CTF学习规划————1、如何入门CTF

原创

FLy_鹏程万里 于 2018-05-16 11:37:54 发布
分类专栏： 【CTF】# CTF基础

本文链接：https://blog.csdn.net/Fly_hps/article/details/79783253


【CTF】同时被 2 个专栏收录
30 篇文章 26 订阅
订阅专栏


CTF基础
4 篇文章 4 订阅
订阅专栏

无意中发现了一个巨牛巨牛的人工智能教程，忍不住分享一下给大家。教程不仅是零基础，通俗易懂，小白也能学，而且非常风趣幽默，还时不时有内涵段子，像看小说一样，哈哈～我正在学习中，觉得太牛了，所以分享给大家。点这里可以跳转到教程！

CTF简介

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全球黑客大会，以代替之前黑客们通过互相发起真实攻击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，2013年全球举办了超过五十场国际性CTF赛事。而DEFCON作为CTF赛制的发源地，DEFCON CTF也成为了目前全球最高技术水平和影响力的CTF竞赛，类似于CTF赛场中的“世界杯”。

CTF竞赛模式

（1）解题模式（Jeopardy）在解题模式CTF赛制中，参赛队伍可以通过互联网或者现场网络参与，这种模式的CTF竞赛与ACM编程竞赛、信息学奥赛比较类似，以解决网络安全技术挑战题目的分值和时间来排名，通常用于在线选拔赛。题目主要包含逆向、漏洞挖掘与利用、Web渗透、密码、取证、隐写、安全编程等类别。
（2）攻防模式（Attack-Defense）在攻防模式CTF赛制中，参赛队伍在网络空间互相进行攻击和防守，挖掘网络服务漏洞并攻击对手服务来得分，修补自身服务漏洞进行防御来避免丢分。攻防模式CTF赛制可以实时通过得分反映出比赛情况，最终也以得分直接分出胜负，是一种竞争激烈，具有很强观赏性和高度透明性的网络安全赛制。在这种赛制中，不仅仅是比参赛队员的智力和技术，也比体力（因为比赛一般都会持续48小时及以上），同时也比团队之间的分工配合与合作。
（3）混合模式（Mix）结合了解题模式与攻防模式的CTF赛制，比如参赛队伍通过解题可以获取一些初始分数，然后通过攻防对抗进行得分增减的零和游戏，最终以得分高低分出胜负。采用混合模式CTF赛制的典型代表如iCTF国际CTF竞赛。

CTF各大题型简介

MISC（安全杂项）：全称Miscellaneous。题目涉及流量分析、电子取证、人肉搜索、数据分析、大数据统计等等，覆盖面比较广。我们平时看到的社工类题目；给你一个流量包让你分析的题目；取证分析题目，都属于这类题目。主要考查参赛选手的各种基础综合知识，考察范围比较广。

PPC（编程类）：全称Professionally Program Coder。题目涉及到程序编写、编程算法实现。算法的逆向编写，批量处理等，有时候用编程去处理问题，会方便的多。当然PPC相比ACM来说，还是较为容易的。至于编程语言嘛，推荐使用Python来尝试。这部分主要考察选手的快速编程能力。

CRYPTO（密码学）：全称Cryptography。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。实验吧“角斗场”中，这样的题目汇集的最多。这部分主要考查参赛选手密码学相关知识点。

REVERSE（逆向）：全称reverse。题目涉及到软件逆向、破解技术等，要求有较强的反汇编、反编译扎实功底。需要掌握汇编，堆栈、寄存器方面的知识。有好的逻辑思维能力。主要考查参赛选手的逆向分析能力。此类题目也是线下比赛的考察重点。

STEGA（隐写）：全称Steganography。隐写术是我开始接触CTF觉得比较神奇的一类，知道这个东西的时候感觉好神奇啊，黑客们真是聪明。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选手获取。载体就是图片、音频、视频等，可能是修改了这些载体来隐藏flag，也可能将flag隐藏在这些载体的二进制空白位置。有时候需要你侦探精神足够的强，才能发现。此类题目主要考查参赛选手的对各种隐写工具、隐写算法的熟悉程度。实验吧“角斗场”的隐写题目在我看来是比较全的，以上说到的都有涵盖。新手盆友们可以去了解下。

PWN（溢出）：PWN在黑客俚语中代表着攻破，取得权限，在CTF比赛中它代表着溢出类的题目，其中常见类型溢出漏洞有栈溢出、堆溢出。在CTF比赛中，线上比赛会有，但是比例不会太重，进入线下比赛，逆向和溢出则是战队实力的关键。主要考察参数选手漏洞挖掘和利用能力。

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。

学之前的思考：分析赛题情况

PWN、Reserve偏重对**汇编、逆向**的理解

Crypto偏重对**数学、算法**的深入学习

Web编程对**技巧沉淀、快速搜索**能力的挑战

Misc则更为复杂，所有**与计算机安全挑战有关**的都算在其中

常规做法

A方向：PWN+Reserver+Crypto随机搭配

B方向：Web+Misc组合

其实Misc所有人都可以做

恶补基础知识&信息安全专业知识

推荐图书：

A方向：

RE for Beginners（逆向工程入门）

IDA Pro权威指南

揭秘家庭路由器0day漏洞挖掘技术

自己动手写操作系统

黑客攻防宝典：系统实战篇

B方向：

Web应用安全权威指南

Web前端黑客技术揭秘

黑客秘籍——渗透测试使用指南

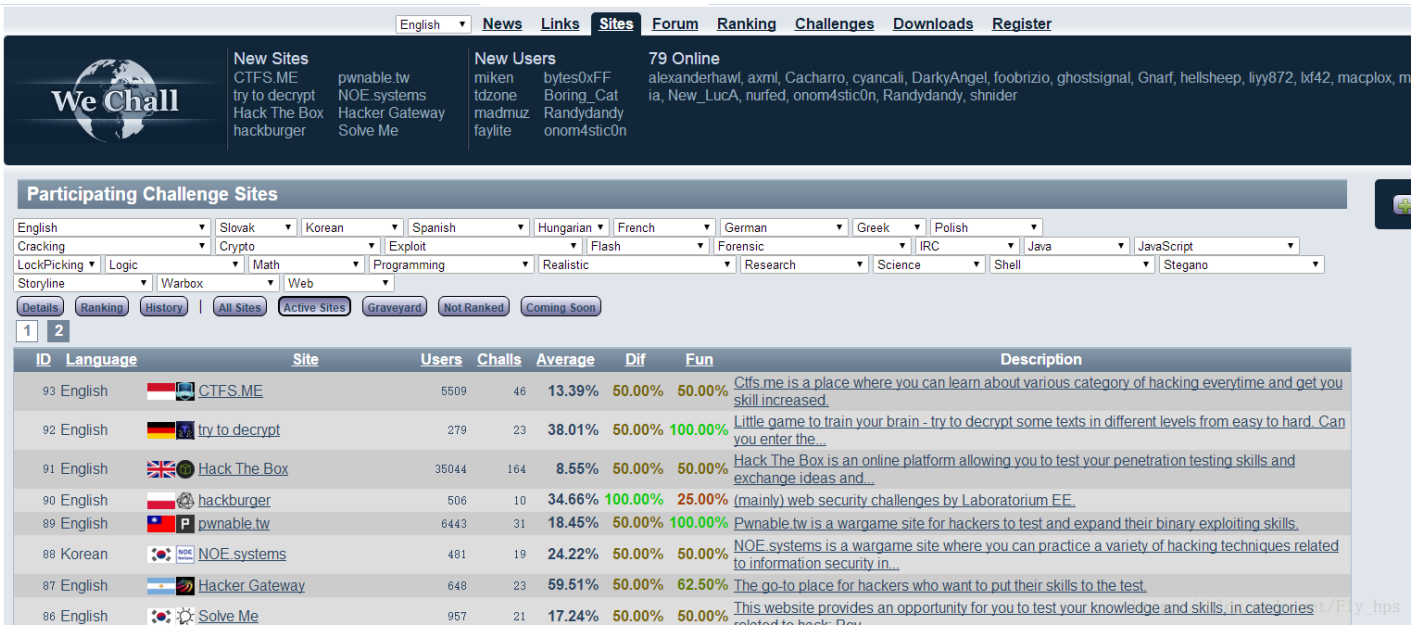
黑客攻防宝典WEB实战篇

代码审计：企业级Web代码安全架构

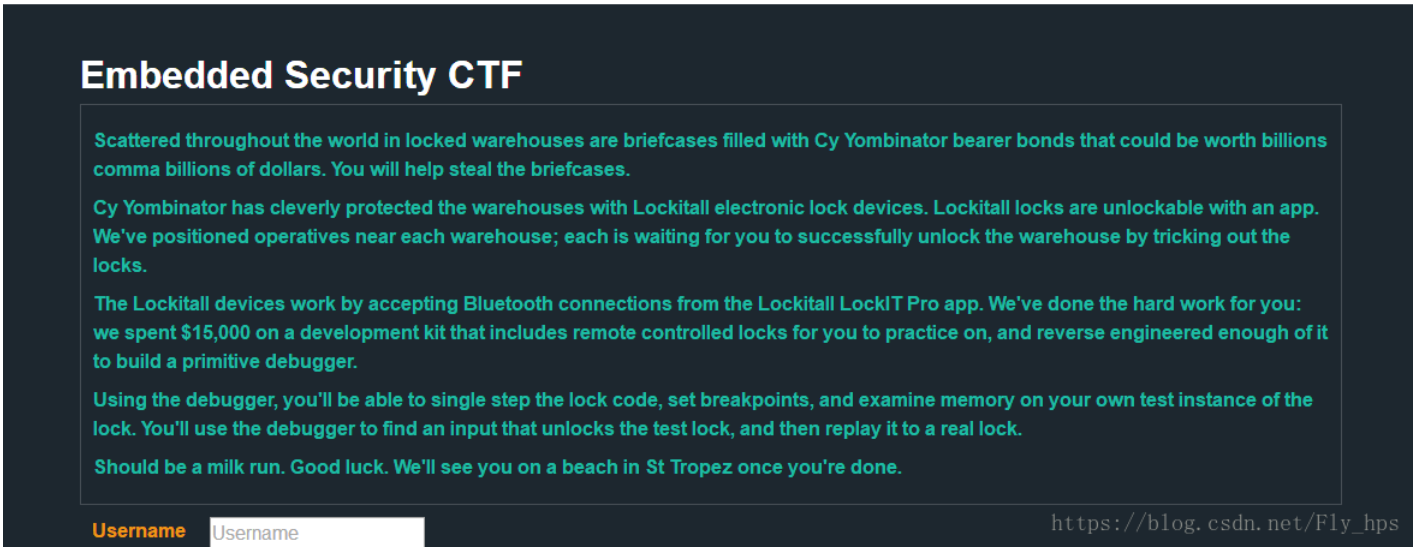
从基础题目出发

i春秋训练平台：https://www.ichunqiu.com/battalion

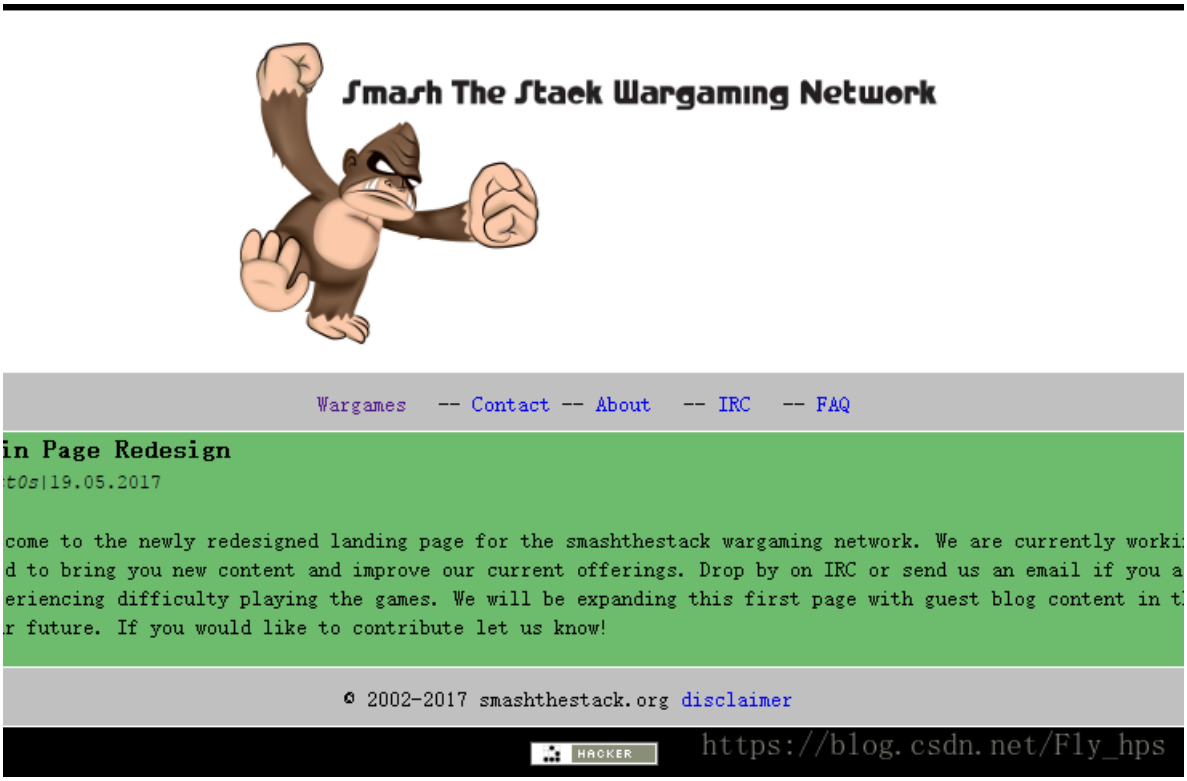
We Chall: http://www.wechall.net/sites.php



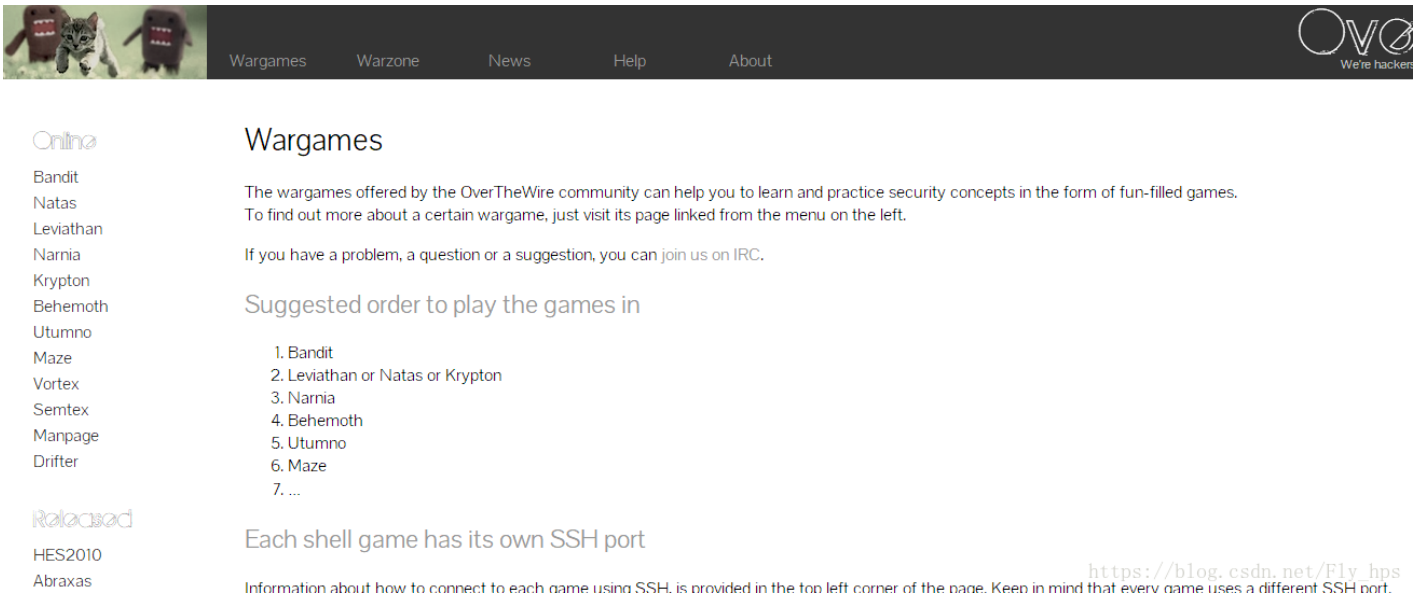
很炫酷游戏化————https://microcorruption.com/login



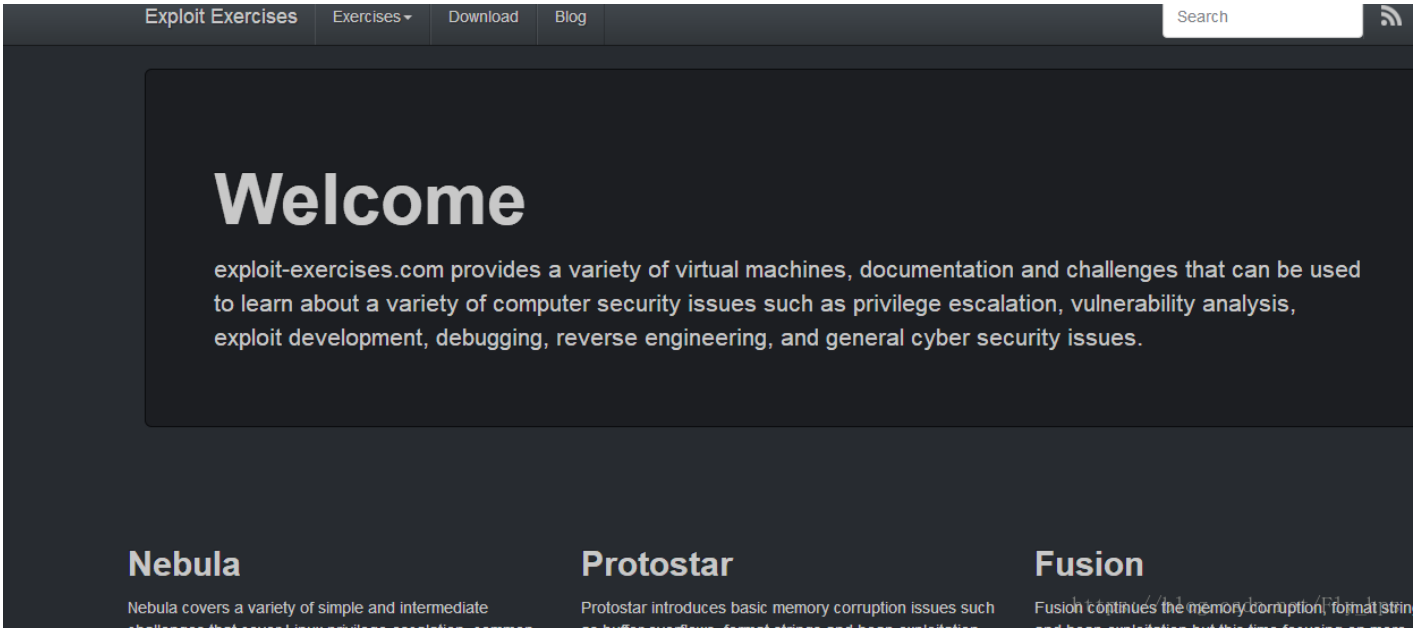
http://smashthestack.org/



http://overthewire.org/wargames/



https://exploit-exercises.com/（**A方向**）



工具集：

https://github.com/P1kachu/v0lt

https://github.com/truongkma/ctf-tools

https://github.com/zardus/ctf-tools