/\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*/

/\* 程序作者：爱的伊苏 \*/

/\* 程序完成时间：2019/1/20 \*/

/\* 有任何问题请联系：740531307@qq.com \*/

/\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*/

//@永远得意的笑下去

<!-- $password=$\_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!';  
} -->

根据输入密码和原有sql的拼接实行sql语句查询

可知是绕过检测并构造语句将password找出来

直接从网上寻找寻找到一个md5加密后以16字符二进制输出恰为' 'or ' 6'

Ffifdyop

276f722736c95d99e921722cf9ed621c

' ' 'or' 6<trach>

or 后面有6，非零值即为真。既可以成功绕过。

题目虽然简单，但是绕过还需要积累过程