GUIDE

ALL ABOUT EverCTF

HACK NOT ONLY FOR FUNCTION
BUT FOR FUN

Table of Contents

历史

第一届**EverCTF**

第一届CTF比赛由Ever404安全实验室主办，承办。于2018年7月举行，面向全校本科生开放比赛报名

第二届**EverCTF**

第二届EverCTF比赛是由北京科技大学计通学院主办，Ever404安全实验室承办、命题、运维测试的面向全校本科生的竞赛。作为CTF校内赛暨全国信息安全大赛预选赛。宗旨是提高我校学生的信息安全技术实战能力，以及信息与网络空间安全意识。

赛前准备

比赛注册

在规定的时间进行比赛的注册。一般访问**ever404**官网⇒**http://down.ever404.com**，点击导航栏报名比赛进行注册。

注册时需要填写学号、邮箱、和参赛昵称。

比赛时因为可能会用到各种插件，所以推荐使用**chrome**浏览器和**Firefox**浏览器。

题目类型

CTF比赛通常包含的题目类型包括**MISC**、**PPC**、**CRYPTO**、**PWN**、**REVERSE**、**WEB**、**STEGA**。

MISC(Miscellaneous)类型，即安全杂项，题目或涉及流量分析、电子取证、人肉搜索、数据分析等等。

PPC(Professionally Program Coder)类型，即编程类题目，题目涉及到编程算法，相比**ACM**较为容易。

CRYPTO(Cryptography)类型，即密码学，题目考察各种加解密技术，包括古典加密技术、现代加密技术甚至出题者自创加密技术。

PWN类型，**PWN**在黑客俚语中代表着攻破、取得权限，多为溢出类题目。

REVERSE类型，即逆向工程，题目涉及到软件逆向、破解技术。

逆向：http://reversing.kr/

STEGA(Steganography)类型，即隐写术，题目的**Flag**会隐藏到图片、音频、视频等各类数据载体中供参赛者获取。

WEB类型，即题目会涉及到常见的**Web**漏洞，诸如注入、**XSS**、文件包含、代码执行等漏洞。

XSS：http://xss.pkav.net/xss/ http://xss-quiz.int21h.jp/ http://escape.alf.nu/

SQL注入：http://redtiger.labs.overthewire.org/ https://github.com/Audi-1/sqli-labs

得分

解题模式：大多数为线上比赛，选手自由组队（人数不受限制），出题者把一些信息安全实战中可能遇到的问题抽象成一个题目，比如一个存在漏洞的网站让选手入侵，一个有漏洞的程序让选手分析来写出漏洞利用程序，一段密文让选手解密，一个图片选手你从里面找出隐藏的线索等等。在完成这些出题的题目后，可以获得一串奇怪的字符串，也就是所谓的flag，提交它，就能获得这道题目的分数。

攻防模式：大多数为线下比赛，参赛队伍人数有限制（通常为3到5人不等），参赛队伍保护自己的服务器，攻击其他队伍的服务器，每个队伍的服务器开始拥有相同的配置和缺陷，比如几个有漏洞的二进制程序、有漏洞的Web应用、某些权限账户弱口令等等，然后队员需要找出这些漏洞并进行加固，同时利用这些漏洞来攻击别人的服务器，拿到其他队伍的权限后，会获取到相应flag后提交，从对方身上赚取相应的分数，每隔一段时间后，可以再次攻击并利用未加固的漏洞获取flag并赚取分数。

混合模式：解题模式和攻防模式同时进行，解题模式可能会根据比赛的时间、进度等因素来释放需解答的题目，题目的难度越大，解答完成后获取的分数越高；攻防模式会贯穿整个CTF比赛的始终，参赛队伍需不断积累分数，最终参数队伍的名次由两种模式累积的分数总和决定。有些有趣的CTF比赛，还会引入一些情景剧情和现场观众的互动，来增加比赛的趣味性。

本次**CTF**比赛采用解题模式。

关于资源

CTF在我校刚刚起步

资源尚需一步步积累。我们所拥有的，必将倾囊相予。

校内资源站的使用

资源站网址⇒**http://down.ever404.com**

资源站进去是一个电脑桌面类似的界面，点最上方的文件管理——公共目录

tools是**CTF**工具，已分类

books是各种书籍，编程，算法，安全都有涉及，已分类

iso是系统镜像 **linux**和**mac**都有

others是其他工具

video为视频教程

校内靶场的使用

练习平台网址⇒**http://ctf.ever404.com**

点击**register**注册，注册后点击**login**登录。

在**challenge**里进行做题。

scoreboard里可以看到各队伍的得分。

国内外各大**CTF**靶场平台

网络信息安全攻防学习平台⇒**http://hackinglab.cn/**

ctf题目⇒**http://captf.com/**

XCTF_OJ练习平台⇒**http://oj.xctf.org.cn/**

Jlu.CTF⇒**http://ctf.3sec.cn/**

i春秋**ctf**挑战⇒**http://www.ichunqiu.com/tiaozhans**

IDF实验室⇒**http://ctf.idf.cn/**

米安网**ctf**⇒**http://ctf.moonsos.com/pentest**

合天**ctf**⇒**http://www.hetianlab.com/CTFrace.html**

实验吧⇒**http://www.shiyanbar.com/ctf/**

BCTF复盘⇒**<https://bctf.cn/#/challenge>**

奖励政策

奖金与创新学分

根据北京科技大学《学生守则》，本次**CTF**比赛属于校级学科竞赛，相关奖励如下：

竞赛类别	一等奖或特等奖	二等奖	三等奖
国家级/国际级	1000	800	500
省市级	500	300	200
校级	200	100	50