实验吧天网管理系统Writeup

原创

Mars_guest 于 2018-05-01 18:25:49 发布 1432 收藏

分类专栏： CTF_Writeup 文章标签： Writeup ctf

本文链接：https://blog.csdn.net/Mars_guest/article/details/80158050

实验吧天网管理系统Writeup

原题地址 实验吧–天网管理系统

用到的知识点：

1.php弱类型相等

2.php函数serialize()与unserialize()（序列化和反序列化）

首先查看源文件，发现提示：

```
<!-- $test=$_GET['username']; $test=md5($test);
if($test=='0') -->
```

意思就是将输入的username的值进行md5加密，之后与0相等即可
php中==是只进行值的比较，不管二者的类型。当两个字符串进行==比较的时候，则比较字符串中第一个不是数字的字符之前的数字串所代表的整数值，例如"0marsguest"与"0"就是相等的。
那么下面的主要任务就是找到md5加密后是0的值，这样的例子有很多，参考链接：http://marsguest.com/2018/05/01/2018-05-01-md5-0/
我这里用的是240610708，将用户名输入240610708，得到提示：

访问这个界面。得到新的提示：

```
$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
```

简单审计一下，大意就是将password的值进行**反序列化**，之后得到的是一个数组，数组中user和pass的值都等于一个东西，但是具体是什么并未给出。

关于序列化和反序列化

大致意思实例化的对象经过序列化**serialize()** 转成一个连续的字符串，将这个字符串再进行反序列化即可得到原本的对象，下面的解释直接上代码

```php
<?php
    class student{
        var $name;
        var $num;
        var $age;
        function student($name="null",$num="null",$age=0){
            $this->name = $name;
            $this->age = $age;
            $this->num = $num;
        }
        function getname(){
            return ($this->name);
        }
    }
    $student1 = new student("marsguest","2016201601",20);//实例化一个对象
    $serStu = serialize($student1);
    echo $serStu;
?>
```

最终打印出的数据：

```
O:7:"student":3:{s:4:"name";s:9:"marsguest";s:3:"num";s:10:"2016201601";
s:3:"age";i:20;}
```

O表示object， s表示string， i 表示int， 数字表示对应字段的长度.
（还有b表示bool，a表示array，后面会用到）
注意： 布尔和整型数不用写长度，直接跟值即可
下面我们将$serStu反序列化；

```php
    unset($student1);//释放student1这个对象
    $newStu = unserialize($serStu);
    echo $newStu->getname();
```

成功打印出student1的名字`marsguest`

---

ok，言归正传，我们最后是要构造password，这个password经过反序列化后是存有user和pass两个键的数组，之后将user和pass对应的值与一个东西相等，这里还有一个重要提示`伟大的科学家php方言道：成也布尔，败也布尔。回去吧骚年` bool类型的true跟任意字符串可以弱类型相等，于是构造password

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

成功拿到flag