hgame 2016 WriteUp： Week1

written by SSGSGoKu

written on Jan.21.2017

- Pentest

lightless 的渗透教室入门篇（一）

这题要求对给定的页面发送 get 和 post 请求，get 请求内容 hacker=HelloGet，post 请求内容为 hacker=HelloPost。通过阅读资料和在网上查 get、post 的相关，知道 get 请求可以被包含在 URL 中发送。我使用的是火狐浏览器的 HttpRequester 插件。在 URL 中用?隔开正常的 URL 和 get 请求，？后输入 get 请求的内容，然后以 post 形式发送所要求内容的请求，在响应的源码里找到 flag.

lightless 的渗透教室入门篇（三）

这题让伪造 cookie。查看源码可发现<!-- Post me a hint can give you some hints... -->这么一句话，于是 post 了 hint 到本页面，发现 cookiecontent 为 admin=1 and isLogin=true，再用火狐查看 cookie 发现正好是两个，于是用火狐的插件把一个 cookie 的名字改为 admin，value 为 1，另一个 cookie 名字 isLogin，value 为 true，刷新页面得 flag.

- Crypto

密码学教室入门（二）

凯撒密码，就是移位，按照 hgame 对应密文的开头 5 个字母进行移

位，从 0 到 25 给每个字母编号，mlfrj 中每个字母的编号减 5 再 mod26 对应的字母得到的字符串为 hgame，其他字母的处理相同。数字和符号的处理有点恶心，经过了自己不少的尝试，后来猛然发现数字里面 1s 和 is 的发音最像 o(╯□╰)o，由此才发现数字是减 7 再 mod 10 处理，符号方面由于有花括号的存在所以不变。于是得 flag.

密码学教室番外篇

也是凯撒密码，与密码学（二）的套路一样，按照同样的规则处理，得到 flag.

密码学教室入门（四）

这题是 RSA 的简化版本，因为 e 是 16 进制表示的 1，所以根据 ed≡1（mod N），d 也可直接赋值为 1，如此一来根据公式 m≡c^d(mod N)，明文 m 就与密文 c 相同，于是将 c 的 16 进制表示用在线转换工具 hex to ascii 转化为 ASCII 码，就为 flag.

密码学教室入门（三）

这题是维吉尼亚密码，凯撒密码的升级版，看资料发现需要分组还需要知道密钥才能解。始终没有什么思路，最后尝试去 google 上找了个维吉尼亚密码的在线破解工具 VIGENÈRE CIPHER CODEBREAKER，密文丢上去然后暴力跑结果……不知道密钥的情况下结果有 500 个左右，大概浏览一下发现都不是正常的英语句子，但发现其中系统猜测的密钥有

规律,很接近 bcdef 的重复,于是修改密钥成 bcdefbcdefbcdefbcdefbcdef 进行尝试，再跑出来就是一段有意义的英语句子，丢到 google 上从 wiki 获知这本书的名字，加上 hgame{}就是 flag.

- Misc

Explorer 的图库之一

首先得到一个文件，用浏览器打开发现是一张图片，可能是图片隐写的题目,再用记事本打开在一开头就发现 flag.后证明 winhex,wireshark 等工具打开同样可以获得 flag.