New issue

Jump to bottom

There is a Stored-XSS vulnerability in Dswjcms 1.6.4 #4

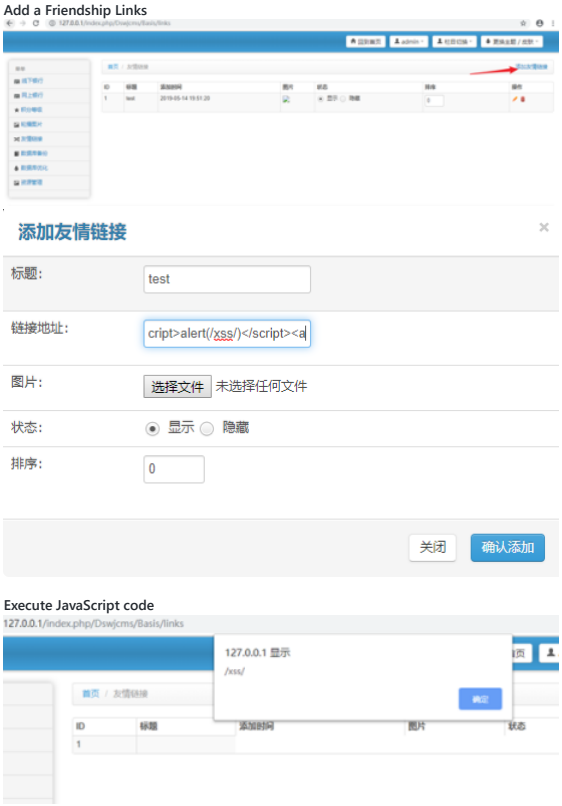
Open 5huai opened this issue on May 14, 2019 · 1 comment

5huai commented on May 14, 2019

A Stored-XSS vulnerability exists in Dswjcms 1.6.4, allowing an remote attacker to execute HTML or JavaScript code via the index.php/Dswjcms/Basis/links

PoC: "><script>alert(/xss/)</script><a

Add a Friendship Links



Execute JavaScript code

tifaweb commented on May 15, 2019 Owner

后台没做SQL注入过滤，后台权限也是最简单的，所以开源版是很容易进行SQL注入的，这个项目也没有进行维护了，TP版本过老，国内市场也不行

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants