial-scale=1.0">

</head>

<body>

session_expiration: null
Logged in: null
Role: unknown

Warning: Undefined array key "role" in /var/www/html/messages.php on line 54

Warning: Undefined array key "role" in /var/www/html/messages.php on line 54

<p style="color:red;">You do not have permission to delete messages.</p>

<p>Messages</p>

<table>

<tr>

<td>New graphic card from Nvidia</td>

<td>Nvidia has announced a new graphic card for desktops</td>

<td>Edit</td>

</tr>

Postbot

Runner

Start Proxy

Cookies

Vault

Trash

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

OverviewGET ShowPOST Add PLPOST AddPUT UpdateDEL Update CopyWebAppSecurityGET Delete message+No environment

WebAppSecurity / Delete messageSaveShare

GEThttp://localhost:8080/privileges.phpSend

ParamsAuthorizationHeaders (7)BodyScriptsTestsSettingsCookies

Query Params

Key	Value	Description	Bulk Edit
Key	Value	Description	

BodyCookies (1)Headers (12)Test Results200 OK886 ms960 BSave Response

PrettyRawPreviewVisualizeHTML

```
41      flex-basis: 50%;
42    }
43
44    #display table {
45      width: 100%;
46      text-align: center;
47    }
48
49    #display table thead {
50      background-color: black;
51      color: white;
52      border-collapse: collapse;
53    }
54
55    #display table tr {
56      box-shadow: inset 0 0 5px 1px #ccc;
57    }
58  </style>
59 </head>
60
61 <body>
62   <br />
63   <b>Warning</b>: Undefined array key "role" in <b>/var/www/html/privileges.php</b> on line <b>284</b><br />
64   <br />
65   <b>Warning</b>: Undefined array key "role" in <b>/var/www/html/privileges.php</b> on line <b>284</b><br />
66
67 </body>
68
69 </html>
```

PostbotRunnerStart ProxyCookiesVaultTrash

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	<input type="text"/>
email	<input type="text"/>
password	<input type="text"/>
repeat password	<input type="text"/>
<input type="button" value="Create account"/>	

Log in

login	<input type="text" value="test"/>
password	<input type="text" value="test"/>
<input type="button" value="Log in"/>	
Code	<input type="text" value="696219"/>
<input type="button" value="Verify"/>	

Change Password

Login	<input type="text"/>
Current Password	<input type="text"/>
New Password	<input type="text"/>
Repeat New Password	<input type="text"/>
<input type="button" value="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

session_expiration: 1732681544

Logged in: 1

Role: user

Messages

[My Messages](#)

New graphic card from NVidia NVidia has announced a new graphic card for desktops

[Edit](#) [Delete](#)

Airplane crash A passenger plane has crashed in Europe

[Edit](#) [Delete](#)

Coronavirus A new version of virus was found!

[Edit](#) [Delete](#)

Bitcoin price raises Price of bitcoin reaches new record.

[Edit](#) [Delete](#)

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.

[Edit](#) [Delete](#)

New post added by user of id 1 Lorem Ipsum

[Edit](#) [Delete](#)

New post added by user of id 1 Lorem Ipsum

[Edit](#) [Delete](#)

Navigation

[Index](#)

[Messages](#)

[Add New Message](#)

Edit for user that owns a message

session_expiration: 1732681742

Logged in: 1

Edit Message

Name

Type

Public ▼

Message Content

NVidia has announced a new graphic card for desktops

Navigation

[Index](#)

[Messages](#)

[Add New 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

Log in

login
password

Code

Change Password

Login
Current Password
New Password
Repeat New 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

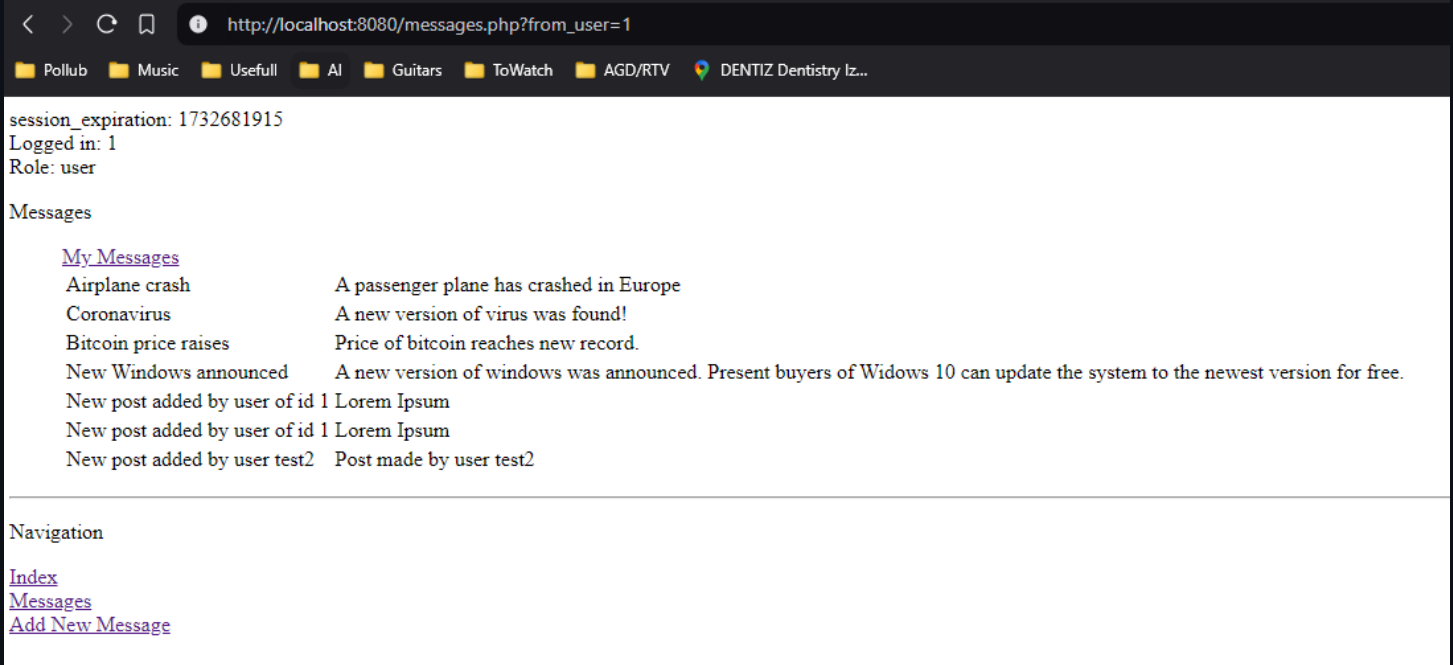
[My Messages](#)

New post added by user test2 Post made by user test2 [Edit](#) [Delete](#)

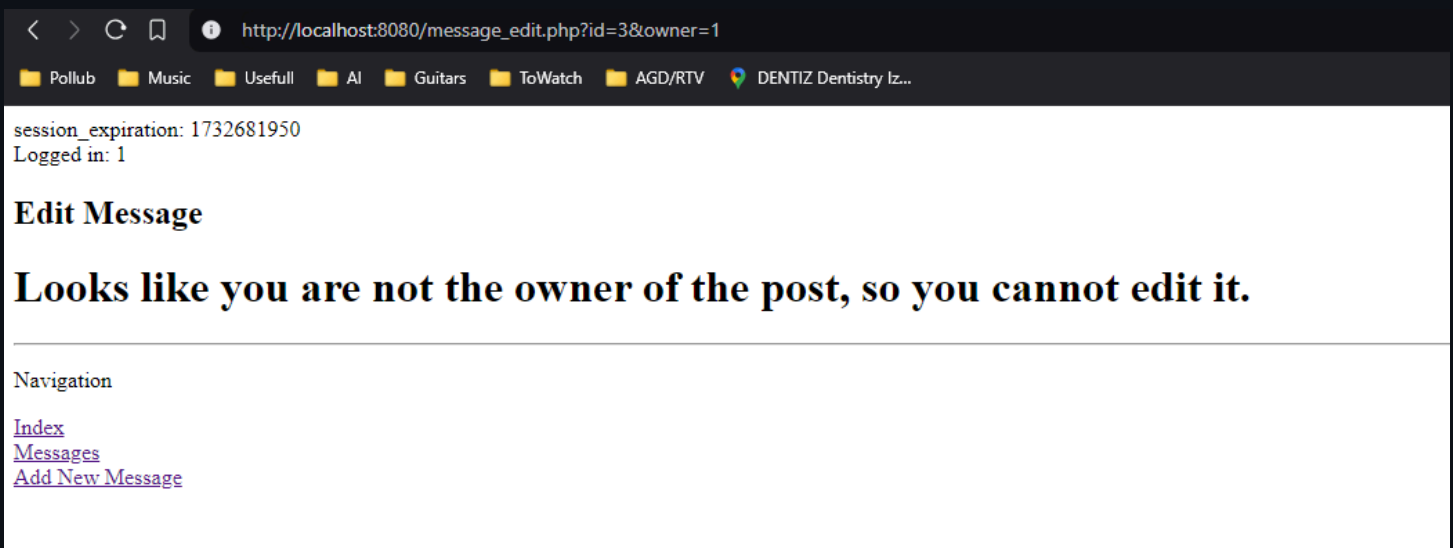
Navigation

[Index](#)
[Messages](#)
[Add New Message](#)

IN this example we can see how "test2" tries to access "My Messages" 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