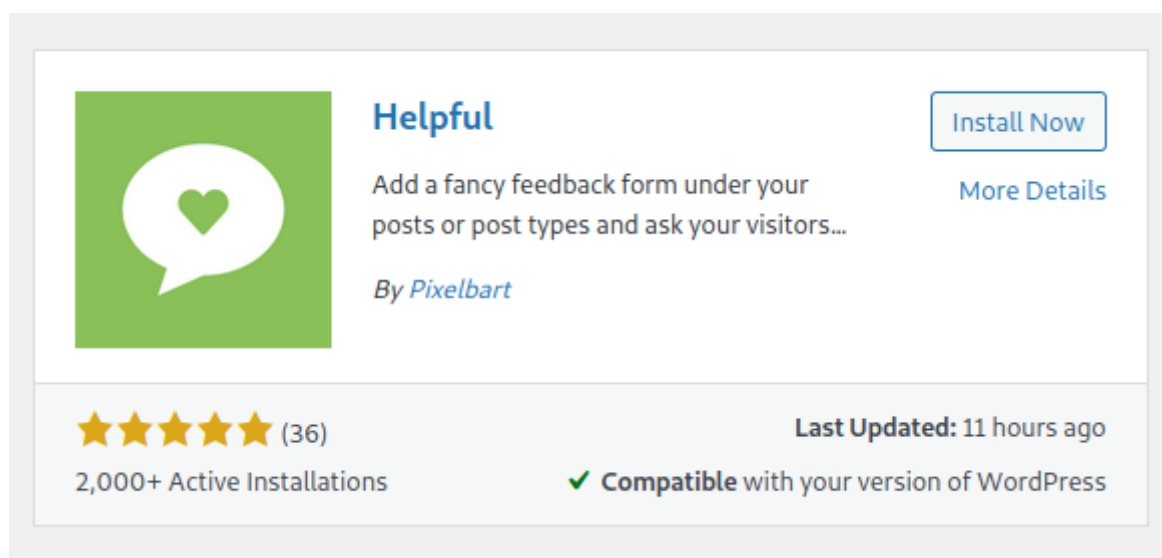


Wordpress Plugin



Helpful

Add a fancy feedback form under your posts or post types and ask your visitors...

By *Pixelbart*

Install Now

More Details

★★★★★ (36)

2,000+ Active Installations

Last Updated: 11 hours ago

✓ Compatible with your version of WordPress

Version : **4.4.55**

Author : <https://pixelbart.de/>

Link : <https://wordpress.org/plugins/helpful/>

Download : <https://downloads.wordpress.org/plugin/helpful.4.4.55.zip>

Information

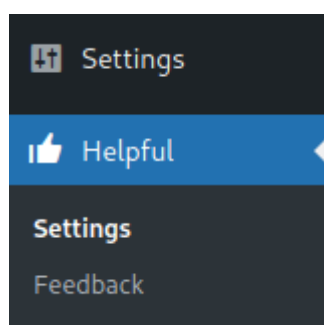
Exploit title : **XSS Stored Helpful 4.4.55**

Date : **06-10-2021**

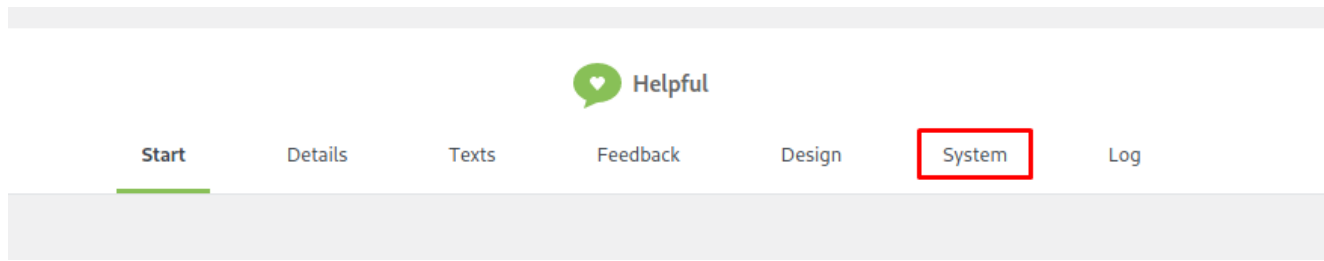
Exploit Author : https://twitter.com/mika_sec

Exploitation

For our example go to **Helpful** and click on **Settings** :



And now navigate to **System** :

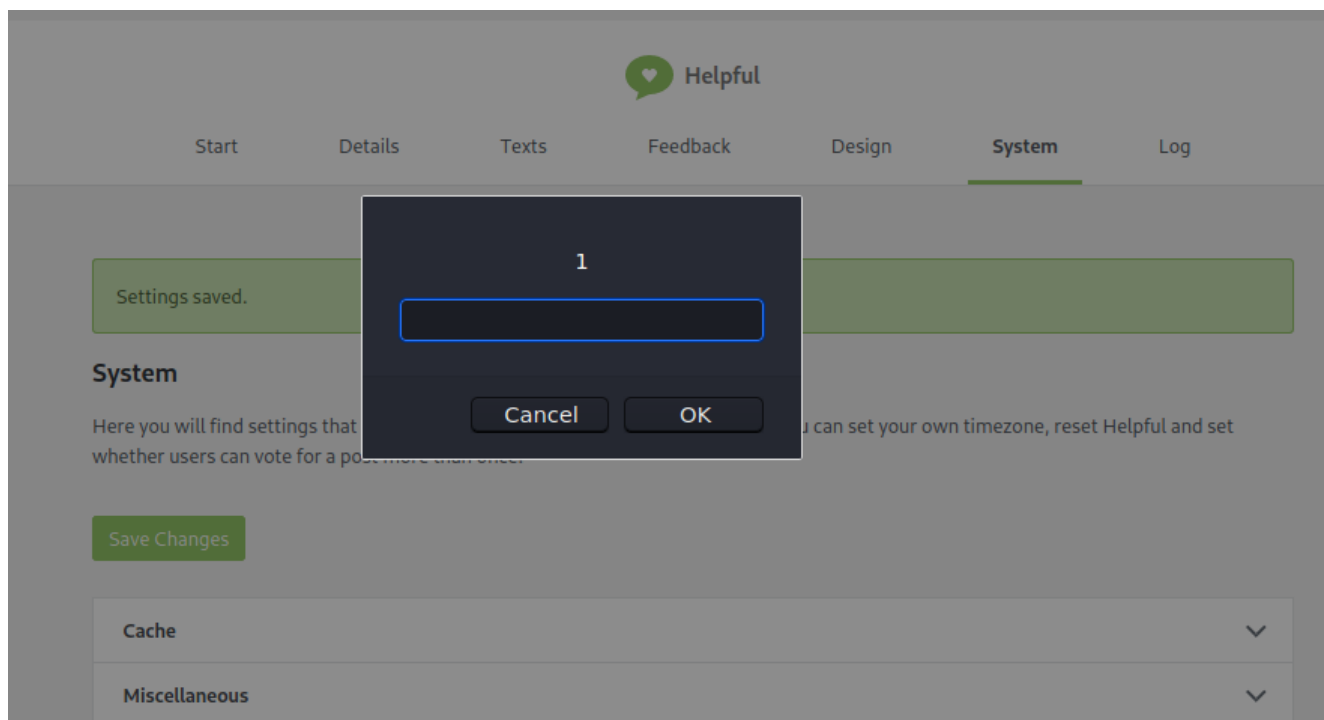


Click on **Miscellaneous** and inject in **Custom timezone** field this payload & after that click on **Save Changes** :

```
"><details open ontoggle="prompt(1)">
```



It will be **stored** and **reflected** every time the **admin** comes here :



But it's not the only **Stored XSS**, now we can use the same technique here :

Helpful

Start Details **Texts** Feedback Design System Log

Texts

Most texts can be changed here. You can also leave fields blank to not display anything at this point. Available helpers: `{pro}`, `{contra}`, `{total}`, `{pro_percent}`, `{contra_percent}`, `{permalink}`, `{author}`, `{feedback_form}`, `{feedback_toggle}`

`{feedback_form}`, `{feedback_toggle}` should only be used in the texts after the user has voted. Otherwise it can lead to bugs and Helpful does not save feedback properly!

Save Changes

- Before voting
- After voting
- Answer buttons**
- Admin columns

Save Changes

It's also works in **Before voting, After voting & Feedback** fields, for our example i'll choose **Answer buttons** :

Answer buttons

Button (pro)

Here you can define your own text for the pro button. You can use HTML to use e.g. Font Awesome.

Button (contra)

`><details open ontoggle="prompt(1)">|`

Here you can define your own text for the contra button. You can use HTML to use e.g. Font Awesome.

Disable the pro button

Disable the contra button

Admin columns

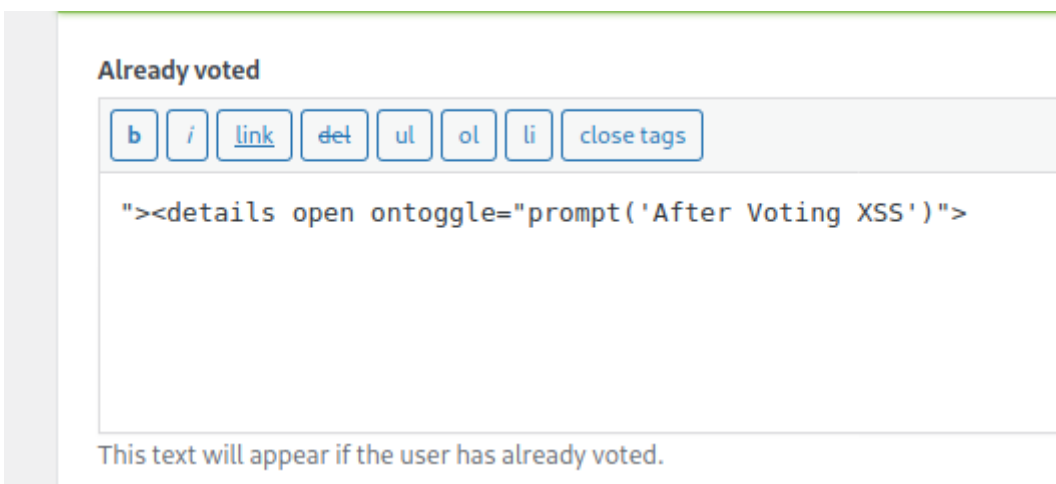
Save Changes

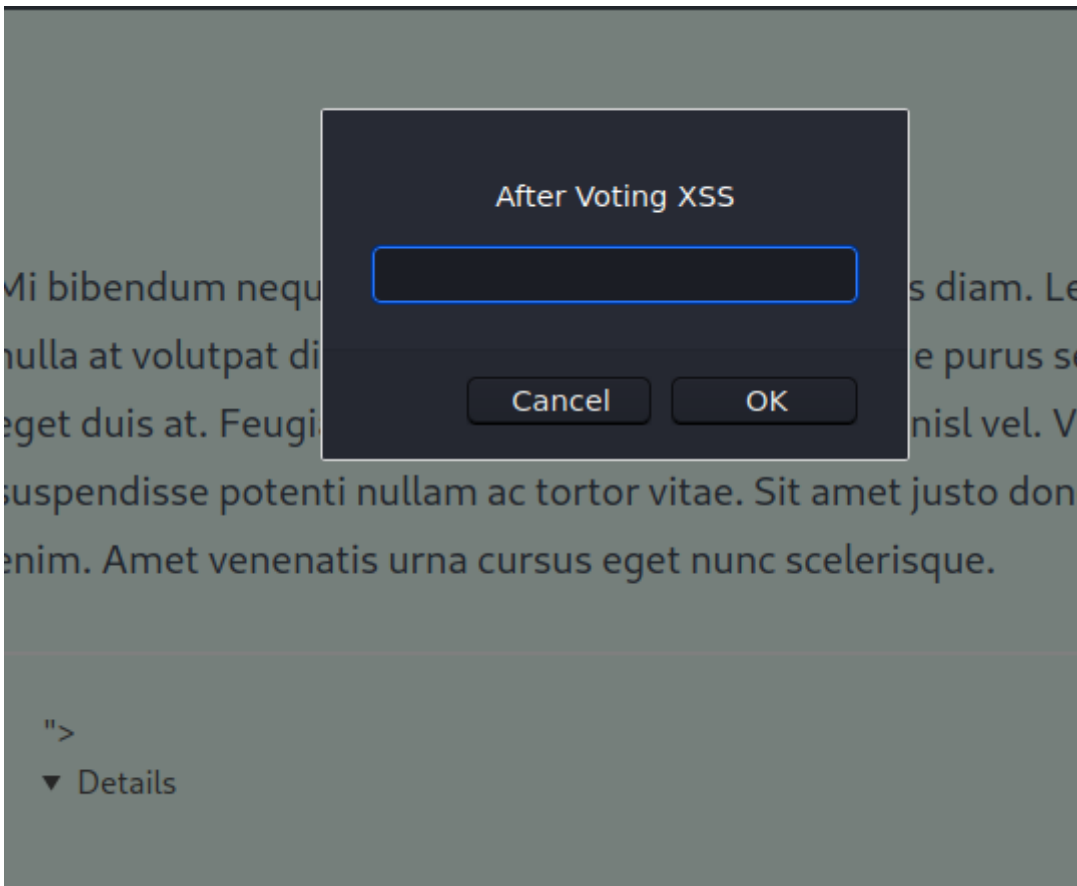
\

If we go to a post where the **Helpful widget** is, the payload will run when the **button loads** :



You can use the same technique for **After voting**, it will run after your vote (depends on your voting choice).





Feedback fields are also vulnerable :

