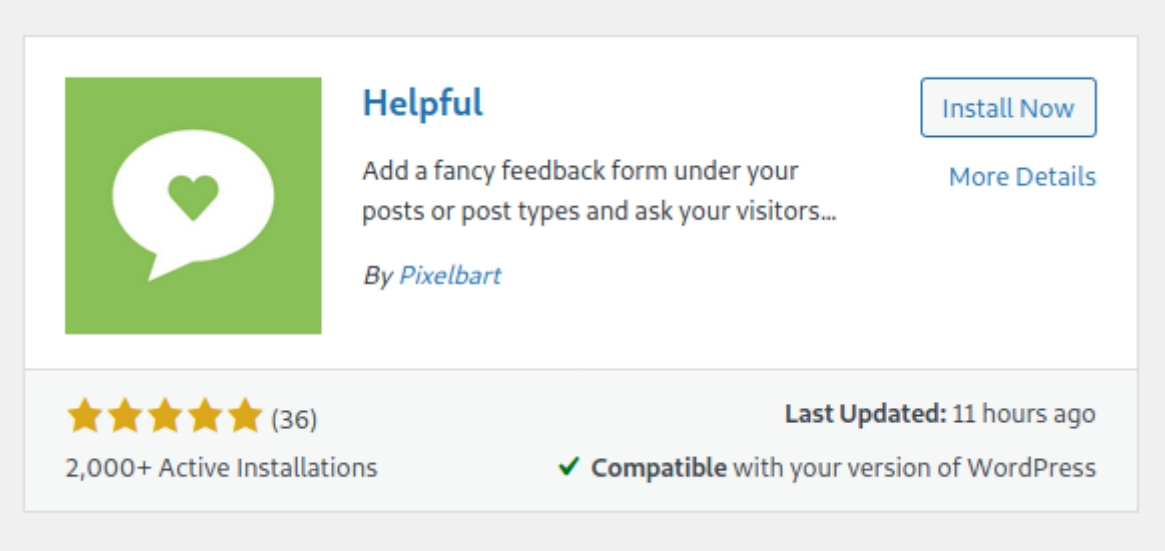
Wordpress Plugin



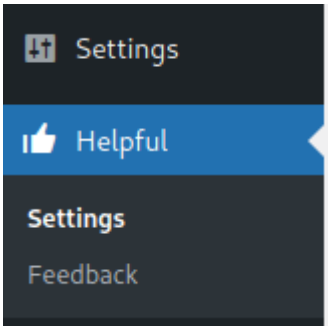
Version : **4.4.55**
Author : **https://pixelbart.de/**
Link : **https://wordpress.org/plugins/helpful/**
Download : **https://downloads.wordpress.org/plugin/helpful.4.4.55.zip**

Information

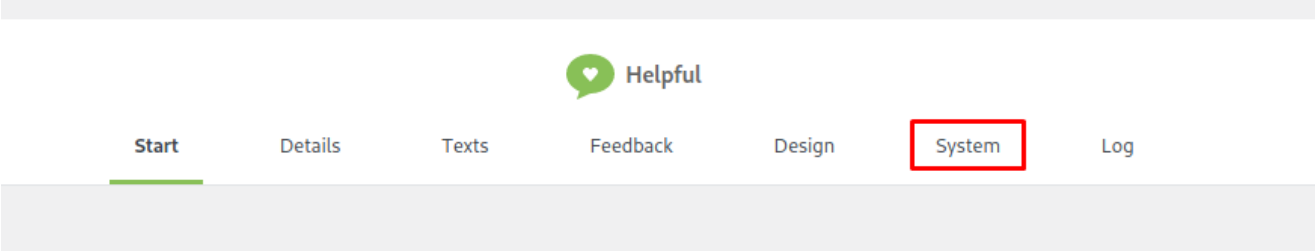
Exploit title : **XSS Stored Helpful 4.4.55**
Date : **06-10-2021**
Exploit Author : **https://twitter.com/mika_sec**

Exploitation

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

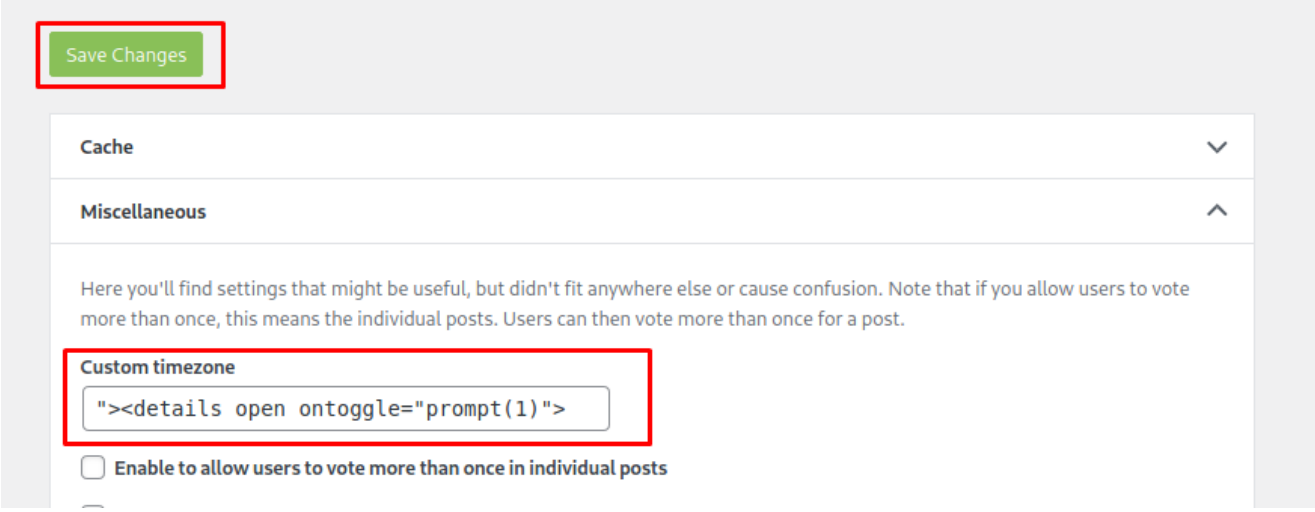


And now navigate to **System** :

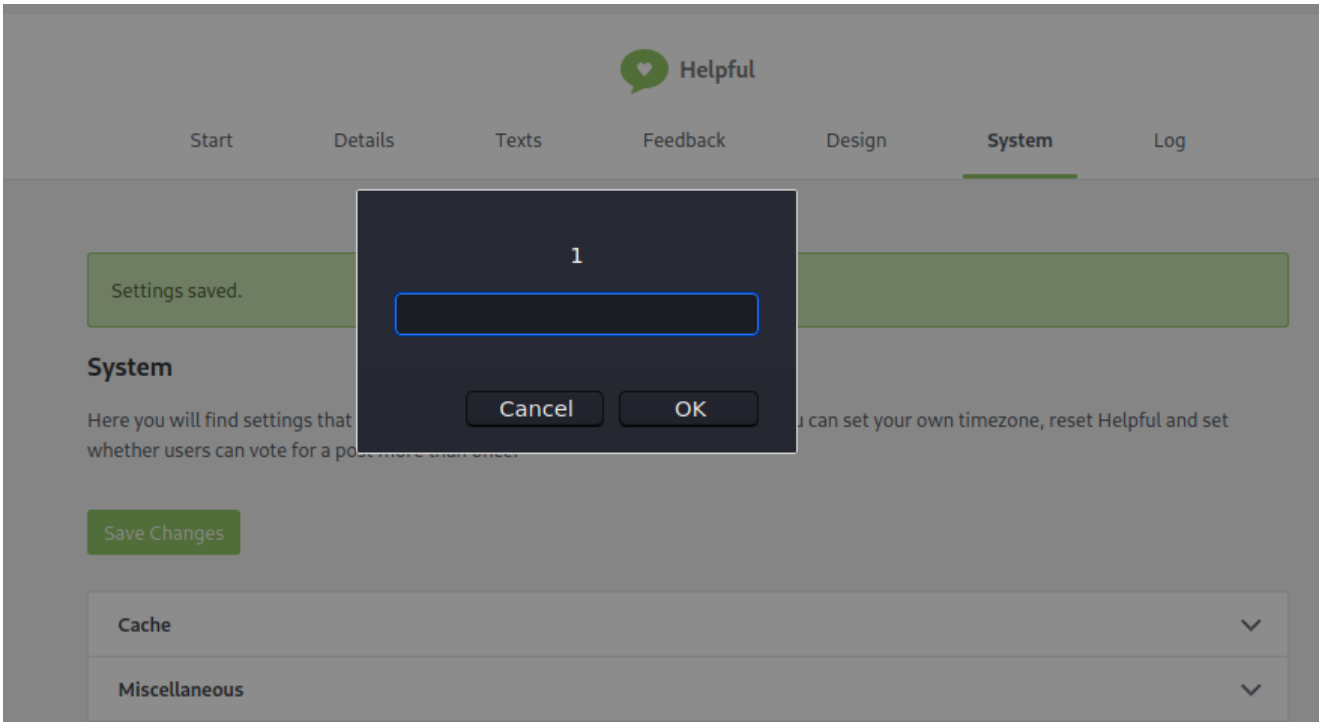


Click on **Miscellaneous** and inject in **Custom timezone** field this payload & after that click on **Save Changes** :

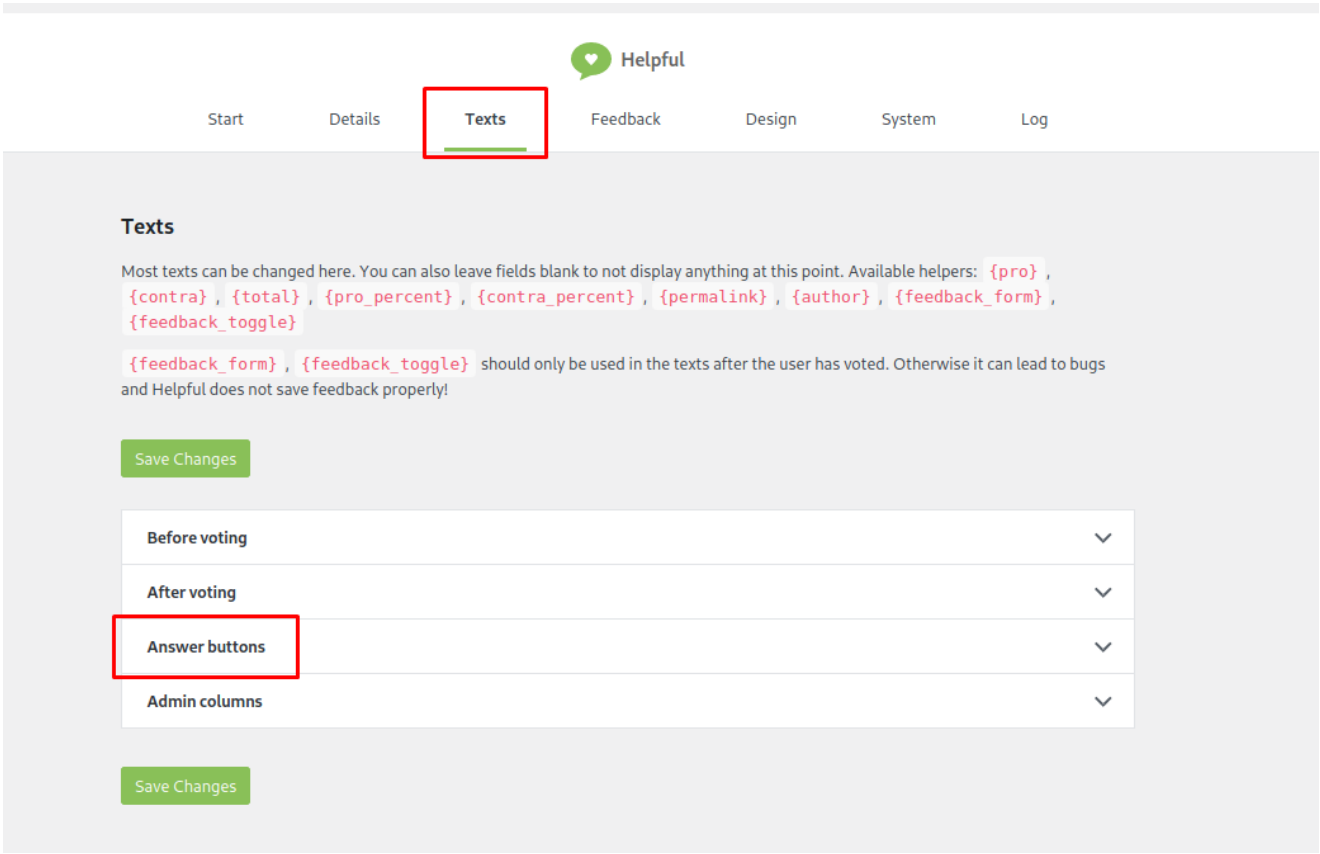
```
"><details open ontoggle="prompt(1)">
```



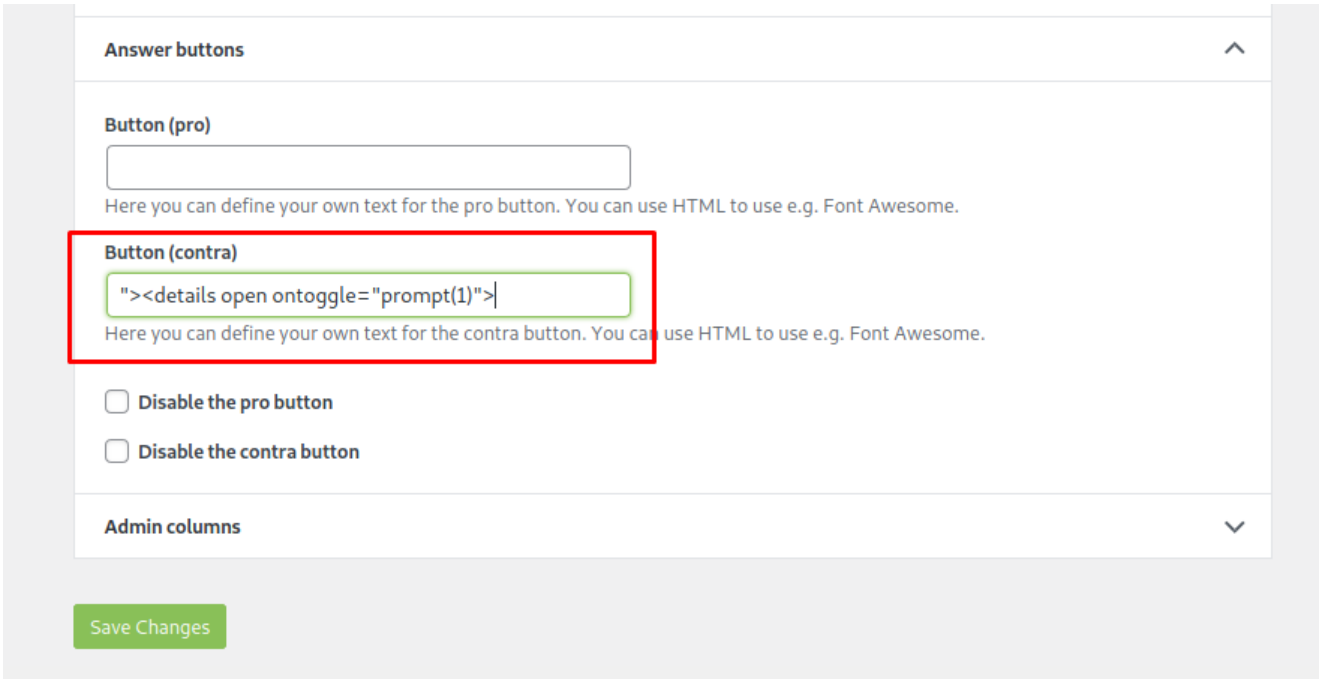
It will be **stored** and **reflected** every time the **admin** comes here :



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

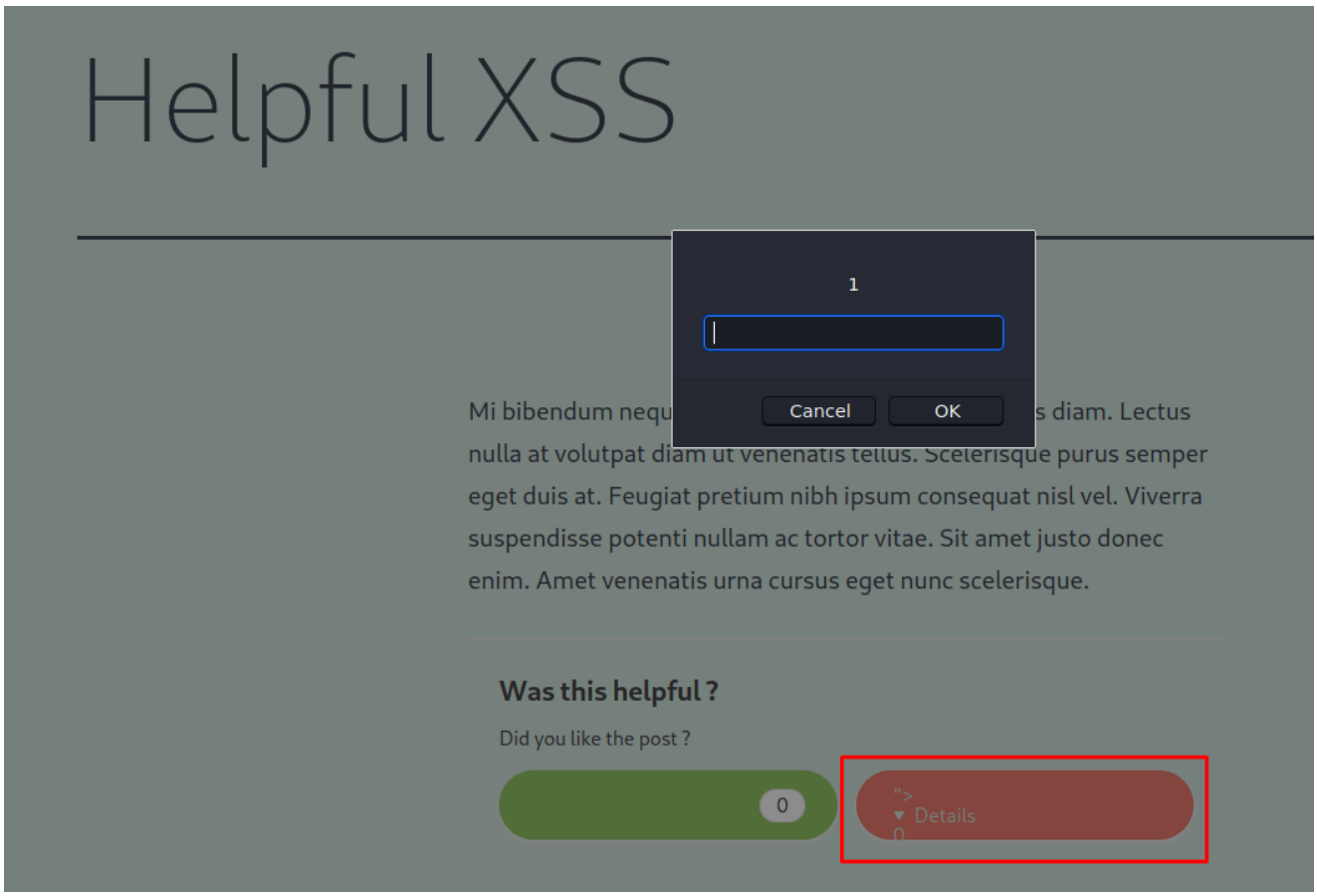


It's also works in **Before voting, After voting & Feeback** fields, for our example i'll choose **Answer buttons** :

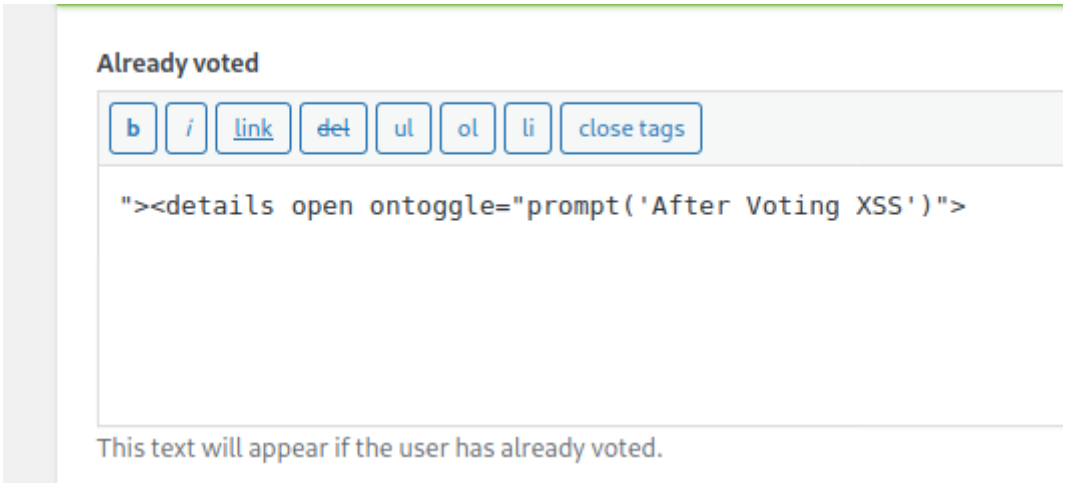


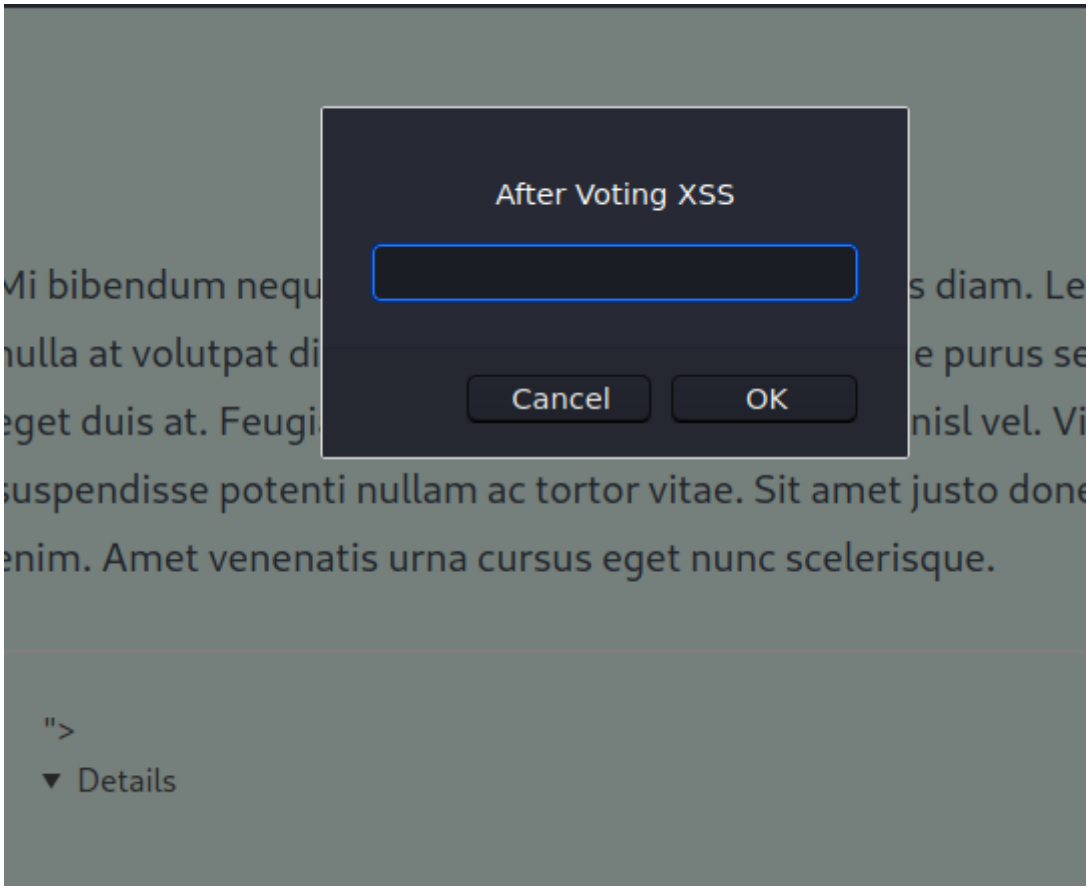
\

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).





Feeback fields are also vulnerable :