CTF入门篇

CTF，capture the flag，夺旗赛。

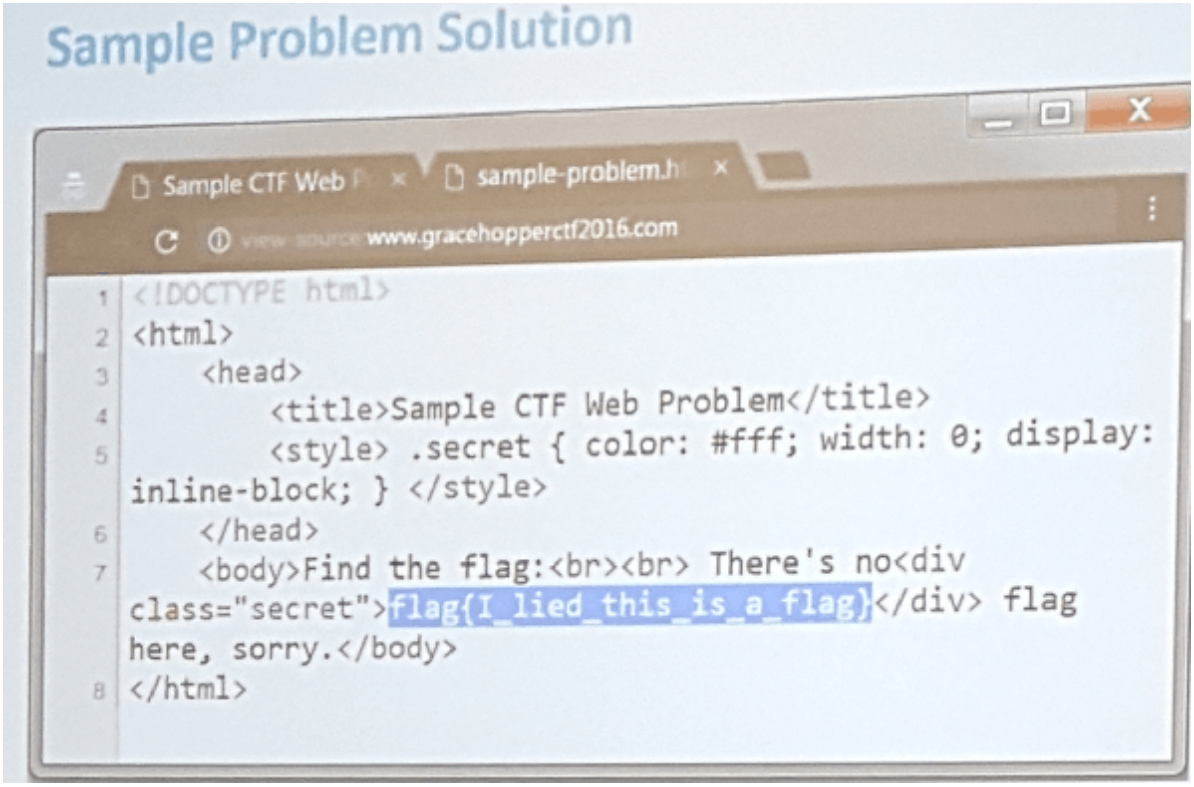
一类计算机安全/网络安全/信息安全相关的竞赛/游戏。

猫猫也能学会的CTF入门教程

Q：旗子（flag）是什么?

旗子是一串字符串，模拟攻击中攻击者获得的敏感信息。计算机攻击有几个目的，其中之一是获取敏感信息（盗窃账号密码、盗窃机密信息），用一串特殊的flag字符串代表敏感信息，当看到flag的时候，代表系统已经被攻陷（获取权限），完整性被破坏（逻辑、密码学攻击），需要保密的敏感信息已经泄露（大坏坏）。

基本上长这个样子：flag{meow_MeoW_m30w_QWQ}



Q：CTF的玩法是什么?

基本有两类，夺旗和攻防。

夺旗通常给出一个系统、一个文件、或一个页面，通过各种奇奇怪怪的手段穿透系统漏洞，找到藏在里面的flag，将flag值填到提交点基本算通过本题。目前大多数CTF都是这种模式。

攻防模式模拟真实入侵环境，分为红蓝队，一方攻击一方防守，线下赛采用这种模式比较多，也不乏一些物理黑客通过殴打对手获得flag。

Q：如何成为CTF大师?

使用黑客精神（Hacker Attitude）：

1. The world is full of fascinating problems waiting to be solved.
2. No problem should ever have to be solved twice.
3. Boredom and drudgery are evil.
4. Freedom is good.
5. Attitude is no substitute for competence.

使用物理攻击

CTF的方向

虽然CTF可以包罗万象，从缓冲区溢出，到硬件攻击，从更换纸尿裤，到消杀蟑螂，但，CTF依然可以分为几个大类：

1. Web：网站攻防，精通网页渗透，从SQL注入花式绕过，到抽奖活动狂薅羊毛，从SSRF内网连跳，到SSTI沙箱逃逸，页面方向同时也是安全方向第一大类，不仅大秀操作应用广泛，还能日常兼职白帽hacker交漏洞赚外快。
2. Forensics：文件分析，搜刮线索，破解谜题。从十六进制穿梭到硬盘加密，从套壳图片到花式隐写，从密码学和最底层分析文件结构。
3. Binary：二进制，软件复杂不要怕，ELF逆向手撕一把梭，程序和系统层面攻击软件结构，破解软件逻辑，绕过脆弱加密体系，深入软件的每一个流程，窥探调用链的每一个DLL。
4. Reverse Enginerring：早些年通常和Binary没有区分，自从Java、Python、Android越来越火之后，软件逆向从二进制中独立。通过反编译器获取伪代码，从dex抽取java源码，偷取流程重新编

辑，动态链接so逆向。

5. Cryptography：密码学，信息安全中的数学家。攻击脆弱密码的各个环节，通过弱点破解密码学加密，直接获取高危或严重级别的漏洞利用。
6. Programming：开发，程序攻击的典范，设计程序针对攻击环节，需要比较强的编程能力。
7. Misc：混合，所有方向一起来吧。

通常我们的CTF队伍会由各个方向的同学组成，各司其职，分别负责不同方向的题目。

如何入门CTF

通过在线教程：

https://ctf101.org/（入门教程，每个分类，英文）

https://trailofbits.github.io/ctf/（入门教程，英文）

http://www.catb.org/~esr/faqs/hacker-howto.html（入门教程，英文）

https://paper.seebug.org/（各种各样的安全收集，中文）

通过平日里各种各样奇怪知识的积累：

https://cve.mitre.org/（CVE漏洞库）

https://0x00sec.org/（奇怪的论坛）

通过夜以继日不断通关CTF题目/比赛的经验：

https://ctflearn.com/challenge/1/browse（在线题库，难度较低）

https://ctftime.org/（比赛时间表）

https://www.ichunqiu.com/competition（国内比赛平台）

等级提升

积累了许多经验之后，你的等级提升了！

终于在这条奇怪的过于漫长且完全不知道往哪里走的技能树上晋升了一个等级，于是又开始了一个不知道如何提升但总之东一锄头西一锤走起来吧。

CTF技能的提升有可能会非常缓慢且看不到成效，但日复一日的积累可以攒下非常恐怖且广泛的知识量，包括但不限于计算机和数学，有时也包括文学（自然语言处理）、哲学（自动论证机）、神秘学（猜解发散联想思维）。

业余时间，开始思考在黑客论坛小有名气（黑客线）、发布安全漏洞提交CVE（白帽线）、入手硬件硬核改装（赛博线）、还是成为天才手撕SCI（科研线）？

总之，都是可以的吧。

使用魔法攻击

物理攻击是基础操作，如何通过魔法打出暴击呢？

常用工具箱

成熟的CTFer要学会巧用github不重复造轮子。

> 案例一：
> 超仔细观察的小A发现了一个SSRF漏洞！
> 小A成功找到了内网的redis！
> 接下来要怎么办呢？对了，用gopher造恶意代码提交吧！
> 小A开始造RESP转gopher的轮子……

成熟的CTFer要学会分享PoC不手搓螺旋丸。

> 案例二：
> 超可爱的小A发现了一个3.x版本的linux内核！
> “我知道了！这里应该是脏牛提权，”小A这么说：“我记得CVE-20xx-xxxxx提到了这个问题！”
> 小A开始手撕linux源码试图写出脏牛提权脚本……

成熟的CTFer会使用在线工具。

> 案例三：
> 超聪明的小A发现了一串过于短小的n，他将要表演口算大整数分解获取p和q的值用于打爆RSA。
> 经过7天7夜的复杂计算，小A终于坐上救护车送去总医院……

成熟的CTFer会适当使用伪代码生成和汇编查看器。

> 案例四：
> 超自信的小A找到了一个114.514MB的泄露可执行文件！
> “我要从二进制里找到激活码！我不会买正版的！”
> 小A打开了他的十六进制编辑器，被淹没在汇编代码的汪洋中……
>
> 【X】错误示范！！支持正版

于是，我准备了超完备的基础工具箱：

https://gchq.github.io/CyberChef/（在线加密解密、编码解码套件）

https://www.filesignatures.net/index.php?page=search（文件指纹数据库）

http://www.factordb.com/（在线大整数分解）

http://shell-storm.org/shellcode/（shellcode数据库）

https://www.exploit-db.com/（exploit在线分享）

极客！

永不止步于此，探索。

> To follow the path:
> look to the master,
> follow the master,
> walk with the master,
> see through the master,
> become the master.

开始夺旗吧！

[Misc] Practice Flag

Try inputting the flag: flag{CTFLearn_is_awesome}

`https://ctflearn.com/challenge/125`

[Web] Don't Bump Your Head(er)

Try to bypass my security measure on this site! http://165.227.106.113/header.php

`https://ctflearn.com/challenge/109`

[Forensics] Binwalk

Here is a file with another file hidden inside it. Can you extract it? https://mega.nz/#!qbpUTYiK!-deNdQJxsQS8bTSMxeUOtpEclCI-zpK7tbJiKV0tXYY

`https://ctflearn.com/challenge/108`

[Binary] Lazy Game Challenge

I found an interesting game made by some guy named "John_123". It is some betting game. I made some small fixes to the game; see if you can still pwn this and steal $1000000 from me!

To get flag, pwn the server at: `nc thekidofarcrania.com 10001`

`https://ctflearn.com/challenge/691`

[Reverse Engineering] Basic Android RE 1

A simple APK, reverse engineer the logic, recreate the flag, and submit! https://ctflearn.com/challenge/download/962

`https://ctflearn.com/challenge/962`

[Cryptography] Hextroadinary

Meet ROXy, a coder obsessed with being exclusively the worlds best hacker. She specializes in short cryptic hard to decipher secret codes. The below hex values for example, she did something with them to generate a secret code, can you figure out what? Your answer should start with 0x.

0xc4115 0x4cf8

`https://ctflearn.com/challenge/158`