bugku writeup 前女友/login1

原创

Ares-T 于 2018-04-02 16:37:05 发布 1903 收藏
分类专栏： CTF 文章标签： writeup

知识点：md5函数数据类型错误返回false（两个md5都返回false时相等），strcmp函数比较i出错返回0（与相等返回一样），sql约束攻击：sql会自动填充空格达到相同长度后再进行比较，sql会截取前n个字符直接进行比较

前女友：

http://118.89.219.210:49162/

flag格式：SKCTF{xxxxxxxxxxxxxxxx}

打开网址后发现是一大段文字

查看源码发现第21行处有一个链接

```
<p>"帮我看看这个..."说着，她发来一个<a class="link" href="code.txt" target="_blank">链接</a>
```

打开链接发现源码，长亭一位大神说过，一个页面如果只有文字的话那么极有可能找到源码。

源码如下：

```
<?php
if(isset($_GET['v1']) && isset($_GET['v2']) && isset($_GET['v3'])){
    $v1 = $_GET['v1'];
    $v2 = $_GET['v2'];
    $v3 = $_GET['v3'];
    if($v1 != $v2 && md5($v1) == md5($v2)){
        if(!strcmp($v3, $flag)){
            echo $flag;
        }
    }
}
?>
```

我们需要构造三个参数，v1，v2，v3，其中v1和v2需要值不同但md5的值相同，看起来是找md5碰撞的问题，但是问题却不在这里，利用md5函数的特性，如果使用一个不可md5的数据类型传入的话那么md5函数将返回false，这个也是返回值，题目要求的是md5函数的返回值相等，所以就可以用两个值不同但不可md5的数据类型传入即可。此处我们使用v1[]=1&&v2[]=2。第二个是strcmp函数，需要v3和flag的值相同才返回flag的值，貌似是一个鸡生蛋问题，但是我们依旧使用函数特性，strcmp函数如果出错，那么它的返回值也会是0，和字符串相等时返回值一致。那么如何出错呢，猜测不可比较时出错，那么传入一个数组试试，所以最后构造参数并用get方法传入，http://118.89.219.210:49162/?v1[]=1&&v2[]=2&&v3[]=3，得到flag。

login1

http://118.89.219.210:49163/

flag格式：SKCTF{xxxxxxxxxxxxxxxx}

hint:SQL约束攻击

打开后是一个管理系统，对于一个管理系统我们的目标总是要得到admin账户的权限，根据提示，我们先看看sql约束攻击时什么。有两个关键的知识点，转至博客：https://blog.csdn.net/wy_97/article/details/77972375，更多内容可查看这篇博客，写得挺详细的。

> 在SQL中执行字符串处理时，字符串末尾的空格符将会被删除。换句话说“vampire”等同于“vampire ”，对于绝大多数情况来说都是成立的（诸如WHERE子句中的字符串或INSERT语句中的字符串）例如以下语句的查询结果，与使用用户名“vampire”进行查询时的结果是一样的。

```
SELECT * FROM users WHERE username='vampire     ';
```

> 但也存在异常情况，最好的例子就是LIKE子句了。注意，对尾部空白符的这种修剪操作，主要是在“字符串比较”期间进行的。这是因为，SQL会在内部使用空格来填充字符串，以便在比较之前使其它们的长度保持一致。
>
> 在所有的INSERT查询中，SQL都会根据varchar(n)来限制字符串的最大长度。也就是说，如果字符串的长度大于“n”个字符的话，那么仅使用字符串的前“n”个字符。比如特定列的长度约束为“5”个字符，那么在插入字符串“vampire”时，实际上只能插入字符串的前5个字符，即“vampi”。

有了以上知识点，我们可以大胆地开始尝试了，我们需要做的就是注册一个在数据库中会被认为是admin的账户，然后使用这个admin账户登录。构造用户名“admin 1”尽可能长的空格，然后设置一个密码就好了。然后用这个账户登陆进去就可以得到flag了。