山东省网络安全技能大赛 部分writeup

转载

weixin_30641465 于 2018-11-08 12:17:00 发布 489 收藏 1
原文链接：http://www.cnblogs.com/whitehawk/p/9928347.html
版权

web1

提示：ip不在范围内

直接抓包加client-ip: 127.0.0.1

即可得到flag

web2

```
<?php

    include 'here.php';
    $key = 'kelaibei';

    if(isset($_GET['id'])){
        $id = $_GET['id'];
        @parse_str($id);
        if ($key[99] != 'aabg7XSs' && md5($key[99]) == md5('aabg7XSs')) {
           echo $hint;
        }
        else{
            echo 'try again';
        }
    }
    else{
        show_source(__FILE__);
    }
```

百度 parse_str()函数，这个函数是将参数变为变量，比如parse_str("a=123"),就是$a=123，然后看 if条件，利用PHP弱类型，百度0e开头的MD5，最后构造payload：$id=key[99]=s878926199a,进入下一关。

这就比较难受了，不管输入什么，文件内容都被修改为too slow，我能有多快，fuck。后续部分，这篇写的更详细，请参考https://www.freebuf.com/column/182132.html

misc crack it

下载文件，得到shadow，打开发现是linux用户密码的格式，直接放到kali下，john解密，得到flag。

misc basic

打开文件都是RGB值，通过一些手段计算一共有135000组RGB值。

```
from PIL import Image

x = 150    #x坐标  分解135000为150X900
y = 900    #y坐标

im = Image.new("RGB", (x, y))   #建立图片
file = open('basic.txt')    #打开basic.txt

for i in range(0, x):
    for j in range(0, y):
        line = file.readline().replace('(','').replace(')','')   #去掉括号
        rgb = line.split(",")    #分割语句  下边举例子解释
        im.putpixel((i, j), (int(rgb[0]), int(rgb[1]), int(rgb[2])))
       #将rgb转化为像素
im.show()


a = "1+2+3"
b = a.split("+")
print(b)

得到：['1', '2', '3']
```

flag在图片里。

misc 进制转换

下载一个zip，查看文件，里边有text.txt，所以把zip后缀改为zip，解压得到text.txt

text.txt里有各种进制，我们写脚本跑一下。

```
a = "d87 x65 x6c x63 o157 d109 o145 b100000 d116 b1101111 o40 x6b b1100101 b1101100 o141 d105 x62 d101
b1101001 d46 o40 d71 x69 d118 x65 x20 b1111001 o157 b1110101 d32 o141 d32 d102 o154 x61 x67 b100000 o141
d115 b100000 b1100001 d32 x67 o151 x66 d116 b101110 b100000 d32 d102 d108 d97 o147 d123 x31 b1100101 b110100
d98 d102 b111000 d49 b1100001 d54 b110011 x39 o64 o144 o145 d53 x61 b1100010 b1100011 o60 d48 o65 b1100001
x63 b110110 d101 o63 b111001 d97 d51 o70 d55 b1100010 d125 x20 b101110 x20 b1001000 d97 d118 o145 x20 d97
o40 d103 d111 d111 x64 d32 o164 b1101001 x6d o145 x7e"
b = a.split(" ")
answer = ""
for i in b:
    if i[0] == 'b':
        answer += chr(int(i[1:], 2))
    if i[0] == 'o':
        answer += chr(int(i[1:], 8))
    if i[0] == 'd':
        answer += chr(int(i[1:]))
    if i[0] == 'x':
        answer += chr(int(i[1:], 16))
print(answer)
```

得到flag。

转载于:https://www.cnblogs.com/whitehawk/p/9928347.html