

Cross-Site Scripting (XSS) Protection

 support.visualsp.com/knowledge-base/cross-site-scripting-xss-protection/

October 17, 2018

Applies to: **VisualSP Classic**

With the availability of the 5.5.9.0 update we now provide cross-site scripting protection. These instructions describe how to disable preview from the edit help item screen and the analytics screen using a Powershell cmdlet.

Summary:

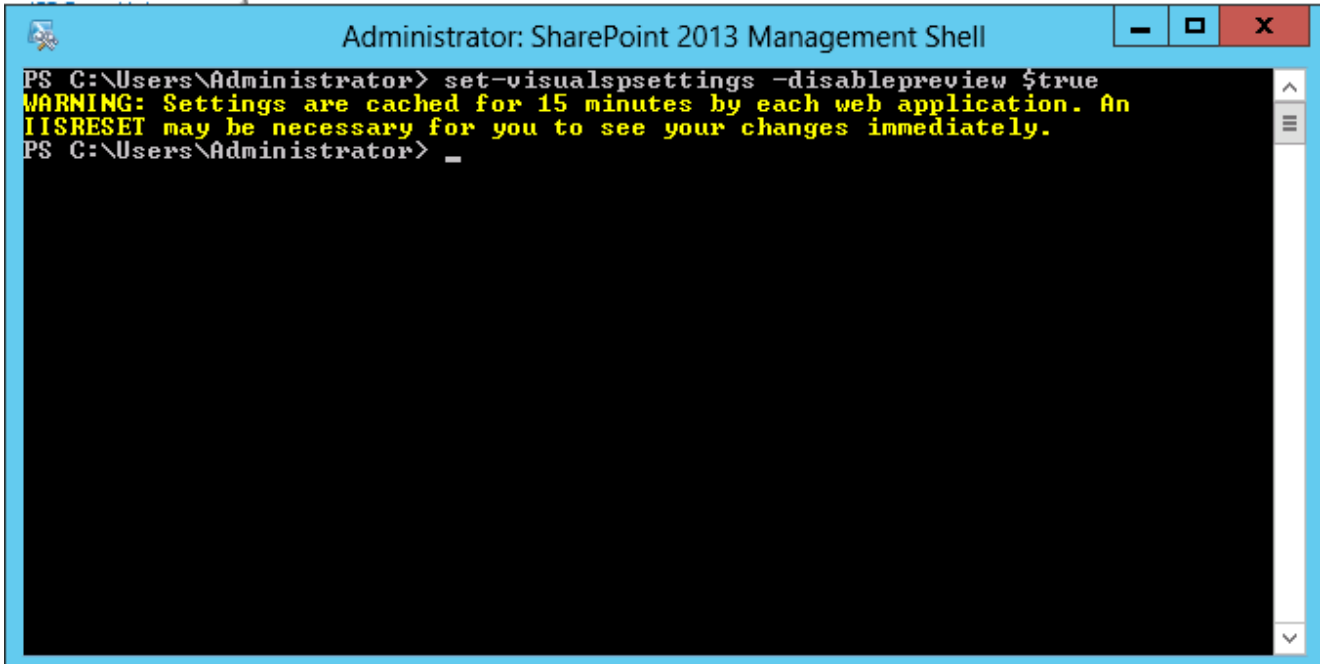
In order to facilitate the preview of a yet unsaved help item we pass the link property along the query string. Depending upon the viewer type, the query string could be rendered in such a way that a malicious user could use it to perpetrate a XSS attack.

Similarly, the analytics pages may provide the ability to preview a help item using the link property even if the original item may no longer exist. By disabling the preview feature the XSS vulnerability is no longer present.

Steps:

1. Deploy the 5.5.9.0 solution.
1. Open the SharePoint Management Shell
1. Run the following command:

```
Set-VisualSPSettings -DisablePreview $true
```



Expected Results

Go to Site Settings -> Manage VisualSP Help Items

Edit a Help item.

Before:

Help Item


Specify the localized details about the help item. Because the help item may be displayed in different web applications it is recommended that you use an absolute URL and not a relative URL (where applicable) for the link.

Locale ID: Default

Group: Existing Group: Library Look and Feel

Title: Add a library to the Quick Launch

Description: This video shows how to add a link to a library on the quick launch menu

Link: 

Show In New Window: If checked then the content will be displayed in a new window. Otherwise, a dialog will be used to display the content.

Viewer / Media Type: Default Video Player

After:

Help Item

Specify the localized details about the help item. Because the help item may be displayed in different web applications it is recommended that you use an absolute URL and not a relative URL (where applicable) for the link.

Locale ID

Default

Help Item Details - Default

Group

Existing Group: Library Look and Feel

Title

Add a library to the Quick Launch

Description

This video shows how to add a link to a library on the quick launch menu

Link

http://c4968397007/sites/visualspfarmhl Browse...



For example, "http://company.com/ContentHub/SiteAssets/1033/Videos/10101/10101.mp4".

Show In New Window

If checked then the content will be displayed in a new window. Otherwise, a dialog will be used to display the content.

Viewer / Media Type

Default Video Player

For Analytics, go to Site Settings -> View Analytics Report

Before:

Clicks by Ribbon Item

	Title	Group	Locale	Clicks	Percentage
1.	Create new documents	Creating Documents	1033	15	14.42%
2.	Wiki Page quick reference	Quick Reference	1033	10	9.62%
3.	Customize Quick Launch menu	Site Look and Feel	1033	6	5.77%
4.	Upload a document	Creating Documents	1033	6	5.77%
5.	Customize Top Navigation	Site Look and Feel	1033	5	4.81%
6.	Document Library quick reference	Quick Reference	1033	4	3.85%
7.	Delete me (absolute URL)	Help documents	1033	4	3.85%
8.	Create a web page	Web Page Creation	1033	3	2.88%
9.	Help System Documentation	Advanced Customization	1033	3	2.88%
10.	Upload multiple documents	Creating Documents	1033	3	2.88%

Show rows: 10 Go to page: 1 1 - 42 of 42

After:

Clicks by Ribbon Item

	Title	Group	Locale	Clicks	Percentage
1.	Create new documents	Creating Documents	1033	7	14.58%
2.	Upload a document	Creating Documents	1033	5	10.42%
3.	Delete me (absolute URL)	Help documents	1033	4	8.33%
4.	Delete me (relative URL)	Help documents	1033	3	6.25%
5.	Customize Top Navigation	Site Look and Feel	1033	2	4.17%
6.	Check in a document	Managing Documents	1033	2	4.17%
7.	SharePoint in Plain English	Overview	1033	2	4.17%
8.	Create new documents	Creating Documents	1033	2	4.17%
9.	Document Library quick reference	Quick Reference	1033	2	4.17%
10.	Help System Videos	VisualSP Help System	1033	2	4.17%

Show rows: 10 Go to page: 1 1 - 24 of 24

Updated on October 17, 2018

Tagged: VisualSP Classic