BIBD Merchant Portal - Bug #16601

[MW-1 & MW-4][BE] Stored Cross-Site Scripting (XSS)

30 May 2023 04:33 PM - Nor Khairun Aqila Jesmen

Status:	Closed	**Start date:**	31 May 2023
Priority:	High	**Due date:**	08 June 2023
Assignee:	wanansari wanansari	**% Done:**	100%
Category:		**Estimated time:**	0.00 hour
Target version:		**Spent time:**	0.00 hour

Description

Description:
Stored cross-site scripting vulnerabilities arise when user input is stored and later embedded into the application's responses in an unsafe way.

Fixes:
1. Disable right-click for all pages as per RIB
2. Hide the user input at the URL
Modules involve - View User Profile, Modify User Profile, User Profile

Apply all fixes to both System Owner and Partner

History

#1 - 06 June 2023 09:55 AM - See Pin Leng

- Status changed from New to Resolved

fixes done.

#2 - 06 June 2023 03:05 PM - Nor Khairun Aqila Jesmen

- Status changed from Resolved to New

- % Done changed from 0 to 50

Issue still happen.

Issue 1: During loading still can right-click
Issue 2: Click the Image URL, display the source. Expected - Display image and cannot right click

#3 - 12 June 2023 12:32 PM - See Pin Leng

- File validate checking user profile.docx added

- Status changed from New to Resolved

- Assignee changed from See Pin Leng to Nor Khairun Aqila Jesmen

Issue fixed as below:
1. URL cant display sensitive information like userid and username- fixed for user profile(Admin) and my profile (etunai/while label/mobile widget)
2. validation user profile and my profile checking - already applied before fixed. Therefore, nothing to fixed and may refer to the document attached for coding validation checking screen capture information.
3. All HTML metacharacters, including < > " ' and =, should be replaced with the corresponding HTML entities (< > etc)- This one already applied to all module. This is due to coding at all listing page module did not replace with the corresponding HTML entities only, so it will display as function code in the listing page when using example :<h1>. Other page actually already automatic convert to HTML entities(refer to same doc with picture name : attachment 1)
4. hide the userid and username in view source web browser - No way can fix,
refer to the link mention no way can hide this: https://stackoverflow.com/questions/15168618/hide-values-from-page-source-but-show-on-page
4. fixed applied also in MA module.
5. For the right click issue, it no way to fixes.
6. Issue 2: Click the Image URL, display the source - will be solve later on

#4 - 12 June 2023 03:05 PM - Nor Khairun Aqila Jesmen

1 - tested good System Owner and MA
2 - noted
3 - tested good. display as per insert. No change color or font
4 - noted
5 - noted. remain unable to right click as per done. okay to remain as it is which able to right click when loading
6 - noted

As per discussed last Friday 9/6/2023, please apply to filter field not allow to enter < > " ' and = for field user id, username (if possible do for other fields also)

#5 - 12 June 2023 04:48 PM - Nor Khairun Aqila Jesmen

- Status changed from Resolved to New

- Assignee changed from Nor Khairun Aqila Jesmen to See Pin Leng

As per discussed last Friday 9/6/2023, please apply to filter field not allow to enter < > " ' and = for field user id, username (if possible do for other fields also if have extra time)

#6 - 12 June 2023 08:20 PM - See Pin Leng

- Status changed from New to Resolved

- Assignee changed from See Pin Leng to Nor Khairun Aqila Jesmen

requirement fixed to excluded <>"'= for username. userid BAU already excluded. It only allow alphanumeric only.

#7 - 13 June 2023 11:25 AM - Nor Khairun Aqila Jesmen

- Status changed from Resolved to Closed

- % Done changed from 50 to 100

Tested good

#8 - 13 June 2023 11:25 AM - Nor Khairun Aqila Jesmen

- Assignee changed from Nor Khairun Aqila Jesmen to wanansari wanansari

#9 - 03 July 2023 05:27 PM - Nor Khairun Aqila Jesmen

- Status changed from Closed to In Progress

- Assignee changed from wanansari wanansari to See Pin Leng

- % Done changed from 100 to 80

Issue:
at the System Information, have user information on the URL. And from there, when click back to the user information, will get error Method Not Allowed

#10 - 03 July 2023 05:36 PM - See Pin Leng

- Status changed from In Progress to Resolved

Issued fixed

1. all **userId** in Administrator User Profile & user information were encoded at URL and source code.
2. Its impact on Administrator User Profile & user information modules. Please re-test the module including validation,add,change,delete,etc.

#11 - 05 July 2023 09:15 AM - Nor Khairun Aqila Jesmen

- Status changed from Resolved to Closed

- Assignee changed from See Pin Leng to wanansari wanansari

- % Done changed from 80 to 100

Tested good by Feerman

Files

validate checking user profile.docx	318 KB	12 June 2023	See Pin Leng