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

/\* 程序作者：爱的伊苏 \*/

/\* 程序完成时间：2019/1/10 \*/

/\* 有任何问题请联系：740531307@qq.com \*/

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

//@永远得意的笑下去

首先拿到题目以后查看网页源代码

$test=$\_GET['username']; $test=md5($test); if($test=='0')

发现如下图的注释，显然是给我们提示用的

将username进行md5加密，若加密后数值为0，而运行某些操作。

那么我们第一步先构造密文为零的md5构造方式

240610708就是其中一种形式

输入后出现 /user.php?fame=hjkleffifer

我们进入地址后发现

$unserialize\_str = $\_POST['password'];

$data\_unserialize = unserialize($unserialize\_str);

if($data\_unserialize['user'] == '???' && $data\_unserialize['pass']=='???')

{ print\_r($flag); }

伟大的科学家php方言道：成也布尔，败也布尔。 回去吧骚年

可知将password反序列化之后会出现’user’ ‘pass’两个变量二者同时判断相等时可以输出flag

这是伟大的php说： 布尔！

这是我们知道bool类型的true与任意字符串可以满足弱类型相等，于是构造password变量

a:2:{s:4:"user";b:1;s:4:"pass";b:1;}