## 讨论记录

**柴冕汉郎**

傅里叶，盲水印，离散变换(对矩阵类似傅里叶变换)

溢出？堆溢出的地址如何寻找

**李云鑫**

曼彻斯特编码：差分、正常（高低变化与低高变化），找到了writeup，曼彻斯特解码之后得到CRC-8校验位，基本逻辑运算校验。

Pwn题目：栈溢出、格式化字符串，利用漏洞。函数指针free掉之后产生UAF漏洞。

**罗晓倩**

密码：摩斯密码、棋盘、base64、栅栏密码、移位密码。进化栅栏密码

安全杂项：脑洞要大。

**魏子豪**

不仅仅是逆向，也有脑洞。

简单逆向题：修改标志位直接出flag、通过简单的密码算法计算flag

高难度：Linux下使用gdb动态调试、和密码学结合（如何识别程序中使用的高强度算法？PEiD插件）

工具：ida ollydbg windbg gdb

**杨智**

Web: Csrf，二次注入，Php目录注入，SQL注入，存储型XSS，

安卓逆向：通过脚本解决算法问题

CTF题目Warmup：zip明文攻击、频域盲水印

Bandhanker（？）：ip转url。

**吴华瑞**

编码：看出使用CRC-8校验位

曼彻斯特编码主要特点：两位分开全都是0和1，标准定义从0到1为1，从1到0为0（高低电平变化）。

差分方法

一张图片，隐写，做成压缩包解压提示文件损坏，通过特殊程序直接打开压缩包（杨智：kali可以直接打开）

**殷悦**

Python RSA加密

修改汇编自动暴力破解（加密的数比较小可以尝试）

## 知识点

逆向：IDA OD APK逆向

Web： SQL注入 XSS 跨站csrf PHP目录扫描

Pwn：gdb rop 堆栈溢出找地址, Return to libc, got覆盖

Misc：脑洞题慢慢积累

密码学：RSA攻击方法专题（攻击方法、攻击脚本）

## 基本工具

逆向：OllyDbg, IDA, Android killer

Web: BurpSuite,

Pwn: gdb, PwnTools, gdb-peda(gdb插件)

Misc: binwalk, Advanced Archive Password Recovery(压缩包爆破)

## 专题



## 时间表及注意事项

1. 各专题负责人于本周四（7月20日）之前将专题三级目录（基础知识->重点知识->不少于10道题的示例）发给魏子豪。
2. 本周五（7月21日）晚，实验室开会，定下具体专题内容。具体时间另行通知。
3. 专题完成时间控制在两周之内，部分简单专题要求一周之内完成。
4. 专题资料汇编原则：在仔细阅读现有资料的基础上加以整理、完善，注意标明来源，写好参考文献目录。
5. 交流会开会频率为每周两次（小学期期间）、每天（小学期结束后）。写好会议记录。