1.观看视频[CTF挑战系列之高手炼成](http://www.shiyanbar.com/courses/detail/473)，并完成学习笔记。

|  |
| --- |
| （简要概述视频中所涉及到的知识点，注意，这不是又臭又长的思想感悟）  简介  分三种，解题，攻防，混合  准备  比脑洞（玩梗？），比团队，比规划（不让攻击主委会评分系统，不让疯狂扫对方服务），比后勤；搜集大量知识，思路开阔，勇于尝试，关注一切信息，提前准备好工具与环境  套路和工具  套路  WEB：mysql，PHP特性，文件上传绕过，伪造http请求头  密码：各种古典密码相互融合，文件异或，hash长度攻击  杂项：花式分析数据包，各种隐写，密码学知识大杂烩  隐写：各种隐写工具，LSB（藏在rgb里面的最后一位），文件开始结束符（图种），exif  隐写分析：分析载体，加密还是编码（熟悉文件格式）  工具  Firefox（hackbar，firebug，tamper data，user agent switcher）  Burpsuite（拦截发到服务器的请求，修改请求，或者多次发送）  Sqlmap（常用命令）  环境python和java等  隐写  初级，Stegsolve，Winhex，Notepad++，QR\_Research（二维码），Binwalk，Foremost  中级，bftools，mp3stego，steghide，adobe fireworks  逆向  OllyDbg，IDA Pro  综合  Kali linux，github，wireshark（抓包）  题目  1 what a fuck  Jother编码，直接运行就好，经验问题（看到有好多的括号）  2 上传绕过  既要jpg又要php矛盾呀，00截断（许多文件以0x00座位截止符），用到Burpsuite还要用到火狐代理，设置端口一致，拦截下来分析一下（repeater），改后缀，转到十六进制里面看到自己打的空格转为00，发过去就可以得到flag  3 我喜欢培根  摩斯密码，培根密码，（大家都说零基础，最后发现只有我才是）  4 这里没有key  遇到不懂先看看源码，vbscript encode  5 丘比龙的最爱  直接百度，，，，  6 A记录  下载数据包，用aircrack得到无线加密前的包，（三个命令，我选择图形化界面），用字典跑一下，找到密码，然后解密，  7 SB  图片放到工具（stegsolve）里，发现灰色通道有二维码，用QR\_Research查看就得到了结果  8 小苹果  扫到一串密码，然后解码得到汉字，当铺密码得到数字，查看一下图片的信息（kali）发现里面藏了一个压缩包，分开后从里面解压出来一个MP3，对其进行解密（密码是之前得到的数字），得到一串乱码（熟悉的人知道是base64），然后就得到了flag。  9 之前的思考题  过滤出http一个一个看（看不懂里面的命令T\_T）。  这次的思考题看到了新工具hashpump。 |

2. 一道隐写术的题，<http://www.wechall.net/challenge/training/stegano1/index.php>。

二进制和十六进制是和计算机打交道所必需的，hexedit和ultraedit都是很好的二进制/十六进制查看编辑器，这道题给了你一张图片，把它拖到hexedit或者ultraedit，看看你能不能找到flag，将答题通过的截图放到下面。

|  |
| --- |
|  |

3.编写PHP程序，将字符串ACEGIKMOQSUWY和字符串BDFHJLNPRTVXZ拼接成ABCDEFGHIJKLMNOPQRSTUVWXYZ，将代码附在下面：

|  |
| --- |
| <?php  $var1 = "ACEGIKMOQSUWY";  $var2 = "BDFHJLNPRTVXZ";  echo "$var1" . "$var2";  ?> |