这 TM 是啥

打开网页直接看源码。发现一堆 ooxx 的东西，放在 js 区域，估计是种异形的 js，网上查找了一下，得知是 JSFuck。

没有其他线索，可能藏在里面，果断想办法翻译过来。

找了半天，“官网”www.jsfuck.com 里只有 js 翻 jsfuck，并没有翻译回来，还得自己写。懒得弄。。。。搜寻好久，辣鸡百度上啥也没有，google “from jsfuck to js”，得到好东西，国外一网站上搞过一个竞赛，看谁写的脚本翻译 jsfuck 又短又好用。。。dalao 就是 dalao。附代码：alert(/\n(.+)/.exec(eval(prompt().slice(0,-2)))[1])。

这东西要在 jsfuck.com 上 console 里用。在弹出的提示框里输入 jsfuck 能够翻译回去并以弹窗显示。但是问题就在于貌似有长度限制。后来，想到里面肯定藏着 hctf 和{}，于是先翻译了这俩然后在一长串中搜索到范围。。再恢复到原来的代码，拿到 flag。

你看看，逆向多简单！

没错，贼简单。下载文件，txt 打开。找到 flag。（我也就能做这种逆向了）

Explorer 的图库之一

第一次见过隐图还能这么玩，第一张简单的，把图 txt 打开，找到 flag。

Explorer 的图库之二

没有老司机带，感觉不可能做出来，还好百度 ctf 隐图，能找到别人的 wp。学着 binwalk 了第一张图。发现里面果然藏着东西。接着 foremost 得到 png 和 jpg。但是 png 没怎么发现东西，然后回头看了看 binwalk 结果发现还有压缩包。学了一下方法，dd 得到压缩包。

但是，打不开的 woc，好气。可能因为 dd 只是把前半部分省略了后半部分还包含着 png 所以有错误的？很绝望，辣鸡的我不知道怎么直接从中间截取的。破罐子破摔直接扔到 vim 里了。竟然就看到 flag 了？？!! 什么原理？？！

Explorer 的图库之三

根据别人的 wp 分析，可能是个 lsb 隐写，藏在 png 里。学着大佬们又是 hex 又是 steg。除了发现，哦~果然藏着东西。也没想到怎么搞到。翻阅大半天 python 和网上内容。最后终于机缘巧合网上找到一串 python，自己又完善了一下，在最低为中提出一个压缩包。但是 !! 还是打不开？？!!

然后放到 txt 里，也啥都没有，再次绝望。又回到原来的方法，dd png。得到的压缩包 of course 也不能开的。这题我就暂时扔了。。后来问学长说要我 hex 看好文件头的？（好像是这个意思）我就又都放了一遍 hex。瞟到某个压缩包的 hex 前一串字竟然不是乱码。结尾还带着等于号。好吧，可能是 base64。果然，解码得 flag。

密码学教室入门（一）

一篇百度文库的 ppt，看起来像是交作业的，但是里面的总结很实用。http://wenku.baidu.com/link?url=GfY4MOy8SCQOK-KBfC123tKj_rWtqQaQTHsNyaJhOGSUUi0RO6qyxuU_Wqe3qfqtk2mPTvC-_VgSn_6V7BOHntHUF5P6fpA55Tr_gm_TZsm

找到一个大数计算器，貌似专门为 rsa 解密而设，还专门有 x^y mod z 功能的。。。然后应该就简单了，把数放进去算就是嘞但怎么弄怎么不对劲，辣么长的结果？？!! 但是有人做出来了，没毛病。。。。

最后修复了一个 bug，d e 颠倒了。。hhh，之前的人不愧是 dalao。然后算出得到看起来就有问题的一串 16 进制。http://www.bejson.com/convert/ox2str/ 转换成字符看到 flag。

密码学教室入门（二）

凯撒密码嘛，不难，c 语言写了一个穷举的，拿到有意思的那一行。数字另外处理，得到 1。得到 flag。

密码学教室入门（四）

不难发现 e 为 1。Rsa 公式直接被简化。拿去算，比一还简单。得到一样开头的一串。当然就是 flag。转换一下，得到结果。

lightless 的渗透教室入门篇（一）

都有教程了还能说什么。虽然用不到教程。。看了看，然后打开 firefox，用 hack bar 提交 post 和 get 页面刷新出 flag。提交。