攻防世界php2_攻防世界 php2 writeup

原创

weixin_39923137 于 2021-01-12 01:53:59 发布 49 收藏
文章标签： 攻防世界php2

0x00前言

讲道理真的被自己菜到了 有的东西还是需要靠练 漏洞既然一时半会找不出来那么就去做ctf 算是积累积累经验了 毕竟现在太多不知道了 只能慢慢来

0x01正文

刚刚看到题目就蒙蔽了 只有一句话 本来想着看看源代码可以发现什么但是一看还是只有这么一句话

随后我输入了 index.php 然后用了扫描器也没有发现有别的 随后去看了一下别人的write up 居然是 index.phps 长见识了 随后发现源代码泄露了 如下图

然后让我们现在来分析一下这个程序 === 不但比较数值 而且还比较数值的类型 所以如果 我们id的数值和类型等于 admin 就会显示 not allowed

== 代表着数值相等 所以我们只要数值相等 就可以获取到我们所需要的flag

但是我之前看的write up 直接给出了 答案 %2561dmin 看的我一头雾水 有可能是我对编码的不熟悉 但是按照如下表格就一下子明白了

所以这里的意思就是 %2561dmin 经过一次url解码 把%25 变成 % 然后就成为%61dmin 然后 %61 又代表a 所以就是数值相当于admin了 然后就可以 在这个界面下/index.php/?id=%2561dmin 得出flag