New issue

Jump to bottom

Reflected XSS attack in /widgets/debug.php with the a parameter in AtomCMS 2.0 #258

Open **bkfish** opened this issue on Feb 16 · 1 comment

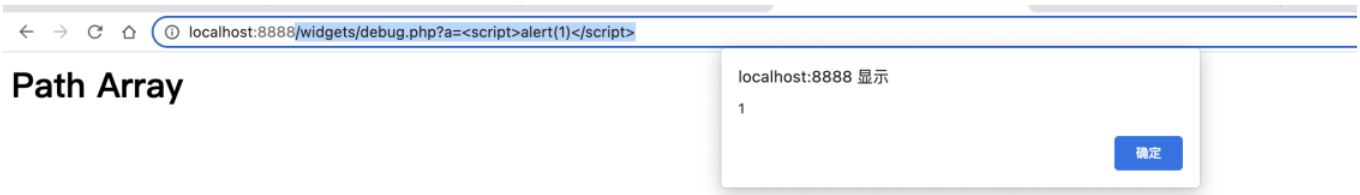
bkfish commented on Feb 16

EXPECTED BEHAVIOUR

An authenticated malicious user can take advantage of a Reflected XSS vulnerability in /widgets/debug.php

exp

```
/widgets/debug.php?a=<script>alert(1)</script>
```



analysis

/widgets/debug.php line 20 without any filter.

```
        <pre>
<?php print_r($_GET); ?>
        </pre>
```

creptor commented on Feb 17 Contributor

Thank you for taking the time to write this Issue for the project. It's very helpful for new users to understand some of the common problems they can face while developing a website on any platform.

XSS (Cross Site Scripting) I believe could be present on various locations (in the Atom.CMS project) due to the very small amount of filters in place and the way they're handled. That said, this is a very interesting problem that I didn't get to explore while I was doing the series.

I haven't investigated deeply but I believe this stack overflow question (and the most upvoted answer) explores some solutions on mitigating the issue, but you should align the solution to the expected output of the site. Also you can find filters on the PHP Documentation.

Either way, I should note that when dealing with inputs there should be always filters in place to block any unwanted values, so there're no negative effects on the behavior of the site, like with XSS.

Remember that Atom.CMS is **not** meant to be used in production, and it should be used solely for learning PHP in a controlled environment.

I'm not the author or maintainer of this project, just someone who learned a lot from the YouTube series and is willing to help.