

CTF从入门到提升

原创

anquanni牛油果 于 2019-07-10 18:17:21 发布 4456 收藏 130

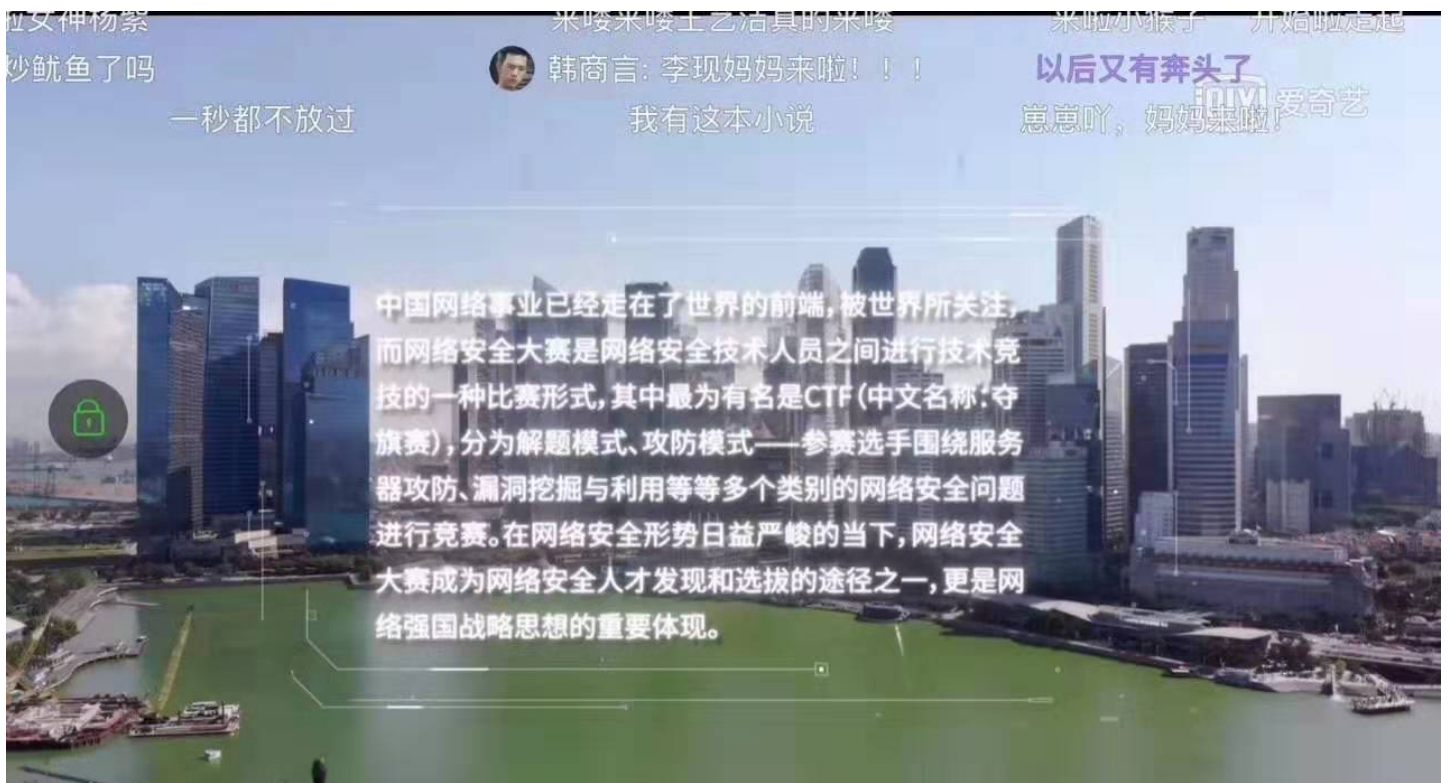
文章标签: [CTF](#) [CTF比赛](#)

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/anquanni/article/details/95361701>

版权

CTF选手的操作都是像吴白那么帅嘛? 如何入门CTF比赛, 一篇经验带你入门。

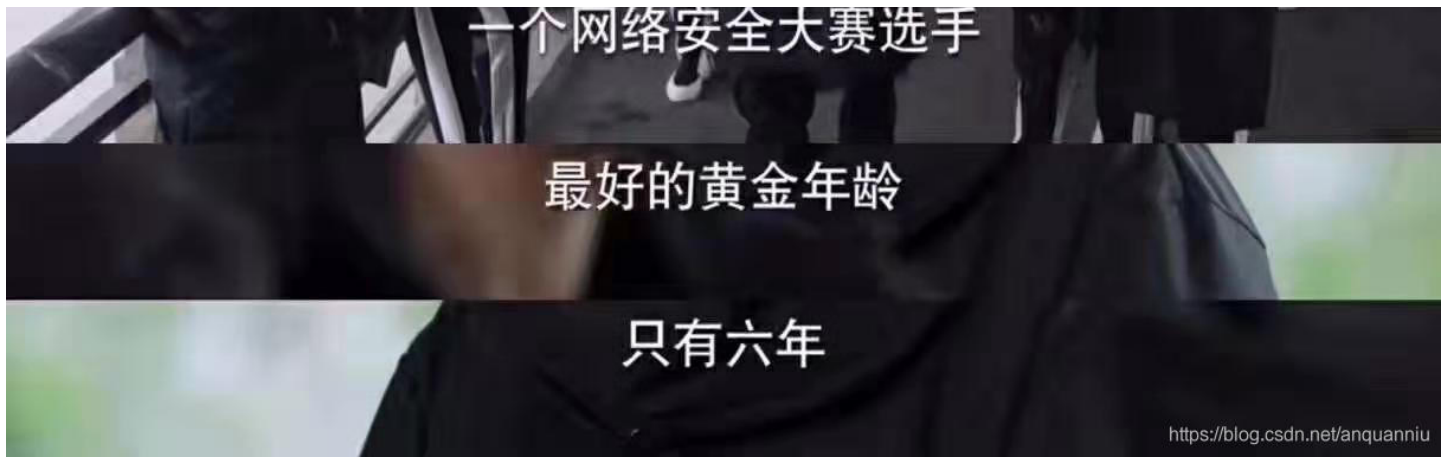


CTF (Capture The Flag) 中文一般译作夺旗赛，在网络安全领域中指的是网络安全技术人员之间进行技术竞技的一种比赛形式。CTF起源于1996年DEFCON全球大会，以代替之前们通过互相发起真实***进行技术比拼的方式。发展至今，已经成为全球范围网络安全圈流行的竞赛形式。



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 侧重对汇编、逆向的理解 对底层理解

Crypto 侧重对数学、算法的深入学习 密码课要深入学

Web 侧重对技巧沉淀、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



平时ctf练习

ctf逆向:

<http://reversing.kr/>

<http://pwnable.kr/>

<http://exploit-exercises.com/>

<http://overthewire.org>

<http://security.cs.rpi.edu/courses/binexp-spring2015/> bin 干货区

<http://www.52pojie.cn/forum-67-1.html> 【2014CrackMe大赛】

SQL:

<https://github.com/Audi-1/sqli-labs>

<http://redtiger.labs.overthewire.org/>

ctf XSS:

<http://prompt.ml/>

<http://xss.pkav.net/xss/>

<http://www.doscn.org/xss/>

<http://xss-quiz.int21h.jp/>

<http://escape.alf.nu/>

ctf综合练习:

<http://hackinglab.cn/> 网络信息安全***学习平台

<http://captf.com/> ctf题目

工具(黑软有分风险, 最好在虚拟机里搞)

<ftp://222.18.158.199/>(校园网内网可以访问, 不仅仅只有工具哦, 有许多总结, 各方面的)

<http://forum.cnsec.org/thread-94330-1-1.html> 2015暗组工具包 (***)

<http://bbs.secbox.cn/thread-196-1-1.html> 2015_安全盒子工具包

<http://www.secbox.cn/hacker/tools/3552.html> 法客论坛2015工具包-第三版

<http://www.52pojie.cn/forum.php?mod=viewthread&tid=388015> 吾爱破解工具包 2015/7/22 (逆向)

<http://down.52pojie.cn/> 爱盘 - 在线破解工具包, 教程,

<http://www.52pojie.cn/thread-341238-1-1.html> 吾爱破解论坛专用破解虚拟机