# 实验吧WEBWP(一）

原创

Neil-Yale 于 2017-03-19 22:36:05 发布 2580 收藏

文章标签： 源码 WEB CTF



本文链接：https://blog.csdn.net/yalecaltech/article/details/63750661

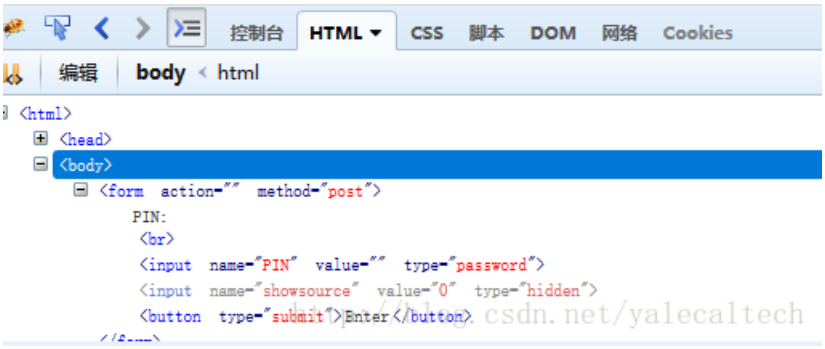


1.Forms（链接：http://www.shiyanbar.com/ctf/1819）

页面很干净，第一反应查看源码

在此之前，我们先随便输入然后点击enter，没什么线索

源码中我们看到value=0




将value改为1，再随便输入然后点击enter

```
$a = $_POST["PIN"];
if ($a == -19827747736161128312837161661727773716166727272616149001823847) {
    echo "Congratulations! The flag is $flag";
} else {
    echo "User with provided PIN not found.";
}
```

User with provided PIN not found.
PIN:
Enter



毫无疑问，输入的内容就应该是a的值

得到flag

2.天网管理系统(http://www.shiyanbar.com/ctf/1810)

思路：

第一步看源码，

意思是Php将username哈希以后与0比较，即'0exxxxxxxx'类似这样的哈希值会相等（弱相等），因为字符串和数字比字符串会转变成数字比较，即0e100相当于0的100次方

于是百度一下0e开头的md5哈希字符串，如下：

QNKCDZO(0e830400451993494058024219903391)
s878926199a(0e545993274517709034328855841020)
s155964671a(0e342768416822451524974117254469)
s214587387a(0e848240448830537924465865611904)
随便挑一个填在用户名中
密码使用admin
提交后得到路径/user.php?fame=hjkleffifer
打开指向的url的网页，查看源码得到
*unserialize* _POST[‘password’];

代码意思是把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都满足，就打印flag
我们不知到???是什么，但是我们注意到信息中判断条件使用的为==（php弱类型）

bool类型的true跟任意字符串可以弱类型相等的，当代码中存在unserialize或者json_decode的时候，我们可以构造bool类型，来达到欺骗。
现在我们构造一个数组，元素分别是user和pass，都是bool类型的true，于是我们得到
a:2:{s:4:”user”;b:1;s:4:”pass”;b:1;}（a代表array，s代表string，b代表bool，而数字代表个数/长度）
意思是数组a中有两个元素，长度为4的user元素的bool值为1，长度为4的pass元素的bool值为1.
这样，经过反序列化后的user以及pass都是1，满足if语句，则会print出flag

然后就有了两种答案（其实本质上是一种答案）
（1）用户名：admin
密码：a:2:{s:4:”user”;b:1;s:4:”pass”;b:1;}
（2）用户名：
QNKCDZO(0e830400451993494058024219903391)
s878926199a(0e545993274517709034328855841020)
s155964671a(0e342768416822451524974117254469)
s214587387a(0e848240448830537924465865611904)
MD前字符串四个中的一个
密码：a:2:{s:4:”user”;b:1;s:4:”pass”;b:1;}