buuctf web buyflag

原创

显哥无敌 于 2021-09-11 12:39:11 发布 62 收藏

分类专栏： BUUCTF 文章标签： web安全

本文链接：https://blog.csdn.net/qq_41696858/article/details/120236134

打开场景，查看源码，发现a链接，pay.php打开目标页面查看源码，发现提示

```
<!--
 ~~~post money and password~~~
if (isset($_POST['password'])) {
 $password = $_POST['password'];
 if (is_numeric($password)) {
  echo "password can't be number</br>";
 }elseif ($password == 404) {
  echo "Password Right!</br>";
 }
}
-->
```

页面还有提示

```
<p>If you want to buy the FLAG:</br>
You must be a student from CUIT!!!</br>
You must be answer the correct password!!!
</p>
<p>Flag need your 100000000 money</p>
```

不明所以，抓个包看看

抓到cookie里有user=0，结合You must be a student from CUIT!!!，把user改为1，发现有变化，you are Cuiter

那第一个条件已经满足

下面就是满足password，post一个包过去，内容password=404a，由于弱相等，Password条件也满足，只剩下最后一道关

Pay for the flag!!!hacker!!!

那结合

Flag need your 100000000 money

，盲猜需要的参数是money

money=100000000，提示Nember lenth is too long

那么考虑是strcmp来判断钱数是否够

尝试money=1e12，成功拿到flag

或者直接money[]=1，由于是非字符型，所以strcmp函数会直接返回0，而相等也返回0，成功绕过

给一个完整payload

money=1e12&password=404a

参考视频链接:https://www.bilibili.com/video/BV1HL4y1a7UQ/