实验吧——WEB-FALSE

原创

小白白@ 于 2019-04-12 15:47:09 发布

分类专栏： CTF 代码审计

本文链接：https://blog.csdn.net/weixin_44677409/article/details/89242438

 CTF 同时被 2 个专栏收录

23 篇文章 2 订阅

订阅专栏

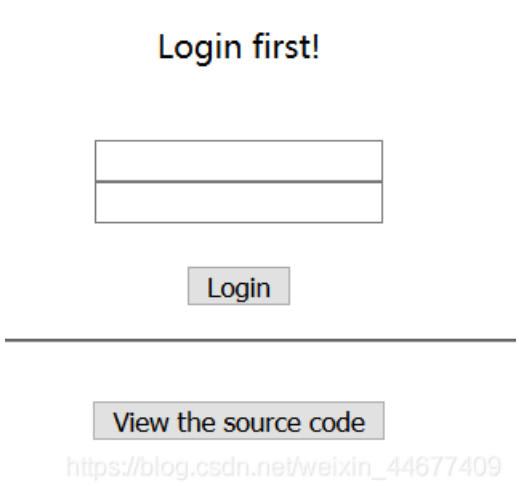
 代码审计

5 篇文章 0 订阅

订阅专栏

FALSE

```
hint: sha1函数你有认真了解过吗？听说也有人用md5碰撞o(ﾉ □ ╰)o
```



查看源码

```php
<?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>';
?>
```

发现只要满足两个条件：

1. name和password值不能相等
2. name和password的sha1加密的散列值相等

sha1()函数默认的传入参数类型是字符串型，当传入为数组类型时，其返回值为false。

我们可以构造payload：

```
?name[]=a&password[]=b
```

false.php?name[]=a&password[]=b

Flag: CTF{t3st_th3_Sha1}