CTF Web篇从菜鸟到精英

原创

anquanniu牛油果 于 2020-09-16 19:45:57 发布 1160 收藏 6

文章标签： CTF

本文链接：https://blog.csdn.net/anquanniu/article/details/108629006

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全球大会，以代替之前们通过互相发起真实***进行技术比拼的方式。发展至今，已经成为全球范围网络安全圈流行的竞赛形式。

入门CTF的内容会从CTF中WEB、MISC、Crypto三个方向的各种漏洞原理学起，同时配合实际例题重现，这样有一个系统的学习过程，同时在各个点了解后，再进一步寻找大型赛事中较难的题目进行复现，进一步提升技能，拓展思路，增加自己点上更多的技能点，实现由点到面的突破。

带着目标去学习既系统又高效，一般是了解各个常见的漏洞原理和利用场景，可以在CTF比赛中熟练的发现漏洞，也就是考点所在。可以掌握常见CTF比赛中的解题思路和解题技巧，能够大致猜测出题人的意图所在。系统地学完这些后，不仅能提升自己在各种CTF比赛中的竞争力。同时也能获得在实际漏洞挖掘过程中的一些trick。
如果你是网络安全爱好者、CTF爱好者欢迎一起交流！

到底如何学？
1.分析赛题情况
2.分析自身能力 自己最适合哪个方向
3.选择更适合的入手

分析赛题
PWN、Reverse偏重对汇编、逆向的理解 对底层理解
Crypto偏重对数学、算法的深入学习 密码课要深入学

Web偏重对技巧沉淀、快速搜索能力的挑战 发散思维，对底层只需要了解，代码原理，关于漏洞点的积累
Misc则更复杂，所有与计算机安全挑战有关的都在其中 隐写，图片数据分析还原，流量，大数据，对游戏分析逆向
入门知识：
都要学的内容：linux基础、计算机组成原理、操作系统原理、网络协议分析
入门路径：http://t.cn/AiOgQ4Q4
A方向：IDA工具使用（fs插件）、逆向工程、密码学、缓冲区溢出等
B方向：Web安全、网络安全、内网***、数据库安全等 前10的安全漏洞

随着网络安全上升到国家战略层面，直接或间接的促进了各种CTF比赛的兴起。一部电视剧“亲爱的，热爱的”让很多喜欢网络安全的朋友纷纷热血沸腾。有很多还没有入门网络安全的朋友苦苦的找不到学习的方法，久久的门外徘徊。《CTF Web篇从入门到精英》这么课程就是为了解决大多数还没有入门的小白，从基础开始讲解，再到答题步步深入。本课程第一部分是对课程的一个介绍，对CTF的一个介绍。第二部分是必备基础知识，包括基础的Linux，Windows，SQL等等。第三部分是对web安全测试的一些讲解，漏洞原理的分析。第四部分是在web线上答题的一些技巧，方法以及案例，第五部分是线下AWD比赛案例讲解，主要包括攻和防，讲解攻防的一些操作和注意事项。

通过本次课程的学习，读者可以了解并掌握以下内容。

（1）对CTF比赛有一个初步的认识和理解。

（2）对CTF比赛的分类更加的清晰明了

（3）对答题类的CTF可以自己独立的思考，并掌握不同类型题目的答题思路和方法。

（4）对AWD线下比赛的一些规则进行了解，并且掌握攻防的思路。

（5）可以组队或者个人参加各种线上或线下的比赛。