XMAN2017选拔赛Web-variacover

原创

H1F 于 2017-07-16 16:25:41 发布 1584 收藏 1

分类专栏： CTF-Web 文章标签： php ctf

本文链接：https://blog.csdn.net/hyrzhrc/article/details/75207807

XMAN2017选拔赛

题目地址

```php
<meta charset="utf-8">
<?php
error_reporting(0);
if (empty($_GET['b'])) {
    show_source(__FILE__);
    die();
}else{
    include('flag.php');
$a = "www.XMAN.com";
$b = $_GET['b'];
@parse_str($b);
if ($a[0] != 'QNKCDZO' && md5($a[0]) == md5('QNKCDZO')) {
    echo $flag;
}else{
exit('你的答案不对0.0');
}
}
?>
```

由于PHP在处理哈希字符串时，会利用"!="或"=="来对哈希值进行比较，它把每一个以"0E"开头的哈希值都解释为0，所以如果两个不同的密码经过哈希以后，其哈希值都是以"0E"开头的，那么PHP将会认为他们相同，都是0。

而

```
md5(QNKCDZO)->0e830400451993494058024219903391
```

通过百度得到常见payload

将b的值设为a[0]=s878926199a

通过访问以下网址get flag

http://challenges.xctf.org.cn:7771/?b=a[0]=s878926199a