

## ✓ FanBoxes: classic CSRF in Special:UserBoxes

Actions

✓ Closed, Resolved

Public

SECURITY

### Assigned To

ashley

### Authored By

ashley

2022-04-23 13:04:04 (UTC+0)

### Tags

Security

Social-Tools (Backlog)

FanBoxes (Backlog)

Vuln-CSRF (Tracked)

SecTeam-Processed (Completed)

### Referenced Files

None

### Subscribers

Aklapper

ashley

Bawolff

sbassett

### Description

`Special:UserBoxes`, the special page used to create new social user boxes and edit existing ones (pages in the `UserBox:` namespace), does not check for the presence of an anti-CSRF token, it will happily create/update the requested page as long as the request was `POST` ed and the desired form fields are set.

Quick patch:

```
diff --git a/includes/specials/SpecialFanBoxes.php b/includes/specials/SpecialFanBoxes.php
index aac26be..7835e2d 100644
--- a/includes/specials/SpecialFanBoxes.php
+++ b/includes/specials/SpecialFanBoxes.php
@@ -115,6 +115,7 @@ class FanBoxes extends SpecialPage {
     $output .= Html::hidden( 'textColorLeftSideColor', $update_fan-
>getFanBoxLeftTextColor(), [ 'id' => 'textColorLeftSideColor' ] ) . "\n";
```


```

        $output .= Html::hidden( 'bgColorRightSideColor', $update_fan-
>getFanBoxRightBgColor(), [ 'id' => 'bgColorRightSideColor' ] ) . "\n";
        $output .= Html::hidden( 'textColorRightSideColor', $update_fan-
>getFanBoxRightTextColor(), [ 'id' => 'textColorRightSideColor' ] ) . "\n";
+         $output .= Html::hidden( 'wpEditToken', $user->getEditToken() );
+
        $fantag_image_tag = '';
        if ( $update_fan->getFanBoxImage() ) {
@@ -254,6 +255,8 @@ class FanBoxes extends SpecialPage {
            <input type="hidden" name="bgColorRightSideColor" id="bgColorRightSideColor"
value="" />
            <input type="hidden" name="textColorRightSideColor"
id="textColorRightSideColor" value="" />;
+
+         $output .= Html::hidden( 'wpEditToken', $user->getEditToken() );
+
        if ( !$destination ) {
            $output .= '<h2 class="fanbox-form-label">' . $this->msg( 'fanbox-
title' )->escaped() . '</h2>
            <div class="create-fanbox-title">
@@ -330,6 +333,13 @@ class FanBoxes extends SpecialPage {

        // Send values to database and create fantag page when form is submitted
        if ( $request->wasPosted() ) {
+
+            // Protect against CSRF
+            if ( !$user->matchEditToken( $request->getVal( 'wpEditToken' ) ) ) {
+                $out->addWikiMsg( 'sessionfailure' );
+                $out->addReturnTo( $this->getPageTitle() );
+                return;
+            }
+
            if ( !$fanboxId ) {
                // @phan-suppress-next-line PhanTypeMismatchArgumentNullable
                $fan = FanBox::newFromName( $title );

```

## Details

Project	Subject
 mediawiki/extensions/FanBoxes	[SECURITY] Add anti-CSRF token to Special:UserBoxes
<a href="#">Customize query in Gerrit</a>	

## Related Objects

### Mentions

### Mentioned In

~~T305209: Write and send supplementary release announcement for extensions and skins with security patches (1.35.7/1.37.3/1.38.2)~~



 **ashley** created this task. 2022-04-23 13:04:04 (UTC+0)

  Restricted Application added a subscriber: **Aklapper**. · [View Herald Transcript](#) 2022-04-23 13:04:05 (UTC+0)


 **ashley** claimed this task. 2022-04-23 13:04:39 (UTC+0)


 **ashley** added projects: **Social-Tools**, **FanBoxes**, **Vuln-CSRF**.


 **ashley** added a subscriber: **Bawolff**. 2022-04-26 15:01:25 (UTC+0)

 **Bawolff** added a comment. 2022-04-26 15:03:10 (UTC+0) 

Looks like it fixes the problem


 **Bawolff** changed the visibility from "**Custom Policy**" to "Public (No Login Required)". 2022-04-26 15:19:45 (UTC+0)

 **Bawolff** changed the edit policy from "**Custom Policy**" to "All Users".

 **ashley** closed this task as *Resolved*. 2022-04-26 15:21:57 (UTC+0)

 **RhinosF1** mentioned this in ~~T305209: Write and send supplementary release announcement for extensions and skins with security patches (1.35.7/1.37.3/1.38.2)~~. 2022-04-27 19:43:38 (UTC+0)

 **sbassett** edited projects, added **SecTeam-Processed**; removed **Security-Team**. 2022-05-02 17:35:16 (UTC+0) 

 **sbassett** added a subscriber: **sbassett**.

**gerritbot**: <https://gerrit.wikimedia.org/r/c/mediawiki/extensions/FanBoxes/+786327>