=。=我根本不会 CTF……

做出来的也不多。根据要求写一下 writeup。

21.这 TM 是啥

打开看了下源码，jsfuck，google 了一个 decoder，搞定。

22.我是谁我在哪？？？

进去吃个 302，抓包，在 header 发现 flag。

25.神奇的数字

php 审计。要拿到 flag，首先 number = intval(number)，其次 number = intval(strrev(number))，最后，不能是回文数。

number 和倒转后的 number 相等，想到 overflow，于是构造个 009223372036854775807，过。

26.不可能拿到的 flag

拿到 flag 的要求是 name 和 password 不相等但是 sha1()结果一样。

去看了下 sha1()的文档发现无法摘要的时候都是返回 false。于是就想都失败。

于是 name 和 password 都给个数组，这样 sha1()无法处理。

27.php 真可怕我要回农村

b 不能过 is_numberic()，但是可以和 a 做运算。

然后 b[10]是 false，于是 b 肯定是个字符串。看到==这种不严格相等，肯定是类型转换，那么 b[10]肯定是 0.

没法过 is_numberic()很简单，在字符串后面随便加点什么玩意就行。

反正我最后构造的 b 好像是”0.730000000000000000000000a”什么的。忘记了。

反正多代几个数字试试就出来了。

23.re?

反编译之。

Java 我是一点都不会。看了下大概是要求输入的 flag 经过 AES 加密和预设的相等。secret key 是从文件中读。那么修改下代码把预设的解密回去就行了。

28.你看看，逆向多简单！

是很简单，winhex 打开就有。

Explorer 的图库

这个有三个 flag 我只找到俩。

第一个很简单，在文件头就有。

第二个，随便试了下后缀，发现可以解压，于是解压出来个文本文件，里面有个 flag。

第三个。。查了很多资料。

用 binwalk 跑了下发现还藏了一张图，是个⑨……然而这张图我翻来覆去也没看出什么毛病……_(:з」∠)_

14.lightless 的渗透教室入门篇（一）

……拿 jQuery 写了个 ajax 就好了。

15.lightless 的渗透教室入门篇（二）

postman 各种魔改请求头，完成。

16.lightless 的渗透教室入门篇（三）

伪造 cookie，这个控制台两行代码就行了。