Some writeup

原创

ByNotD0g 已于 2022-01-23 01:19:25 修改 167 收藏

分类专栏： 笔记

于 2020-08-31 12:31:13 首次发布

强网杯部分wp

1.funhash

套娃

```php
<?php
include 'conn.php';
highlight_file("index.php");
//level 1
if (($_GET["hash1"] != hash("md4", $_GET["hash1"]))
{
        die('level 1 failed');
}

//level 2
if($_GET['hash2'] === $_GET['hash3'] || md5($_GET['hash2']) !== md5($_GET['hash3']))
{
        die('level 2 failed');
}

//level 3
$query = "SELECT * FROM flag WHERE password = '" . md5($_GET["hash4"],true) . "'";
$result = $mysqli->query($query);
$row = $result->fetch_assoc();
var_dump($row);
$result->free();
$mysqli->close();


?>
```

level 1 failed

第一层涉及MD4，之前没见过

可以用MD4(0e001233333333333334557778889)=0e251288019

绕过

第二层白给，用数组

第三层md5(xxx,true)后会返回原始二进制字符串

'ffifdyop'字符串对应的16位原始二进制的字符串就是" 'or'6\xc9]\x99\xe9!r,\xf9\xedb\x1c

带入后相当于'or true

原理是

> or' 对应的16进制是 276f7227 ，所以我们的目标就是要找一个字符串取32位16进制的md5值里带有276f7227这个字段的，接着就是要看关键的数字部分了，在276f7227这个字段后面紧跟一个数字，除了0，1-9，对应的asc码值是49-57，转化为16进制就是31-39，也就是我们需要有276f7227+（31-39）这个字段，就可以满足要求

2.upload
wireshark分析数据包，发现传了一张图片上去
把图片对应的原始文件保存下来
图片名称得到提示用到steghide，但没有密码，需要爆破
网上找了一个爆破脚本

```
#bruteStegHide.sh
#!/bin/bash

for line in `cat $2`;do
    steghide extract -sf $1 -p $line > /dev/null 2>&1
    if [[ $? -eq 0 ]];then
        echo 'password is: '$line
        exit
    fi
done
```

原文地址，脚本用法
https://blog.csdn.net/Blood_Seeker/article/details/81837571

buuoj

1.ping ping ping
做烂了的题，注意涉及命令执行时空格被过滤可以用IFS1等形式代替空格
通过`a=g;fla $a.php`的形式绕过对flag的过滤

2.include
说到include想到php input和filter
而且提示了file=flag.php
据说php input不行，我直接用的filter得出flag
file=php://filter/read=convert.encode/resource=flag.php

3.枯燥的抽奖
看wp才会的，考的是用php伪随机生成的种子，要使用php_mt_seed工具爆破
但需要先将伪随机数转化为php-mt-seed可以识别的内容

```
str1='abcdefghijklmnopqrstuvwxyz0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZ'
str2=......
str3 = str1[::-1]
length = len(str2)
res=''
for i in range(len(str2)):
    for j in range(len(str1)):
        if str2[i] == str1[j]:
            res+=str(j)+' '+str(j)+' '+'0'+' '+str(len(str1)-1)+' '
            break
print(res)
```

然后得到数据放入php-mt-seed得到种子，放入相同的php代码里求出密钥即可
参考大佬的博客