安全小课堂第115期【聊聊CTF比赛】

京东安全应急响应中心 1周前

CTF（Capture The Flag），中文一般译作夺旗赛，在网络安全领域中指的是网络安全技术人员之间进行技术竞技的一种比赛形式。CTF起源于1996年DEFCON全球黑客大会，是目前较流行的网络安全赛事。

JSRC **安全小课堂第115期**，邀请到**腹黑**作为讲师就**CTF比赛的一些想法**为大家进行分享。

CTF比赛吸引你的是什么？

京安小妹

腹黑：

CTF吸引我的地方，首先是在比赛的时候可以学到很多东西，比如很多web题就会用一些最新的漏洞来开发题目，在做这些题目的时候就可以get到最新的漏洞。还有就是CTF题目考察面比较广他能够让你对各种技术都有所了解和使用。再者的话如果在ctf中拿到一些很好的名次其实你本人也会很有成就感和荣誉感，而且还有奖金（奸笑.jpg）

CTF比赛和实战中的漏洞挖掘，有什么区别和联系？

京安小妹

腹黑：

我觉得CTF和漏洞挖掘最大的区别就是CTF有的题目偏向于理想化，理论在实战中不一定能用到，但是很多的CTF题目却需要用到许多实战技巧。CTF的套路太多，导致有可能一个实战很厉害的人去玩CTF未必会得心应手，甚至会不知道从何下手，CTF是竞赛，他会有各种玩法或者说套路，但是实战的话完全靠的就是经验。还有就是CTF有的题目更偏向于研究，在实战中不一定能用到，但是他却能够为实战打下很好的技术基础。

讲师

很多高校都会举办自己的CTF比赛，也有很多同学是以CTF比赛开启了自己信息安全道路，那么以CTF入门，怎么样才能快速得到成长呢？

京安小妹

腹黑：

CTF入门的话我觉得最好的方法就是以赛代练。一开始刚接触可以去一些CTF平台上做一些简单的题目比如bugku这类平台以达到入门的目的,我们可以称它为刷题。然后就是多参加比赛，每次参加比赛都能有不一样的感悟，这种感悟是你只看书得不到的。当你参加的比赛多了之后做的题目自然也就多了，这个阶段你看到一个题目就大概可以知道他是想考你什么了。还有一点对学习也很重要，就是多看大佬们的WriteUp然后去复现

讲师

推荐一些高质量的CTF赛事

京安小妹

腹黑：

高质量的比赛其实还是蛮多的特别是一些国际赛，今年长亭办的Real World CTF 2018质量应该算是公认的比较高了，其他的一些高质量的比赛可以参考下ctfrank

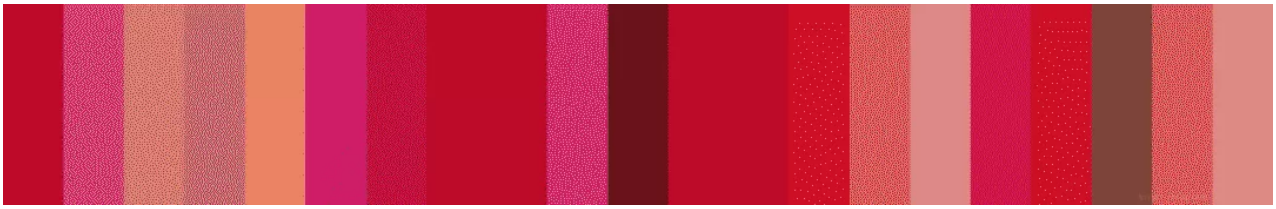
讲师

分享一道你觉得非常有意思的（脑洞大的）题目，分析一下思路

京安小妹

腹黑：

我印象比较深的应该是N1CTF的Lipstick，作为一个直男，我做这题做哭了：



他的题目长这样，是的没错就是口红，先通过隐写发现提示YSL。emmm然后我就懵逼了，一个CTF和杨树林有啥关系，但是题目还是要做的呀，于是继续一顿骚操作发现有个PK开头的东西，显然是个压缩包，提取出来发现没密码……折腾半天放弃了然后丢给了队里小姐姐，小姐姐拿着图片去官网找到了他的色号然后一波操作猛如虎把色号转成二进制，再组合，bin2text，然后得到了解压密码（直男的我哭了……）

讲师

本期JSRC 安全小课堂到此结束。更多内容请期待下期安全小课堂。如果还有你希望出现在安全小课堂内容暂时未出现，也欢迎留言告诉我们。

安全小课堂的往期内容开通了自助查询，点击菜单栏进入“安全小课堂”即可浏览。

简历请发送：cv-security@jd.com

微信公众号：jsrc_team

新浪官方微博：京东安全应急响应中心