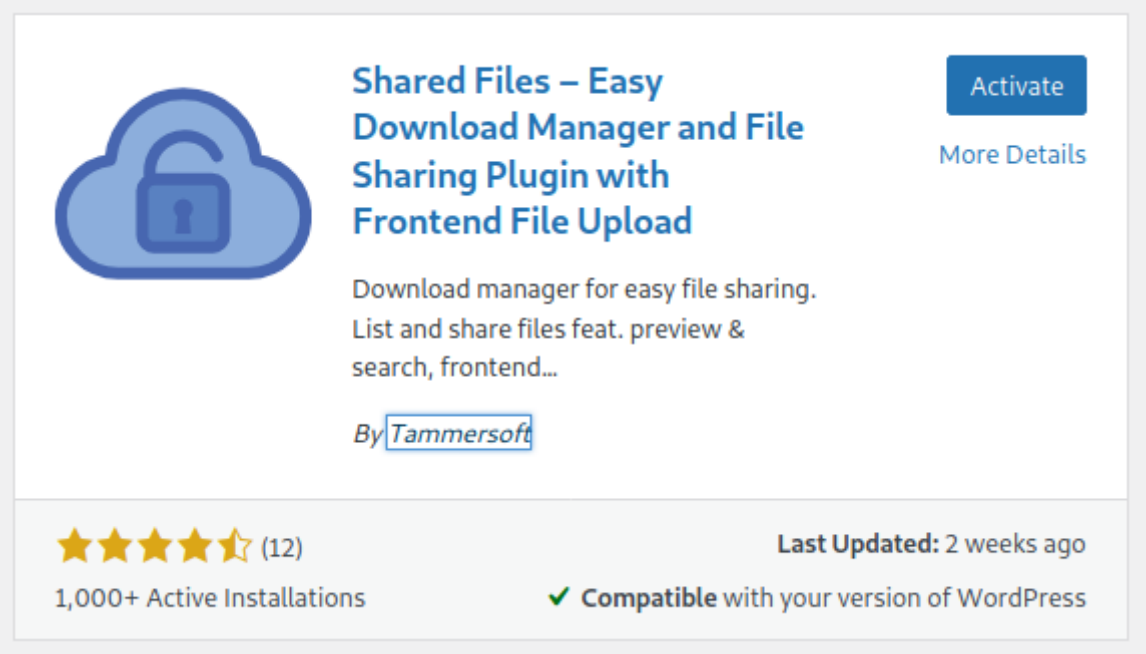
Wordpress Plugin



Version : ****1.6.59****
Author : https://www.tammersoft.com/
Link : https://wordpress.org/plugins/shared-files/
Download : https://downloads.wordpress.org/plugin/shared-files.1.6.59.zip

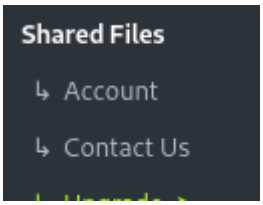
---

Information

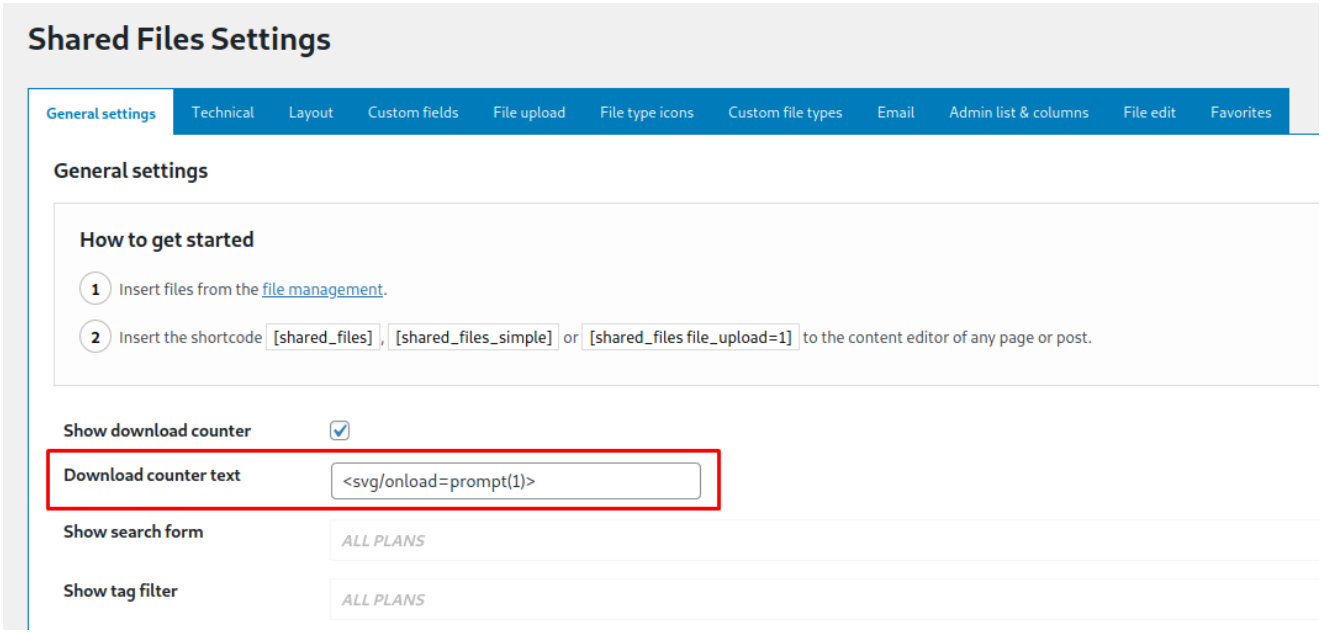
Exploit title : **XSS Stored Shared Files**
Date : **11-10-2021**
Exploit Author : https://twitter.com/mika_sec

Exploitation

Go to **Settings** & **Shared Files** :



Download counter text is vulnerable to **XSS Injection** :



You can use this **payload** :

```
<svg/onload=prompt(1)>
```

If we go to a page where the **Shared Files** widget is, the payload will run when the **Download counter text** loads :