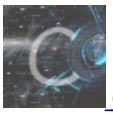
BugkuCTF - 练习平台 - 代码审计——Writeup

原创

@北陌 于 2019-02-15 21:11:20 发布 423 收藏

分类专栏： CTF

本文链接：https://blog.csdn.net/weixin_43921596/article/details/87388168



1.extract变量覆盖

extract变量覆盖

50

http://123.206.87.240:9009/1.php

```
<?php
$flag='xxx';
extract($_GET);
if(isset($shiyan))
{
$content=trim(file_get_contents($flag));
if($shiyan==$content)
{
echo'flag{xxx}';
}
else
{
echo'Oh.no';
}
}
?>
```


白话代码：
一个名叫flag的变量等于'xxx'
将通过GET传过来的数组转为一个名为数组名，值为数组值的变量(如果新的变量和已有变量重名，会将已有变量替换)
如果存在一个名叫shiyan的字符串
将flag变量的值赋给名为content变量
如果变量shiyan和变量content的值相同，
就输出flag的值
否则就输出Oh,no
因为extract()会把符号表中已存在的变量名的值替换掉，所以制造Payload: `shiyan=&flag=`
也就是利用新传入的值为空的flag替换原有的flag的值。构造空等于空，成功输出flag的值

转自——爱吃鱼L
原文：https://blog.csdn.net/qq_40980391/article/details/80097596

2.strcmp比较字符串

数组绕过，构造payload `a[]=`

3.md5()函数

数组绕过，构造payload `username[]=1&password[]=2`

4.数组返回NULL绕过

数组绕过，构造payload `password[]=`

5.弱类型整数大小比较绕过

数组绕过，构造payload `password[]=`

6.sha()函数比较绕过

数组绕过，构造payload `name[]=1&password[]=2`

7.md5加密相等绕过

百度QNKCDZO的MD5，构造payload `a=240610708`

8.strpos数组绕过

数组绕过，构造payload `ctf[]=`