# 攻防练习之CTF

## CTF练习题1

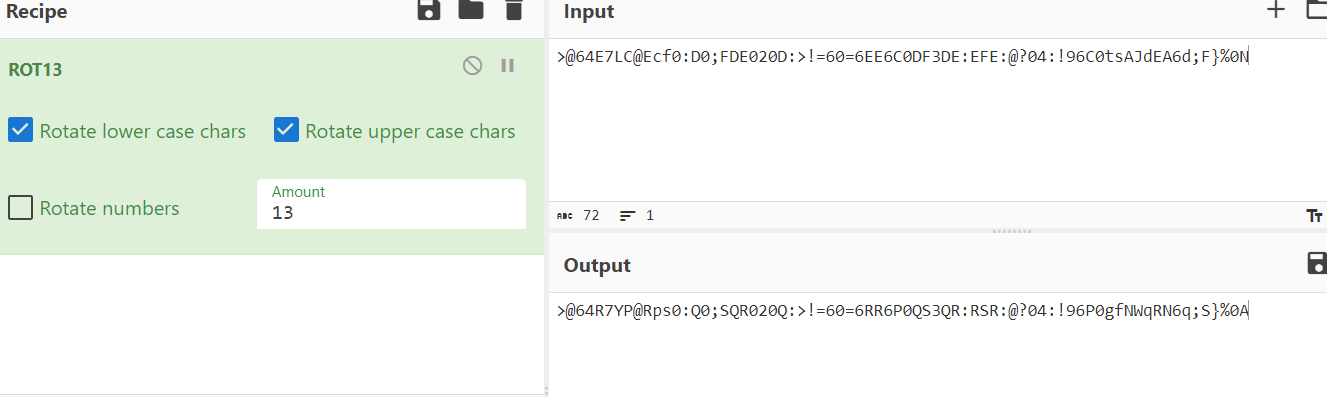
Classical Crypto——ezrot

附件中信息如下。

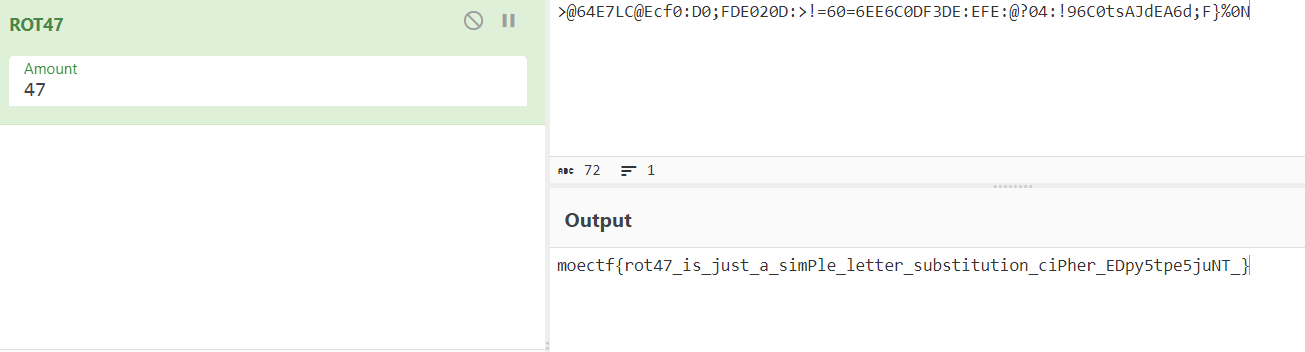
>@64E7LC@Ecf0:D0;FDE020D:>!=60=6EE6C0DF3DE:EFE:@?04:!96C0tsAJdEA6d;F}%0N

根据题目可以推测出这是一个家族编码rot

尝试rot13仍是乱码



尝试rot47，得到flag



moectf{rot47\_is\_just\_a\_simPle\_letter\_substitution\_ciPher\_EDpy5tpe5juNT\_}

## CTF练习题2

猫言喵语

文件内容如下

|  |
| --- |
| 喵喵？喵喵喵喵喵喵喵喵喵喵喵喵 喵喵喵 喵喵喵喵喵喵喵喵？喵喵？喵喵喵喵喵？喵喵？喵喵喵喵喵？喵喵喵喵喵？喵喵喵喵喵？喵喵？喵喵喵喵喵？喵喵喵喵喵喵 喵喵喵喵喵喵 喵喵喵喵喵喵喵喵？喵喵？喵喵喵喵喵？喵喵？喵喵喵喵喵？喵喵喵 喵喵喵喵喵？喵喵？喵喵喵喵喵喵喵喵？喵喵？喵喵喵喵喵？喵喵？喵喵喵喵喵喵喵喵喵 喵喵喵喵喵喵喵喵？喵喵？喵喵喵喵喵喵喵喵？喵喵？喵喵喵喵喵？喵喵？喵喵喵喵喵喵喵喵喵 喵喵喵 喵喵喵喵喵喵喵喵？喵喵？喵喵喵喵喵？喵喵？喵喵喵喵喵？喵喵喵 喵喵喵喵喵？喵喵喵喵喵？喵喵喵喵喵喵 喵喵喵喵喵？喵喵喵喵喵喵 喵喵喵 喵喵？喵喵喵喵喵喵 喵喵喵喵喵喵喵喵？喵喵？喵喵喵喵喵？喵喵？喵喵？喵喵喵 喵喵？喵喵？喵喵？喵喵喵喵喵喵喵喵？喵喵？喵喵？喵喵喵喵喵喵 喵喵喵喵喵喵 喵喵喵喵喵喵喵喵？喵喵？喵喵喵喵喵？喵喵？喵喵喵喵喵喵喵喵喵 喵喵？喵喵喵喵喵？喵喵？喵喵喵喵喵喵喵喵？喵喵？喵喵喵喵喵？喵喵喵喵喵？喵喵喵 喵喵？喵喵喵喵喵喵喵喵？ |

根据文件提示”Morse code”，是摩斯密码。众所周知。摩斯密码只有两种符号，所以得把文件内容根据特征划分成两块。内容中的空格相当于分隔符，根据观察，可以看出”喵喵？”是一组，”喵喵喵”是一组，根据这个规律进行转换，得到如下内容。

喵喵喵转化为.

喵喵？转化为-

|  |
| --- |
| **-/...././..--.-/-.-/.-/.--/.-/../../..--.-/-.-./.-/-/..--.-/-.../..-/-/..--.-/-..././..--.-/-.-./.-/.-../.-.././-../..--.-/--./---/..-/--../../..--.-/-.../-.--/..--.-/.-./-..-** |



得到结果THE\_KAWAII\_CAT\_BUT\_BE\_CALLED\_GOUZI\_BY\_RX

## CTF练习题3

图片内藏有5位数密码，你能找出来吗？

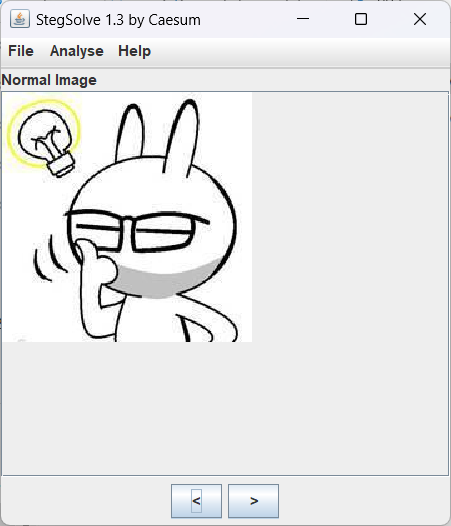
解题链接： http://ctf5-shiyanbar-com/stega/FIVE1/1111110000000000-jpg

首先把图片下载下来

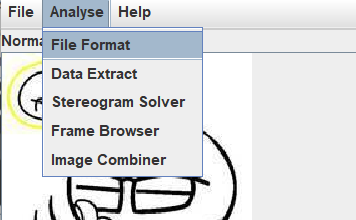


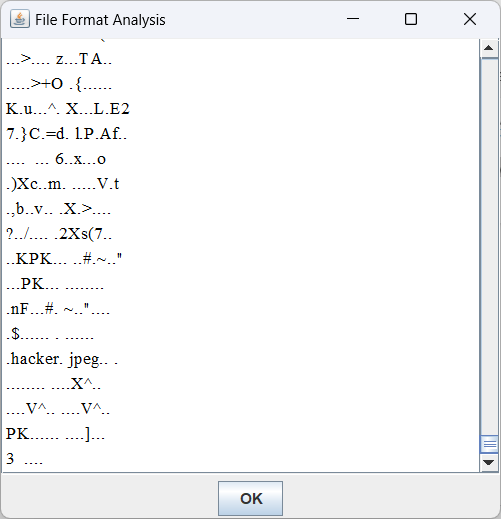
使用CTF竞赛中常用的Stegsolve进行分析

（Stegsolve是一款强大的隐写分析工具，广泛应用于网络安全和CTF(Capture The flag)竞赛中。它能够帮助用户分析和提取隐藏在图像文件中的信息-。）

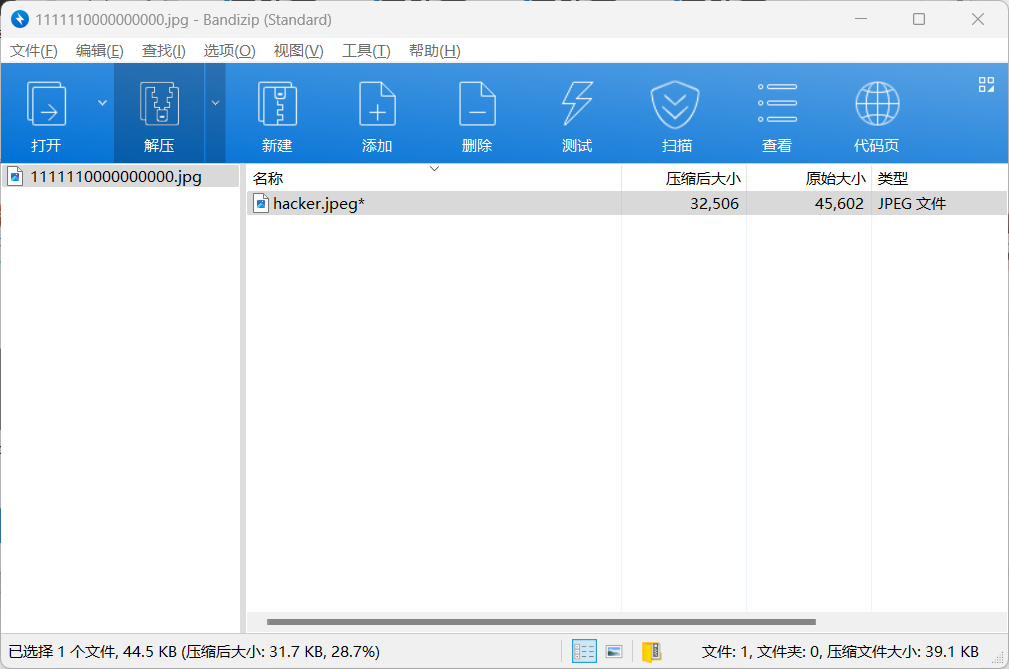


点击文件分析

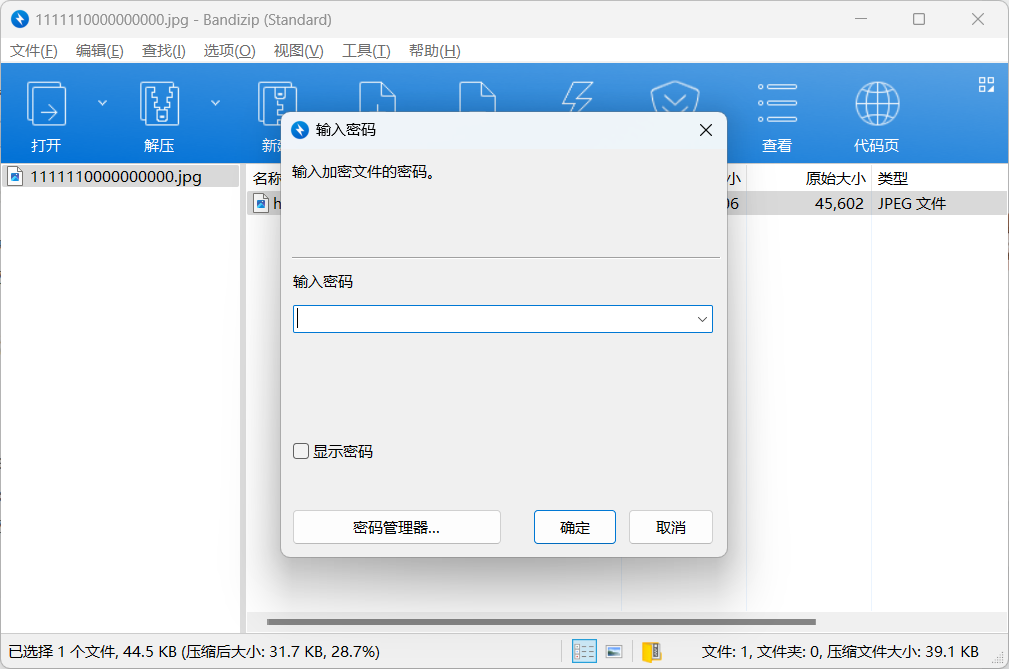


纵观组成文件的无序编码中，出现了hacker-jpeg这种文件格式，推测图片内有其他文件

用压缩包的形式打开，里面确实藏有文件

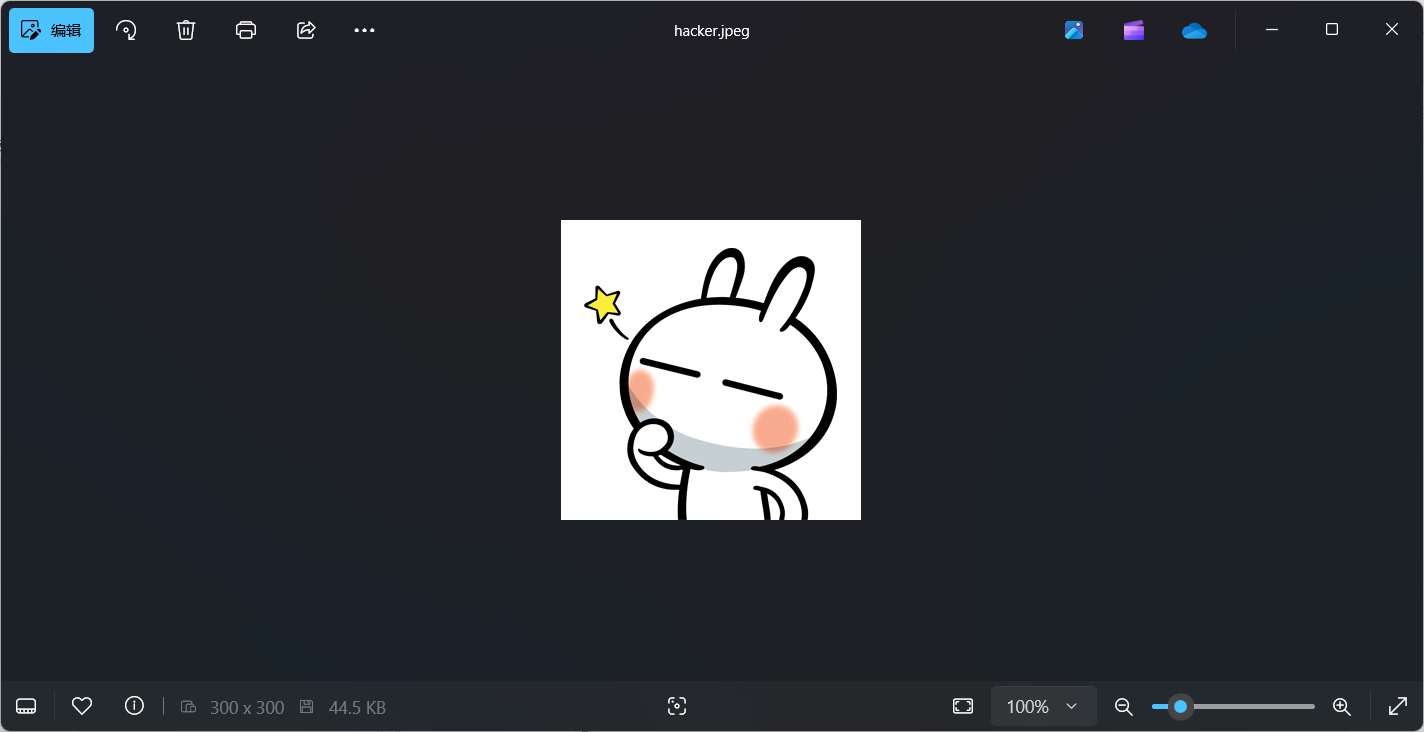


想要拿出来，发现压缩包有密码

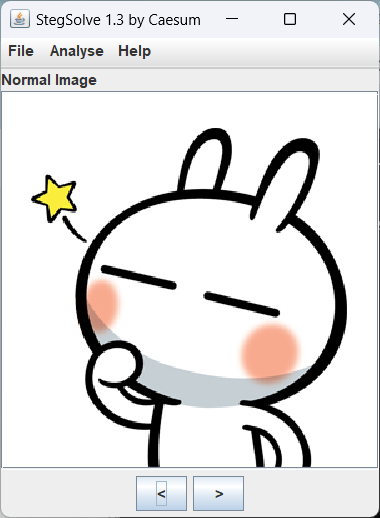


分析文件名1111110000000000，全是01，可以当成二进制，共有十六位，感觉可以用八进制十六进制换算试试，换算成16进制是fc00，果然密码正确

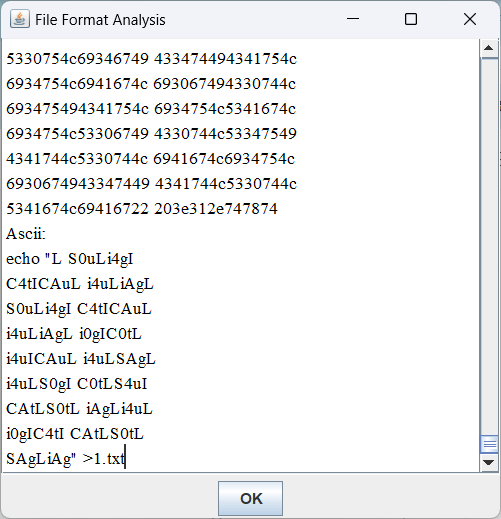
然而打开内部文件



发现并不是密码，还需要继续解题，再用Stegsolve进行分析



分析文件之后发现内部有一部分命令



Echo一下得到了一串字符

根据经验推测、这些字符极像base64编码后的密文。因此我们在http://tool-oschina-net/encrypt?type=3中粘贴这段密文并进行解密，得到了一些由‘.’和‘-’组成的字串。



得到了-和\_那就是摩斯密码

根据摩斯密码对照表我们将其进行破译，破译后得到7A57A5A743894A0E。



还是无序，这种形式和md5有些相似，解码吧！

在http://www-cmd5-com/中输入这个字串



得到答案admin。

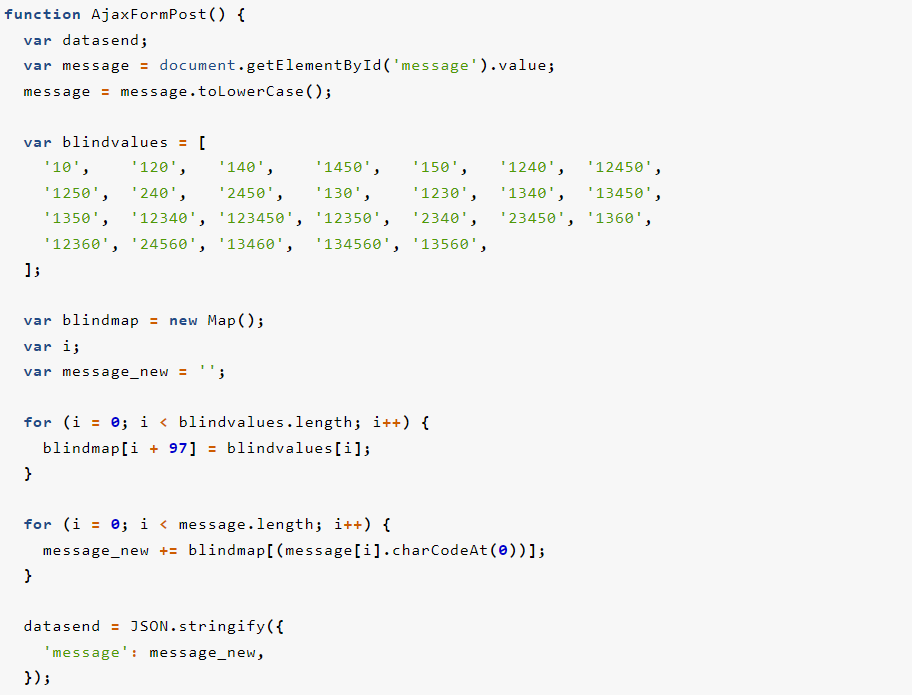
## CTF练习题4

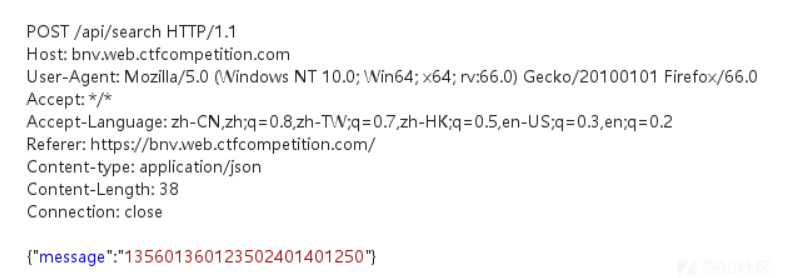
Web: BNV

首先给定一个网站https://bnv-web-ctfcompetition-com/。打开它，是一个盲人网，可以根据他们的城市找到最近的盲人协会。还有一个提交按钮，可用于搜索最近的盲人协会。



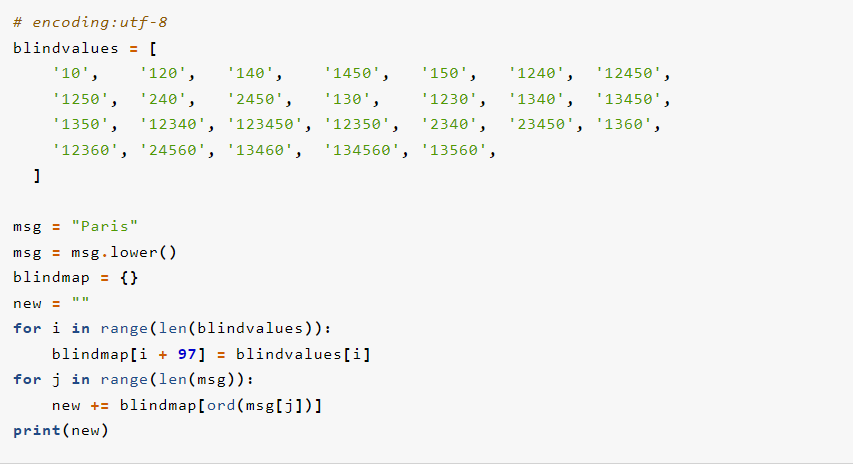
查看源代码看到有一个 post-js 文件，访问可以得到重要的 javascript 代码：

这段代码就是把 City 输入框的值每个字母转换为小写再映射到 长度为 26 的 blindvalue 数组对应位置的数字，然后将这串数字发送到 api/search 后端，Content.type 类型是 application/json，如果使用 Burp 截取数据包如下：



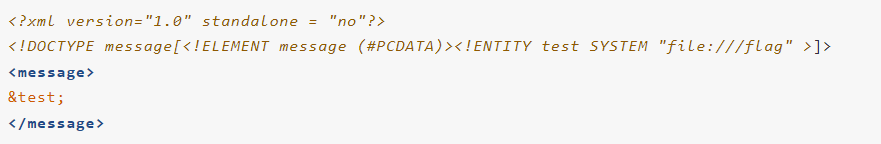
blindvalue 的数组是布莱叶盲文

小写字母映射到 blindvalue 数字：



想到既然是 application/json 那么是否支持 XML 呢？于是尝试了修改 Content.type 类型为 application/xml

可以成功利用的 payload 如下：



尝试使用system之后引号内的地址



返回

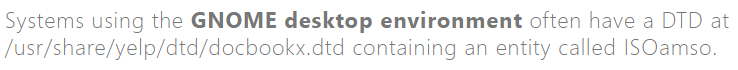


如果不存在返回的并不是这个内容，而是



经过测试 file:///flag 是存在的，而且这里只支持 file 协议，因此你是无法将数据传递至外部服务器。这也是本题的一个难点，解决办法就是利用服务端的一个本地 dtd，然后重新定义它里面的一个 entity 触发错误，然后错误信息显示的时候会泄露你需要读取的文件内容。

尝试系统默认的 dtd：/usr/share/yelp/dtd/docbookx-dtd



最终利用 payload：



成功得到flag

Invalid URI: file:///nonexistent/CTF{0x1033\_75008\_1004x0}, line 4, column 15