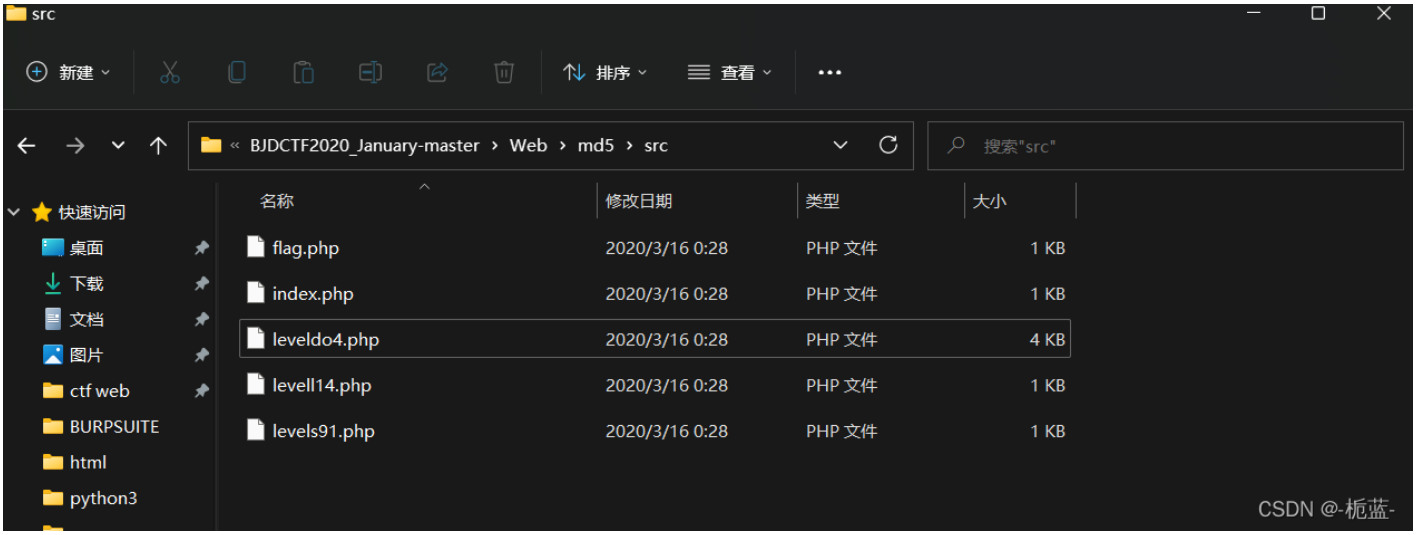
BUUCTF Easy MD5

原创

-栀蓝- 已于 2022-02-28 20:39:54 修改 2488 收藏
文章标签： php 开发语言 后端
于 2022-02-28 20:11:12 首次发布
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_54929891/article/details/123172635
版权

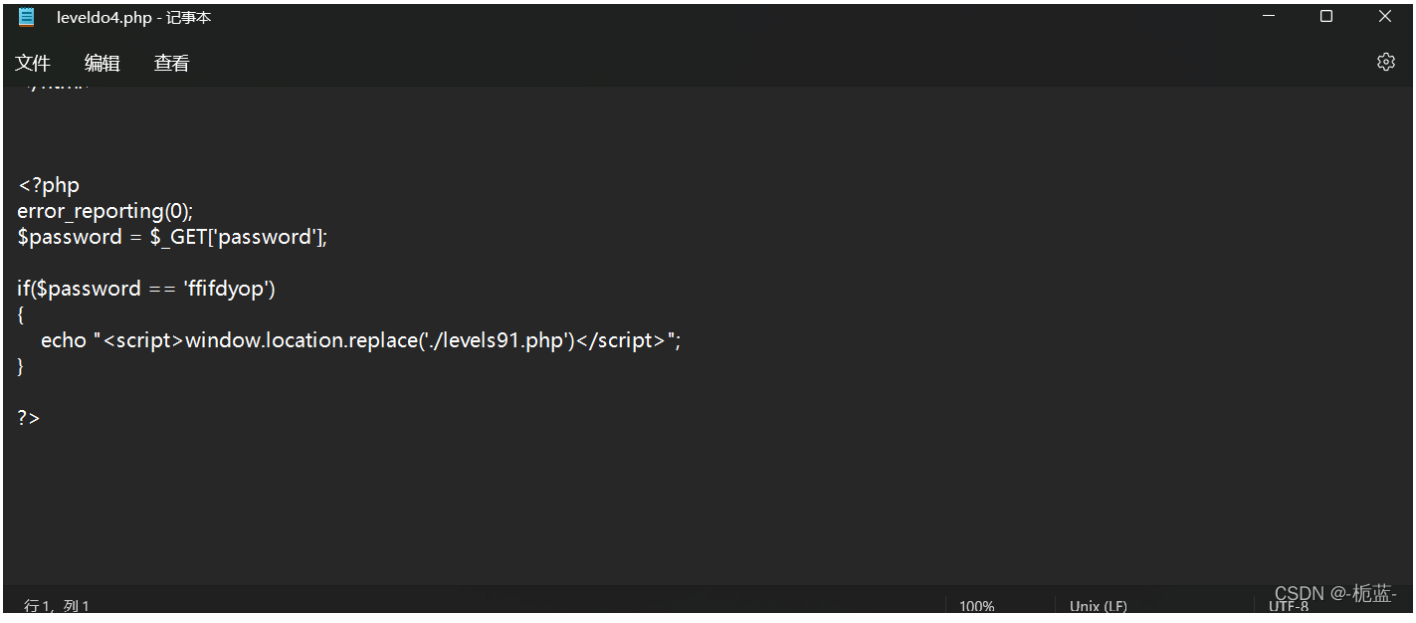
先把提示的文档下载下来，可以发现md5里面的几个php文件



既然提示是MD5，我就没往sql注入方向想，在F12下找下有没有可利用的线索

没有什么注释可以让我们知道要输入什么

既然是leveldo4.php页面，那我们便打开一下给我们的源代码看看



可以看到GET方法传入一个参数给password，如果这个参数等于ffifdyop，则跳到levels91.php页面，输入正确的密码后

可以发现levels91.php这个界面的注释里面有一段代码（我们也可以看一下这个页面的源码）

可以知道知道用用GET方法传入a，b不同的值但md5加密后却相同的值，如果条件匹配成功则跳到level14.php页面，考的是md5的弱比较md5、sha1弱比较，md5($pass,true)总结 - 87x00 - 博客园

这里跟字符串和数字弱比较类似，如“123”==“123qwer”，答案是True，因为字符串与数字比较时，会将字符串转换为数字，则123qwer会转化为123；但是开头不是数字的话"qwe123"，则会转化为0.

MD5也有一些特殊情况，一些字符串进行md5加密后会转化为同一个格式0e……，从而会会识别为科学计数法都为0，从而通过条件

a=QNKCDZO,加密后为0e830400451993494058024219903391

b=240610708,加密后为0e462097431906509019562988736854

所以既满足了a!=b，也满足了md5($a) == md5($b)

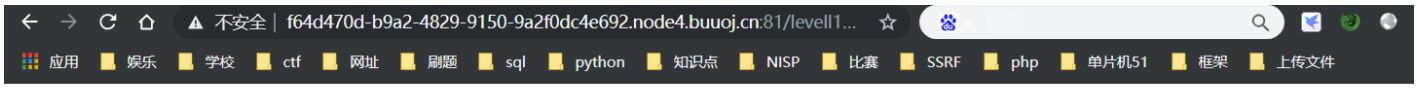
这里附上常见的0E开头的MD5

0e开头的md5和原值：

```
QNKCDZO
0e830400451993494058024219903391
240610708
0e462097431906509019562988736854
s1091221200a
0e940624217856561557816327384675
s1836677006a
0e481036490867661113260034900752
s532378020a
0e220463095855511507588041205815
s1665632922a
0e731198061491163073197128363787
s1184209335a
0e072485820392773389523109082030
s1885207154a
0e509367213418206700842008763514
s155964671a
0e342768416822451524974117254469
s1502113478a
0e861580163291561247404381396064
s214587387a
0e848240448830537924465865611904
s878926199a
0e545993274517709034328855841020
```

CSDN @-栀蓝-

还有一种情况是md5是不能加密数组的，如果你传入a[0]=1&b[0]=3,都会返回False从而相等，因此两种方法我们都可以选择



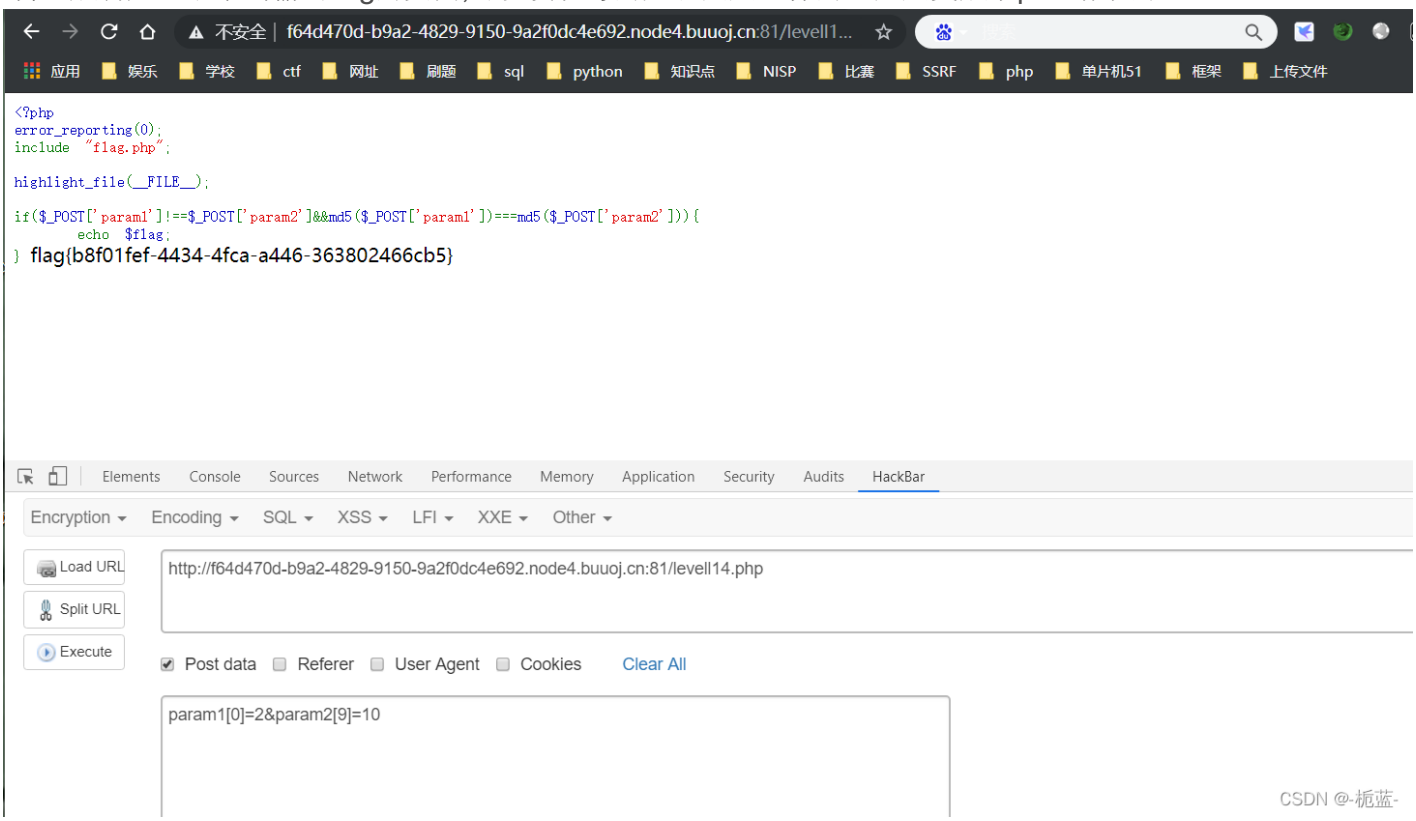

```php
<?php
error_reporting(0);
include "flag.php";

highlight_file(__FILE__);

if($_POST['param1']!==$_POST['param2']&&md5($_POST['param1'])===md5($_POST['param2'])){
        echo $flag;
}
```

CSDN @-栀蓝-

传入成功后终于来到输出flag的页面,可以发现考的知识点是一样的，只是变成了post请求而已



其实最快来到此页面的方法是，前面的源码告诉了你完成if语句就可以跳转页面，既然你知道了会跳转到哪个页面，我们可以无视那个if语句直接改url页面即可，也算一个快的方法吧