☑ PrivateDomains: No anti-CSRF token in the edit form (CVE-2022-29903)

☑ Closed, Resolved 🌍 Public SECURITY

Actions

Assigned To

ashley

Authored By

ashley
2022-04-16 03:36:39 (UTC+0)

Tags

Security

PrivateDomains (Backlog)

Vuln-CSRF (Tracked)

SecTeam-Processed (Completed)

Referenced Files

None

Subscribers

Aklapper

ashley

Reedy

sbassett

Description

PrivateDomains' form at `Special:PrivateDomains` allows to effectively edit a bunch of pages in `NS_MEDIAWIKI` which are used by PrivateDomains to store its settings on-wiki...buuuuuuut there's no anti-CSRF check implemented on the special page, all it cares about is that the request was POSTed and that `action` is `submit`.

Details

Risk Rating
Medium

Author Affiliation
Wikimedia Communities

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)~~

rEPRD1ad65d4c1c19: [SECURITY] Add anti-CSRF token to the edit form + adjust some messages' escaping

ashley created this task. 2022-04-16 03:36:39 (UTC+0)

Restricted Application added a subscriber: **Aklapper**. · View Herald Transcript 2022-04-16 03:36:40 (UTC+0)

ashley claimed this task. 2022-04-16 03:37:09 (UTC+0)

ashley added projects: **PrivateDomains**, **Vuln-CSRF**.

ashley added a comment. 2022-04-16 03:40:34 (UTC+0)

```
diff --git a/includes/SpecialPrivateDomains.php b/includes/SpecialPrivateDomains.php
index 2b6c2ef..f13f444 100644
--- a/includes/SpecialPrivateDomains.php
+++ b/includes/SpecialPrivateDomains.php
@@ -67,18 +67,24 @@ class SpecialPrivateDomains extends SpecialPage {
         */
        public function execute( $par ) {
                $request = $this->getRequest();
+               $user = $this->getUser();

                $this->setHeaders();

                $msg = '';

                if ( $request->wasPosted() ) {
-                       if ( $request->getText( 'action' ) == 'submit' ) {
+                       $tokenOk = $user->matchEditToken( $request->getVal( 'wpEditToken' ) );
+                       if ( !$tokenOk ) {
+                               $msg = $this->msg( 'sessionfailure' )->parse();
+                       }
+
+                       if ( $request->getText( 'action' ) == 'submit' && $tokenOk ) {
                                $this->saveParam( 'privatedomains-domains', $request->getText(
'listdata' ) );
                                $this->saveParam( 'privatedomains-affiliatename', $request->getText(
'affiliateName' ) );
                                $this->saveParam( 'privatedomains-emailadmin', $request->getText(
'optionalPrivateDomainsEmail' ) );

-                               $msg = $this->msg( 'saveprivatedomains-success' )->text();
+                               $msg = $this->msg( 'saveprivatedomains-success' )->escaped();
                        }
                }

@@ -119,13 +125,14 @@ class SpecialPrivateDomains extends SpecialPage {
                // Render the main form for changing PrivateDomains' settings.
                $out->addHTML(
                        '<form name="privatedomains" id="privatedomains" method="post" action="' .
$action . '">
-               <label for="affiliateName"><br />' . $this->msg( 'privatedomains-affiliatenamelabel'
)->text() . ' </label>
+               <label for="affiliateName"><br />' . $this->msg( 'privatedomains-affiliatenamelabel'
)->escaped() . ' </label>
                <input type="text" name="affiliateName" width="30" value="' . $this->getParam(
'privatedomains-affiliatename' ) . '" />
-               <label for="optionalEmail"><br />' . $this->msg( 'privatedomains-emailadminlabel' )-
>text() . ' </label>
+               <label for="optionalEmail"><br />' . $this->msg( 'privatedomains-emailadminlabel' )-
>escaped() . ' </label>
                <input type="text" name="optionalPrivateDomainsEmail" value="' . $this->getParam(
'privatedomains-emailadmin' ) . '" />' );
                $out->addWikiMsg( 'privatedomains-instructions' );
                $out->addHTML( '<textarea name="listdata" rows="10" cols="40">' . $this->getParam(
'privatedomains-domains' ) . '</textarea>' );
-               $out->addHTML( '<br /><input type="submit" name="saveList" value="' . $this->msg(
'saveprefs' )->plain() . '" />' );
+               $out->addHTML( Html::hidden( 'wpEditToken', $user->getEditToken() ) );
+               $out->addHTML( '<br /><input type="submit" name="saveList" value="' . $this->msg(
'saveprefs' )->escaped() . '" />' );
                $out->addHTML( '</form>' );
        }
```

Quick patch which also adjusts the escaping of several UI messages used by the form because might as well fix that while I'm editing this portion of the code. (Also I'm too lazy to split out the changes, so...)

Reedy edited projects, added **SecTeam-Processed**; removed **Security-Team**. 2022-04-16 16:58:28 (UTC+0)

ashley mentioned this in **rEPRD1ad65d4c1c19: [SECURITY] Add anti-CSRF token to the edit form + adjust some messages' escaping**. 2022-04-17 09:02:14 (UTC+0)

sbassett 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)**~~. 2022-04-18 17:09:11 (UTC+0)

sbassett added a subscriber: **sbassett**.

@ashley - Seeing as how this was merged to master in gerrit, we can likely make this task public, correct? Or would other, affected mediawiki operators still prefer it remain protected for the time being?

sbassett triaged this task as *Medium* priority. 2022-04-18 17:10:37 (UTC+0)

sbassett changed Author Affiliation from N/A to Wikimedia Communities.

sbassett changed Risk Rating from N/A to Medium.

ashley closed this task as *Resolved*. 2022-04-19 18:35:16 (UTC+0)

ashley added a subscriber: **Reedy**.

> In ~~**T306290#7861597**~~, **@sbassett** wrote:
>
> **@ashley** - *Seeing as how this was merged to master in gerrit, we can likely make this task public, correct? Or would other, affected mediawiki operators still prefer it remain protected for the time being?*

Right, sorry, I meant to poke @Reedy about that on IRC but forgot; please feel free to do so, since that's really all that's left here, the bug is effectively resolved and the fix has been made available.

sbassett changed the visibility from "**Custom Policy**" to "Public (No Login Required)". 2022-04-19 18:44:17 (UTC+0)

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

Mstyles renamed this task from *PrivateDomains: No anti-CSRF token in the edit form* to *PrivateDomains: No anti-CSRF token in the edit form (CVE-2022-29903)*. 2022-07-06 17:51:27 (UTC+0)