ctf入门题库_「ctf比赛」web安全CTF比赛习题（初级） - seo实验室

原创

weixin_40001967 于 2020-12-22 06:12:44 发布
文章标签： ctf入门题库

ctf比赛

一、Robot

访问URL，可以看到一张骚气十足的图片，然后就什么都没了。。。没了。。。

不可能啊，一张骚图片就想欺骗小编，想的太美(长得丑了)

题目说明写的是robot，想想多半是有猫腻，想来也就是关于”robots.txt”了，上百度百科。

好的，直接在URL后面加上robots.txt访问，哟呵，果然是成功了，佩服小编的聪明才智了。

访问查看到的目录，很容易就发现“admin/3hell.php/”存在问题，右键查看源码，flag信息立马出现。

二、seelog

这次的题目是seelog，很明显呢，查看日志，访问URL(一样一样滴)

呃呃呃，居然告知我是“内部网站，非请勿入”，着实伤了一把小编的玻璃心，不过越是这样小编就越要去看一看了。

题目说明给的是“seelog”，这让刚做完了“robot”的小编延续了优良的传统，直接网址后面加一个“log”访问，不出意外成功了(小编的运气应该还算不错)，马上就可以看到两个日志文件，ok，直接访问“access.log”文件。

一大堆的日志，审计起来多半得丢了半条命，那么如何关键快速的照到我们想要的结果呢？(答案：挨着找)

我们可以“Ctrl+f”快速查找关于200的状态代码(200-确定。客户端请求已成功。)，找到我们想要利用的信息

分析找到的信息，可以看到是“GET”请求方式

OK，把找到的信息添加到URL后进行访问，flag信息就自己乖乖的出来了。。

三、ip spoofing(ip欺骗)

题目说明给的是非常明显了，直接访问网址，进入登录界面(还是来张图吧，不然略显单调)

查看登录界面的源代码，直接就获取到了登录用户名和密码(有个查看源代码的习惯，小编觉得还是很不错的)，然后高兴的拿去登录，尴尬的来了，“你的ip不在许可范围内”，怎么办呢？

简单粗暴，burp抓包，先“repeater”一波，可以看到返回了许可ip地址(可以好好利用了)

“X-Forwarded-For”，伪造ip地址，进行欺骗，皇天不负有心人，flag信息我来了。

四、phpinfo

小编遇到更简单粗暴的了，phpinfo直接给出来了，看着这满屏的信息，小编顿时头大，可一看到这URL网址，柳暗花明又一村啊，细心查看配置，发现“allow_url_fopen”处于“On”状态，果然是存在远程文件包含的。

ok，小编也准备继续简单粗暴了，直接包含“flag.php”文件，可以成功访问(鼓鼓掌)，好的，利用php的“filter”伪协议，读取文件的内容，经过base64解码后flag信息就出来了。

相关阅读

方法一：如果你的win2000系统装了officeXP或以上版本，它会在你和系统里留下一个可误的ctfmon.exe，这真的是一个恶魔，曾经困扰了无数的

ExtractFilePath是C++builder开发环境里面比较常用的方法，今天就帮大家理一理。函数原型如下: De

网络安全日益重要，近期热播电视剧让观众开始关注CTF(网络安全大赛)这个词，真实的CTF是怎么样的？长亭科技主办的2019年第二届Real World

原文链接：
http://rcoil.me/2017/06/CTF%E7%BA%BF%E4%B8%8B%E8%B5%9B%E6%80%BB%E7%BB%93/

作者：Rcoll

总结的非常好，转载收藏，感谢表哥

作者:fbysssmsn:jameslastchina@hotmail.com blog:blog.csdn.net/fbysss声明：本文由fbysss原创，转载请注明出处关键字：java strict