基础工具的使用

AssassinQ

- 新建->变量名"JAVA_HOME"，变量值"C:\Program Files\Java\jdk1.8.0_211"（即JDK的安装路径）
- 编辑->变量名"Path"，在原变量值的最后面加上";%JAVA_HOME%\bin;%JAVA_HOME%\jre\bin"
- 新建->变量名"CLASSPATH"，变量值".;%JAVA_HOME%\lib;%JAVA_HOME%\lib\dt.jar;%JAVA_HOME%\lib\tools.jar"

- 虚拟机：VMware Workstation、VirtualBox
- Linux：Kali、Ubuntu

- WEB：Burpsuite、FoxyProxy、hackbar、phpStudy
- MISC：Stegsolve、010Editor
- 基础的命令行工具（Linux）：git、binwalk、foremost
- Else：github、google（Bing/百度）、python（脚本）

Burpsuite

- Burp Suite 是用于攻击web 应用程序的集成平台。它包含了许多工具，并为这些工具设计了许多接口，以促进加快攻击应用程序的过程。所有的工具都共享一个能处理并显示HTTP 消息，持久性，认证，代理，日志，警报的一个强大的可扩展的框架。

- **Proxy**：BurpSuite的核心功能，作为一个在浏览器和目标应用程序之间的中间人，允许你拦截、查看、修改数据流
- **Intruder**：可以执行许多任务，合适的攻击类型取决于应用程序的情况，比如有目录遍历；fuzz、xss 和 sqli，还有暴力破解等
- **Repeater**：用于手动操作和发送个别HTTP请求，并分析应用程序的响应一个简单的工具。可以发送一个内部请求从Burp任何地方到Repeater，修改请求并发送。
- **Decoder**：将原始数据转换成各种编码和哈希表的简单工具。它能够智能地识别多种编码格式采用启发式技术。
- ……

- 如果8080端口被占用了怎么办?
- netstat -aon | findstr "8080"
- 根据PID在电脑的任务管理器中查看对应的占用程序，然后将其关闭

HTTP的请求方式

- HTTP1.0定义了三种请求方法： GET, POST 和 HEAD方法。
- HTTP1.1新增了五种请求方法：OPTIONS, PUT, DELETE, TRACE 和 CONNECT 方法。
  - GET：请求指定的页面信息，并返回实体主体。
  - POST：向指定资源提交数据进行处理请求（例如提交表单或者上传文件）。数据被包含在请求体中。

前端三剑客

- HTML（Hyper Text Markup Language）：超文本标记语言，通过标签语言来标记要显示的网页中的各个部分，浏览器认识的规则，它是一种标记语言，不是编程语言，使用标记标签来描述网页
- CSS（Cascading Style Sheets）：层叠样式表定义如何显示 HTML 元素
- JavaScript是一种脚本语言，其源代码在发往客户端运行之前不需经过编译，而是将文本格式的字符代码发送给浏览器由浏览器解释运行

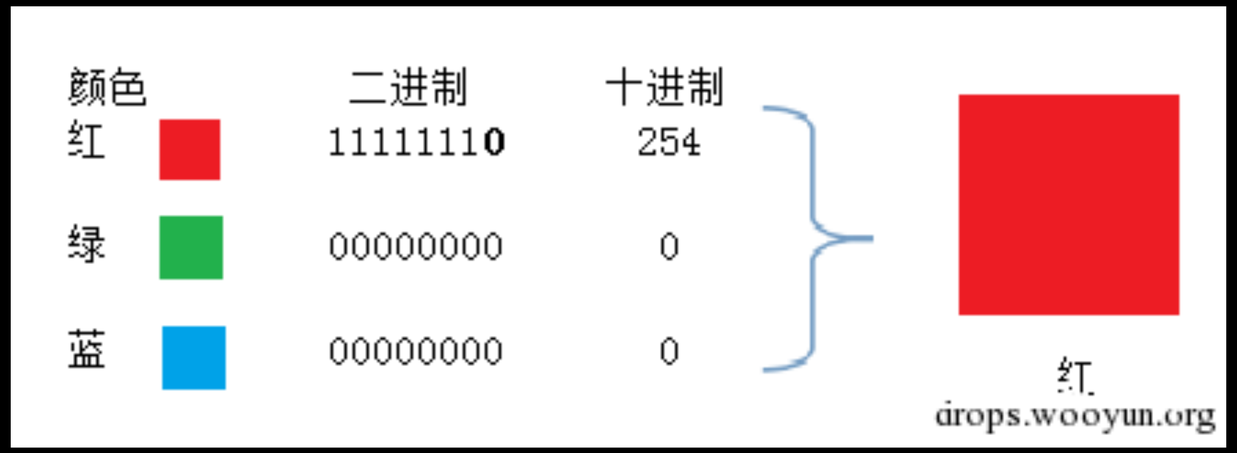
phpStudy

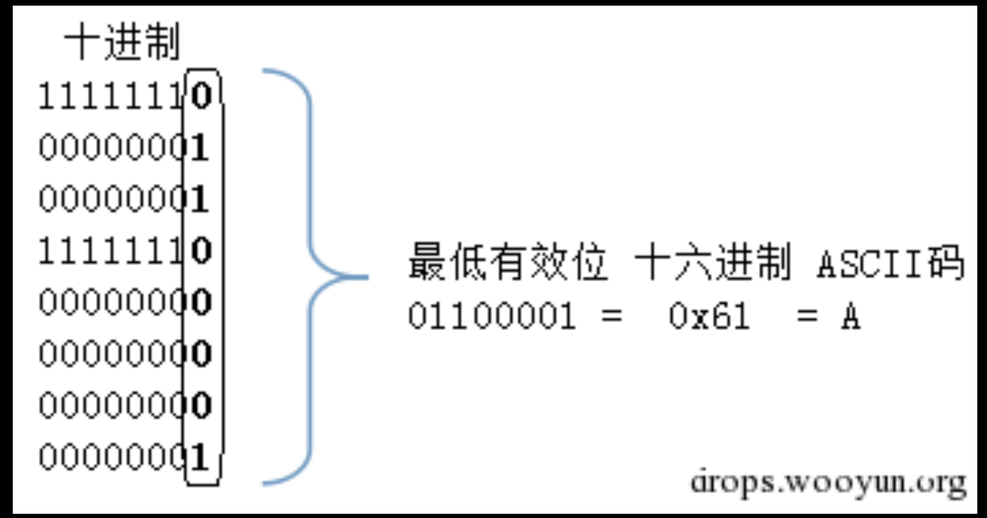
- phpStudy是一个PHP调试环境的程序集成包。
- 该程序包集成最新的Apache+PHP+MySQL+phpMyAdmin+ZendOptimizer，一次性安装，无须配置即可使用。

Steganography

- Steganography（隐写术）是一门关于信息隐藏的技巧与科学，所谓信息隐藏指的是不让除预期的接收者之外的任何人知晓信息的传递事件或者信息的内容。 隐写术的英文叫做Steganography，来源于特里特米乌斯的一本讲述密码学与隐写术的著作Steganographia，该书书名源于希腊语，意为“隐秘书写”。

Least Significant Bit





- 图片分析：https://ctf-wiki.github.io/ctf-wiki/misc/picture/introduction/
- Magic Number：https://asecuritysite.com/forensics/magic

BMP

- https://www.siggraph.org/education/materials/HyperVis/asp_data/compimag/bmpfile.htm
- 24位真彩色BMP图像包含三个部分：文件头、位图信息头、位图数据

- typedef struct tagBITMAPFILEHEADER { /* bmfh */
- UINT bfType;　　//两个字节，低位字节为B，高位为M
- DWORD bfSize; //四个字节，整个文件大小
- UINT bfReserved1; //两个字节，保留，设置为0
- UINT bfReserved2; //两个字节，保留，设置为0
- DWORD bfOffBits;　//四个字节，文件开始到位图数据的偏移量
- 　　　　//对24位真彩色BMP，该值固定为54
- } BITMAPFILEHEADER;

社工

- 在计算机科学中，**社会工程学**指的是通过与他人的合法地交流，来使其心理受到影响，做出某些动作或者是透露一些机密信息的方式。 这通常被认为是一种欺诈他人以收集信息、行骗和入侵计算机系统的行为。
- 妈妈认为在朋友圈发照片很危险，该怎么反驳她？ - 幻泉的回答 - 知乎
- 一些社工密码经验

博客

- Hexo+GitHub
- 简书
- 博客园
- PS：学习Markdown的语法

References

- Burpsuite使用介绍：http://drops.xmd5.com/static/drops/tools-1548.html
- Burpsuite简介：https://blog.csdn.net/zhang14916/article/details/86623667
- 隐写术总结：http://bobao.360.cn/learning/detail/243.html