网络安全竞赛实战任务书

1. 练习目的:

经过一系列的学习之后，对所学的知识有更加直观的了解，使动手能力得到进一步提高，同时根据学校的现有条件，特设置了以下题目。

1. 练习内容

任务三-综合练习

练习一：粗心了

题目地址：http://106.52.138.23:10001/

解题：使用御剑后台扫描工具扫描

练习二：Where is logo

题目地址：http://106.52.138.23:10002/

解题：使用御剑后台扫描工具扫描

练习三：头等舱

题目描述：听说http消息头可以隐藏信息，你能找到吗？

题目地址：http://106.52.138.23:10003/

解题：使用chrome浏览器F12,可以查看http头部信息，可找到flag

练习四：flag在这里

题目描述：X老师让小宇同学找藏在网站的flag值，但小宇同学好像被404页面卡住了。

题目地址：http://106.52.138.23:10004/

解题：使用chrome浏览器F12,可以查看http头部信息，可找到flag

练习五：特殊的浏览器

题目地址：http://106.52.138.23:10005/

解题：使用kali系统中的BurpSuite代理proxy，修改http头部信息User-Agent

练习六：密码忘记了

题目地址：http://106.52.138.23:10006/

解题：暴力破解密码（重复测试不同密码）,使用kali系统中的BurpSuite代理proxy，暴力破解Intruder(设置payload,添加密码字典)

练习七：流量数据包分析

题目地址：http://106.52.138.23:10007/

解题：通过wireshark进行搜索flag,进行http stream流量跟踪Follow.

练习八：图片隐写

题目地址：http://106.52.138.23:10008/

解题：使用winhex打开图片，将最后明文字符复制，进行base64解码即可

练习九：加密的压缩包

题目地址：http://106.52.138.23:10009/

解题：RAR伪加密

练习十：奇怪的编码

题目描述：请通过一系列的编码转换，得到最终的flag值。

题目地址：http://106.52.138.23:10010/

解题：将字符进行base64解码得到是16进制值，再将该值转为字符串

练习十一：成绩查询

题目描述：请找到数据库中的flag值。

题目地址：http://114.67.175.224:19341/

解题：SQL post注入