

后台登陆(实验吧) Write_up

原创

[太阳已经起床了](#) 于 2019-04-08 16:24:29 发布 5729 收藏

分类专栏: [web](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/qq_42105549/article/details/89094473

版权



[web](#) 专栏收录该内容

0 篇文章 0 订阅

订阅专栏

后台登录

格式: flag:{xxx}

解题链接: <http://ctf5.shiyanbar.com/web/houtai/ffidyop.php>

打开链接, 如下:

请用管理员密码进行登录~~

密码:

密码错误!

https://blog.csdn.net/qq_42105549

打开源代码:

```
密码错误! </div>
<!-- $password=$_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!';
    } -->
```

https://blog.csdn.net/qq_42105549

其中最重要的一句就是:

```
sql = "SELECT * FROM admin WHERE username = 'admin' and password = '".md5(password,true)."'";
```

首先解释一下md5这个函数:

语法

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

参数	描述
<i>string</i>	必需。规定要计算的字符串。
<i>raw</i>	可选。规定十六进制或二进制输出格式: <ul style="list-style-type: none">● TRUE - 原始 16 字符二进制格式● FALSE - 默认。32 字符十六进制数

https://blog.csdn.net/qq_42105549

这里的参数为TRUE,大致意思就是对你输入的密码进行32位md5加密后,再进行十六进制和字符串之间的转化。

实例化:

5d41402abc4b2a76b9719d911017c592

]A@* K*v q

F:\wampserve\www\1.php - Notepad++

文件(F) 编辑(E) 搜索(S) 视图(V) 编码(N) 语言(L) 设置(S)



汉化启动.bat x start.bat x 1.php x 1.php x

```
1 <?php
2 $str = "hello";
3 echo md5($str,false);
4 echo '<br>';
5 echo md5($str,true);
6 ?>
```

https://blog.csdn.net/qq_42105549

这道题的思路应该是构造一个 'or'xxx' 的密码，只要后面的字符串为真即可。那么可以根据32位16进制的字符串来查找'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，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，也就是含有276f7227+（31-39）这个字段，就可以满足要求。

比如说：276f722736c95d99e921722cf9ed621c正是fffdyop的md5转义。但是这个fffdyop又是怎么出来的？

其实就是最开始打开那个php链接的名字。（这种谜底就在谜面上的题真的很烦人有趣）

看了很多评论，好像e58也可以，试了一下，，是真的。

e58经过MD5函数后输出为：ïc±R%'-)è5m©，估计是 xxx'-'xxx 的形式，然后让password变为一个可以查询到密码。