20200808信息安全实训

笔记本:	我的第一个笔记本		
创建时间:	2020/8/8 11:47	**更新时间:**	2020/8/8 12:31
作者:	820410740@qq.com		
URL:	https://blog.csdn.net/qq_40481505/article/details/89929978		

攻防世界
command_excution 因为可以直接ping显示 那么可以查询所有文件 找到flag所在文件 查看
simple_php 代码审计 根据代码显示 flag被存放于两个文件中 需满足参数a=0且a为真和b大于1234且不为数字
关于php的弱类型比较 1234=1234a 所以在地址栏后加上 a="0"&b=1235a
xff_referer 因为xff和referer可以伪造 使用bp抓包在http头加入一条X-Forwarded-For:123.123.123.123
send 发现响应必须来自谷歌 所以在Referer:https://www.google.com
send 得到falg
webshell 一句话木马 使用蚁剑配合 获取falg
simple_js 在html中插入了一段js代码 通过审计可知有一段十六进制代码可能与密码有关，将其转换为10进制为55，56，54，79，115，69，114，116，107，49，50再将其转换为字符串可知为 7860sErtk12
而后将其拼入格式中为 `Cyberpeace{7860sErtk12}`