Tamevic's Ctf-Web writeup@实验吧‘FALSE’

原创

TameVic 于 2019-04-13 09:12:57 发布 120 收藏

分类专栏： web 文章标签： ctf web

本文链接：https://blog.csdn.net/qq_43264421/article/details/89277652

Tamevic’s Ctf-Web writeup@实验吧‘FALSE’

> 密码学刚刚开课就搞到了这个…

url： http://ctf5.shiyanbar.com/web/false.php

分析

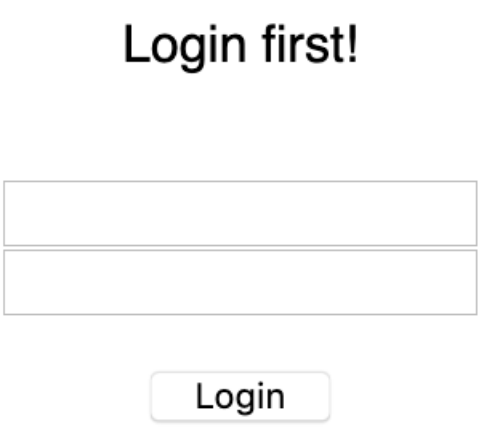
FALSE 分值：10

来源： iFurySt 难度：易 参与人数：8975人 Get Flag：4801人 答题人数：4850人 解题通过率：99%

PHP代码审计
hint：sha1函数你有认真了解过吗？听说也有人用md5碰撞o(╯□╰)o
格式：CTF{}

解题链接： http://ctf5.shiyanbar.com/web/false.php **通过**

点开url看到是个登录窗口



先不管他，先看源码

```
&lt?php
if (isset($_GET['name']) and isset($_GET['password'])) {
    if ($_GET['name'] == $_GET['password'])
        echo '<p>Your password can not be your name!</p>';
    else if (sha1($_GET['name']) === sha1($_GET['password']))
      die('Flag: '.$flag);
    else
        echo '<p>Invalid password.</p>';
}
else{
 echo '<p>Login first!</p>';
?&gt;
```

这一段是key code，我们来仔细分析一下。对于用户名和密码的第一个要求是"Your password can not be your name!"，第二个要求是用户名和密码的SHA1散列值要相同。第一个比较容易干到，但是第二个就有点难了。虽然很多大牛在尝试SHA1碰撞但是我也不会啊。

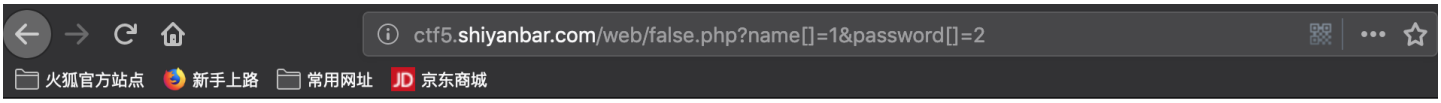
这里就利用到SHA1()函数的漏洞

SHA1()函数能对字符串类型的文本进行散列，但是对其他类型却不能执行前，都会返回NULL或是FALSE（不管是啥反正是一样的东西），这样就达到了我们想要的效果。这里我们用数组来进行绕过！

```
name[]=1&password[]=2
```

结果

进行提交，得到结果



Flag: CTF{t3st_th3_Sha1}


```
Flag: CTF{t3st_th3_Sha1}
```

End

积累绕过姿势中…