Explorer 的图库之一

下载后用记事本打开，在前面几行发现 flag

Explorer 的图库之二

把下载的东西加上后缀.jpg，放到 binwalk 里跑了下　发现有个 gzip 和 png 文件，用 dd if= /root/Desktop/12.jpg of= /root/Desktop/1.gzip skip=45654 bs=1 命令拉出来，解压得 txt 里的 flag

Explorer 的图库之三

Hint:最简单的 LSB 隐写

dd if= /root/Desktop/12.jpg of= /root/Desktop/1.png skip=45801 bs=1
打开 Stegsolve -> analyse –> Data Extract 把红绿蓝的 0 通道勾上然后分析　发现开头有段 base64 代码，放到网上一跑就出 flag

lightless 的渗透教室入门篇（一）

进渗透群的时候学到了?xxx 是 get，所以用火狐的 hackbar 往 http://115.28.78.16:13333/pentest/01/?hacker=HelloGet POST hacker=HelloPost，得到 flag

lightless 的渗透教室入门篇（二）

修复漏洞后用火狐的 modify headers 构造 http 头，在响应头里找到 flag

lightless 的渗透教室入门篇（三）

F12 发现在响应头里有 cookiecontent:admin=1 and isLogin=true，于是设置 cookie 域名为 115.28.78.16:13333,get flag

我是谁我在哪？？？

internet 设置->安全–>自定义设置->META TEFRESH->禁用
来源: https://zhidao.baidu.com/question/585638506.html

神奇的数字

看源码，查谷歌 intval($req["number"]) 的意思时 发现了原题 wp…https://www.leavesongs.com/PENETRATION/some-sangebaimao-ctf-writeups.html

不可能拿到的 flag

拿到 flag 要满足两个条件 name!=password&&sha1(name)==sha1(password)
所以用 hackbar POST name[]=1&password[]=2
Get

php 真可怕我要回农村

因为不懂 php 所以很多语句去谷歌用法，无意间就发现原题，gg
http://www.thinkings.org/2015/06/10/360-geekgame-writeup.html

你看看，逆向多简单

下载，dbg 打开，在 00F21055 处发现 flag

密码学教室入门（二）

mlfrj{Hfjxfw_hnumjw_8x_ozxy_ktw_kzs}
Hint: 这都不会可以退出密码学了
放到网上的在线解密跑了下 发现数字没变并且不对，手动往上位移 5 个从 8 变到 3 还是不对，然后从 1 开始试了下，没想到 1 就对了。

密码学教室番外篇

yxrdv{uxwupytip19954902180//+/%}
还是在网上跑了下，手动把数字向下位移 9 个，符号打算用 ASCII 位移但是嫌麻烦先移数字，没想到对了。

PS：虽然用工具用的很爽，但这并不是真的能力，解 rsa 的时候尝试写 python 解，但不知为何解出来的数字不对。。。还有 php 不会真的寸步难行，php 题目大多是搜代码时发现有原题，也不算能力。我的路还很长，希望自己以后不要老想着飞吧。