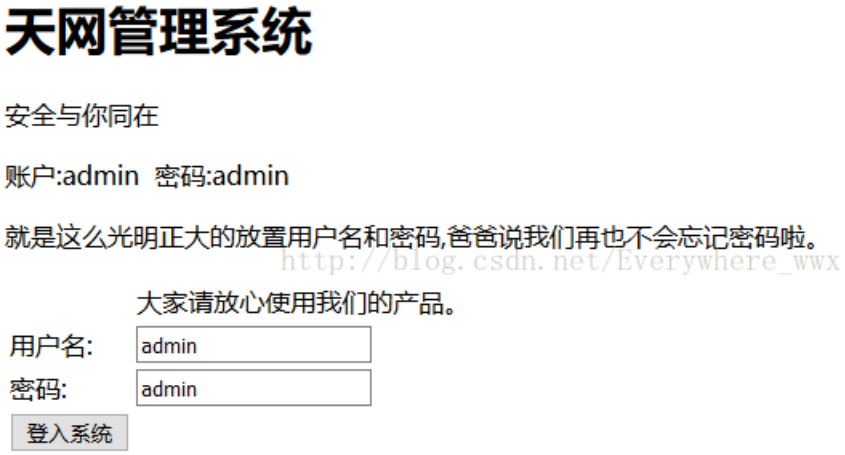
CTF 实验吧 天网管理系统

原创

Flemington、 于 2017-10-18 16:17:40 发布 4127 收藏
分类专栏： web 文章标签： CTF web php



1.

点击登入系统，并没有反应

2.直接F12 查看源码

3.发现异常 有一段代码：<!-- $test=$_GET['username']; $test=md5($test); if($test=='0') -->

要求用户名传入一个字符串，经过md5加密后要等于0。

md5加密自行百度就可得知

4.插播一段有关于 PHP弱类型的相关知识

在php中

==： 比较运算符号 不会检查条件式的表达式的类型

===: 恒等计算符，同时检查表达式的值与类型。（会检查表达式类型，如bool）

比如：

*** 当php进行一些数学计算的时候，当有一个对比参数是整数的时候,会把另外一个参数强制转换为整数。**

```
1 var_dump(0 == '0'); // true
2 var_dump(0 == 'abcdefg'); // true 3 var_dump(0 === 'abcdefg'); // false 4 var_dump(1 == '1abcdef'); //
true
```

*** bool类型的true跟任意字符串可以弱类型相等**

PHP会把类数值数据（如含有数字的字符串等）转换成数值处理，== 运算符就是其中之一。

在使用 == 运算符对两个字符串进行松散比较时，PHP会把类数值的字符串转换为数值进行比较，

如果参数是字符串，则返回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。比如: '3' == '3ascasd'结果为true。

因此只要找到一个字串加密后第一个字符为0即可，这里提供几个：240610708，aabC9RqS 可以验证

5.username=240610708

可得到提示 /user.php?fame=hjkleffifer

6.访问可得到 ctf5.shiyanbar.com/10/web1/user.php?fame=hjkleffifer

$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

理解这段代码：

7.插播关于php 序列化与反序列化
serialize（） 对输入的数据进行序列化转换
unserialize() 恢复原先变量，还原已经序列化的对象。

8.题目意思就是post提交的password值经过"反序列化"得到一个数组，要求数组里的user和pass都等于某个值时就打印flag。

9.php代码：

```
<?php
$test3=array('user'=>true,'pass'=>true);
$disc3=serialize($test3);
var_dump($disc3);
?>
```

string(36) "a:2:{s:4:"user";b:1;s:4:"pass";b:1;}"

或者通过构造：借一句话 成也bool 败也bool **bool类型的true跟任意字符串可以弱类型相等。可以构造bool类型的序列化数据**，无论比较的值是什么，结果都为**true。（a代表array，s代表string，b代表bool，而数字代表个数/长度）**

10.得到password:

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

11.输入：得到flag:ctf{dwduwkhduw5465}