CTF入门之web和逆向

原创

小傅老师 于 2019-07-01 11:52:17 发布 4038 收藏 28
版权声明：本文为博主原创文章，遵循 CC 4.0 BY-SA 版权协议，转载请附上原文出处链接和本声明。
本文链接：https://blog.csdn.net/haodeshua/article/details/94384369
版权
题型：

MISC（安全杂项）、PPC（编程类）、CRYPTO（密码学）、REVERSE（逆向）、STEGA（隐写）、PWN（溢出）

WEB（web类）：WEB应用在今天越来越广泛，也是CTF夺旗竞赛中的主要题型，题目涉及到常见的Web漏洞，诸如注入、XSS、文件包含、代码审计、上传等漏洞。这些题目都不是简单的注入、上传题目，至少会有一层的安全过滤，需要选手想办法绕过。且Web题目是国内比较多也是大家比较喜欢的题目。因为大多数人开始安全都是从web日站开始的。

个人经验（主要碰的是web，其次是逆向，其他类型的题没碰过）：

本人的经验，学习计算机安全知识，主要是理论和实践结合。理论主要是看书，实践则是实操。对于没有机会去公司等实际环境中实践的同学，刷ctf题是个不错的选择，因为一些ctf题的网站已经把实操的环境给搭好了，可以节省大量的配置环境的时间。

解ctf题目中会应用到一些基础的安全知识，像web安全的sql注入，csrf,文件上传，文件包含等都会在ctf题中有所体现。密码学的一些知识，逆向中一些工具的使用等知识。当然要解出题目还需要也要有很大脑洞。

本人觉得对于基础比较菜的菜鸟，像我，可以从web类的题目开始，因为web比较简单。之后刷完web后可以刷逆向的。密码学的则需要先看书，密码学。

入门：

在这里推荐一下一个网站xctf：

https://adworld.xctf.org.cn/task

这个网站的题目（我只刷了web和逆向的一部分），由易到难，最好是先将新手练习区刷了（快速入门）。

进阶：

入门后可以继续在此网站刷进阶区（自带writeup，不过要金币，不懂就自己照着做一遍，一定要理解为什么才开始下一题），也可以去其他网站如http://www.shiyanbar.com/ctf/practice实验吧刷题。

个人刷题经验：

本人感觉xtcf的新手练习区特别适合菜鸟入门。如果新手练习区你还是入不了门，说明你的理论基础还不行。如web,你可以自己先建一个简单web网站（基础知识），逆向则建议你则可以先看一下加密和解密这本书。密码学则需要系统的学习一下密码学的书。

最后说一下，个人感觉菜鸟刚开始刷题的时候不要死磕，尝试了2个小时还没思路，可以先看writeup先做一遍。而且刚开始刷题最好是偏重于理解ctf题里的安全知识，writeup的代码最好自己独立写一般。