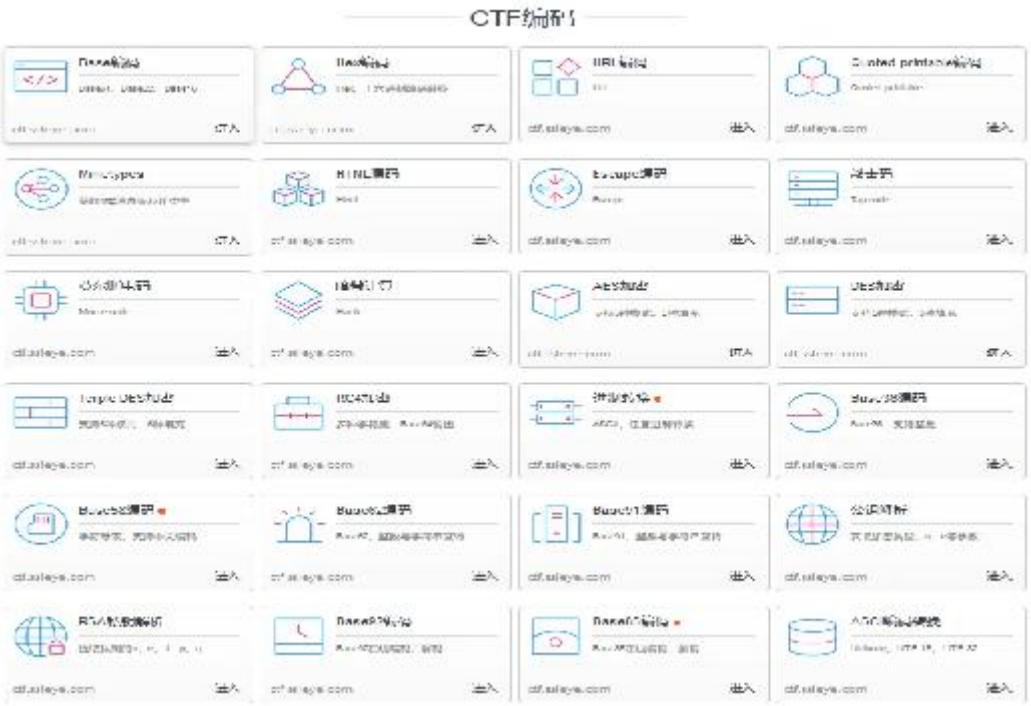
网络安CTF学习资源整理

对于想学习或者参加 CTF 比赛的朋友来说，CTF 工具、练习靶场必不可少，今天给大家分享自己收藏的 CTF 资源，希望能对各位有所帮助。

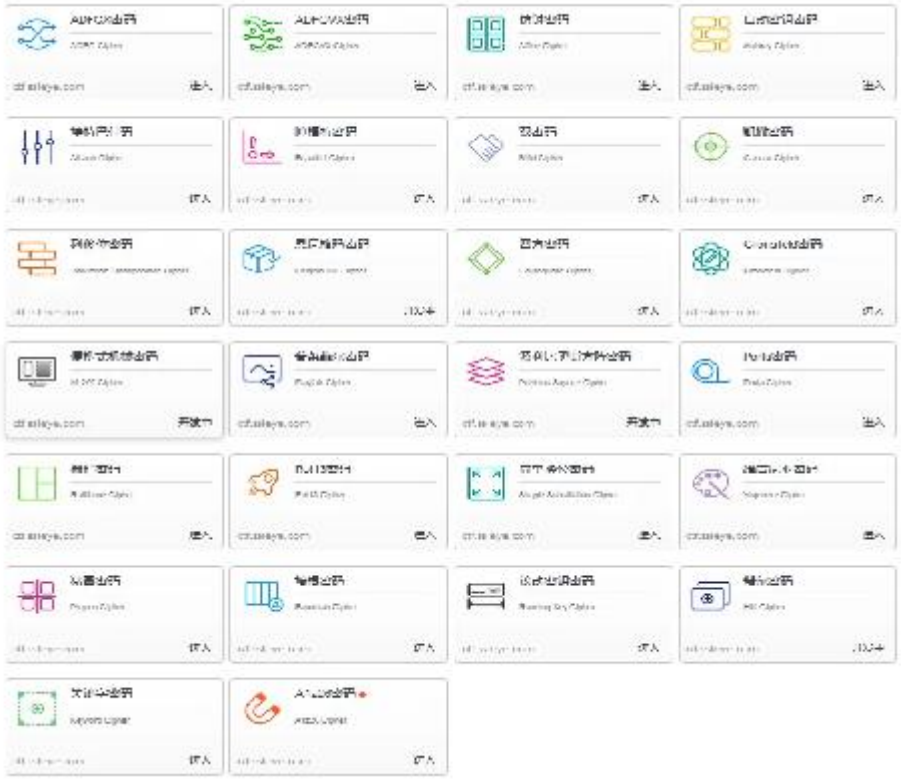
CTF 在线工具

首先给大家推荐我自己常用的 3 个 CTF 在线工具网站，内容齐全，收藏备用。

1、CTF 在线工具箱：http://ctf.ssleye.com/　包含 CTF 比赛中常用的编码、加解密、算法。



CTF算法

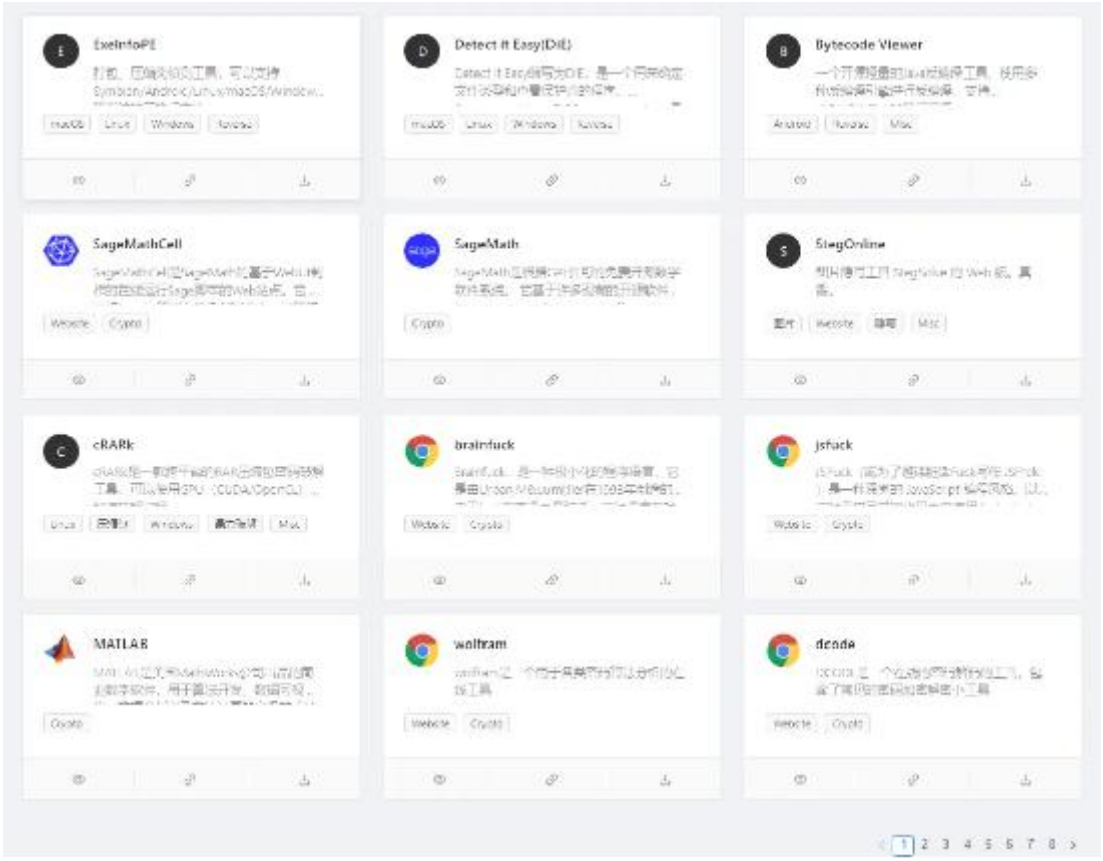


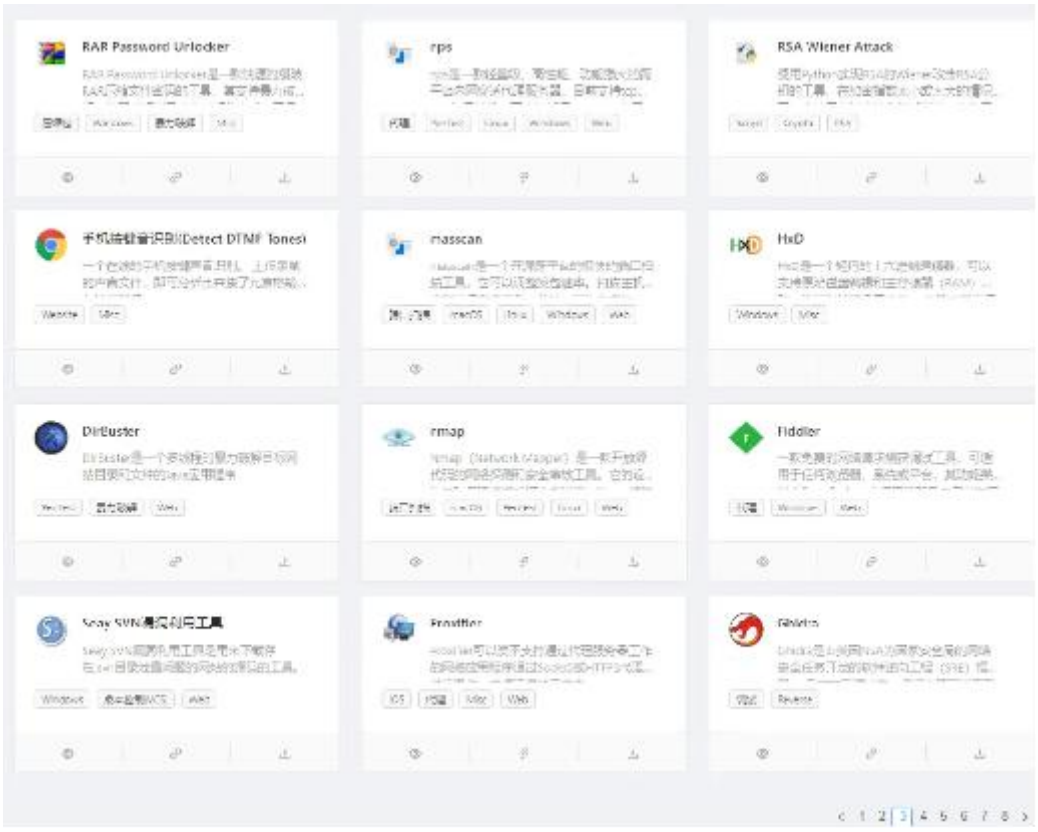
CTF杂项

2、CTF 加解密工具箱：

http://www.atoolbox.net/Category.php?Id=27

3、ctfhub 在线工具：https://www.ctfhub.com/#/tools





4、还有一些常用的网站

字符串 2 进制互转：http://www.5ixuexiwang.com/str/from-binary.php 栅栏密码：http://www.practicalcryptography.com/ciphers/classical-era/rail-fence/语言加密(将明文加密为各种语言)：https://www.qqxiuzi.cn/bianma/wenbenjiami.php 与佛论禅：https://www.keyfc.net/bbs/tools/tudoucode.aspx 维吉尼亚解密：https://www.guballa.de/vigenere-solver 培根密码：https://mothereff.in/bacon 摩尔斯电码：http://www.zhongguosou.com/zonghe/moErSiCodeConverter.aspx 盲文在线解密：https://www.dcode.fr/braille-alphabet 凯撒密码：https://www.dcode.fr/caesar-cipher 进制转换：https://tool.oschina.net/hexconvert/词频分析：https://quipqiup.com/草料二维码：https://cli.im/UUencode：http://web.chacuo.net/charsetuuencodeURL 编码解码：https://meyerweb.com/eric/tools/dencoder/Serpent 加密解密：http://serpent.online-domain-tools.com/ROT 编码(5 13 18 47)：https://www.qqxiuzi.cn/bianma/ROT5-13-18-47.phpMIME 编码：https://dogmamix.com/MimeHeadersDecoder/MD5：https://www.cmd5.com/JS 加密：https://tool.lu/js/JSfuck：https://utf-8.jp/public/jsfuck.htmlJJencode：https://www.120muban.com/tools/jjencode/CRC32：https://crc32generator.de/代码在线运行：https://tool.lu/coderunner/Base 编码解码：http://ctf.ssleye.com/AES 解密：http://tool.chacuo.net/cryptaesADFGVX 密码：http://www.atoolbox.net/Tool.php?Id=917AAencode：https://utf-8.jp/public/aaencode.html

CTF 赛事篇

i 春秋和 XCTF 社区经常会发布各类 CTF 赛事

i 春秋: https://www.ichunqiu.com/competition

XCTF 社区：https://time.xctf.org.cn

CTFwiki（入门必看 wiki）：

https://ctf-wiki.github.io/ctf-wiki/#/introduction

CTFrank: https://ctfrank.org/

CTFtime（基本都是国外的）：https://ctftime.org

公众号：网络安全实验室，国内外 CTF 比赛时间发布，各种 CTF 常用工具

网络安全实验室

专注于网络安全领域，包括安全岗位招聘、红蓝队建设、实战攻防、内网渗透、社工、CTF 比赛、安全技术分享等。

靶场篇

1、在线靶场

BugKu（简单，推荐新手入门，还有在线工具）

https://ctf.bugku.com/index.html

北京联合大学 BUUCTF（新靶场，难度中上，搜集了很多大赛原题）
https://buuoj.cn/

CTFhub 靶场（含历年赛题） https://www.ctfhub.com/#/index

CTFshow 靶场（题较多） https://ctf.show/challenges

网络攻防世界（挺好的网站，不过老是维护） https://adworld.xctf.org.cn/

CTFwiki（含 CTF 各项知识点，扫盲专用）
https://ctf-wiki.org/misc/recon/

BUUCTF（推荐，但不适合新手）https://buuoj.cn/

i 春秋（推荐，还有漏洞复现环境）

https://www.ichunqiu.com/competition

xctf（知名）https://adworld.xctf.org.cn/

浙大 OJ（pwn 手入门推荐）https://www.jarvisoj.com/

2、自己搭建靶场

- **SQLI-LABS 专有靶场**

  包含了大多数的 sql 注入类型，以一种闯关模式，对于 sql 注入进行漏洞利用　　下载地址 https://github.com/Audi-1/sqli-labs

- **DVWA 专有靶场**

  推荐新手首选靶场，DVWA 的目的是通过简单易用的界面来实践一些最常见的 Web 漏洞，这些漏洞具有不同的难度，是一个涵盖了多种漏洞一个综合的靶机 https://github.com/ethicalhack3r/DVWA

- **OWASP 靶场**靶场由 OWASP 专门为 Web 安全研究者和初学者开发的一个靶场，包含了大量存在已知安全漏洞的训练实验环境和真实 Web 应用程序；

  靶场在官网下载后是一个集成虚拟机，可以直接在 vm 中打开，物理机访问 ip 即可访问到 web 平台，使用 root owaspbwa 登入就会返回靶场地址，直接可以访问靶场。dvwa 适合了解漏洞和简单的漏洞利用，owaspbwa 则就更贴近实际的复杂的业务环境。下载地址：https://sourceforge.net/projects/

- DSVW 靶场

- Damn Small Vulnerable Web (DSVW) 是使用 Python 语言开发的 Web 应用漏洞的演练系统。其系统只有一个 python 的脚本文件组成，当中涵盖了 26 种 Web 应用漏洞环境，并且脚本代码行数控制在了 100 行以内，当前版本 v0.1m。需要 python (2.6.x 或 2.7)并且得安装 lxml 库。下载地址：git clone https://github.com/stamparm/DSVW.git

- WebGoat 靶场

- WebGoat 是 OWASP 组织研制出的用于进行 web 漏洞实验的 Java 靶场程序，用来说明 web 应用中存在的安全漏洞。WebGoat 运行在带有 java 虚拟机的平台之上，当前提供的训练课程有 30 多个，其中包括：跨站点脚本攻击（XSS）、访问控制、

线程安全、操作隐藏字段、操纵参数、弱会话 cookie、SQL 盲注、数字型 SQL 注入、字符串型 SQL 注入、web 服务、Open Authentication 失效、危险的 HTML 注释等等。WebGoat 提供了一系列 web 安全学习的教程，某些课程也给出了视频演示，指导用户利用这些漏洞进行攻击。GitHub 地址为：
https://github.com/WebGoat/WebGoat

- **XVWA 靶场**

Xtreme Vulnerable Web Application (XVWA) 是一款使用 PHP/MySQL 编写的靶场，可以帮助初学者快速学习安全姿势。

https://github.com/s4n7h0/xvwa

- Pikachu 靶场
- 一个好玩的 Web 安全漏洞测试平台，跟 DVWA 类似，不过看上去比前者清晰（中文的），有简单的漏洞页面，不那么单调。项目地址：github.com/zhuifengshao
- Vulnhub 靶场
- Vulnhub 是一个提供各种漏洞环境的靶场平台，供安全爱好者学习渗透使用，大部分环境是做好的虚拟机镜像文件，镜像预先设计了多种漏洞，需要使用 VMware 或者 VirtualBox 运行。每个镜像会有破解的目标，大多是 Boot2root，从启动虚机到获取操作系统的 root 权限和查看 flag。

下载链接

https://download.vulnhub.com/breach/Breach-1.0.zip

- mutillidaemutillidae
- mutillidaemutillidae 是一个免费，开源的 Web 应用程序，提供专门被允许的安全测试和入侵的 Web 应用程序。它是由 Adrian“Irongeek”Crenshaw 和 Jeremy“webpwnized”Druin.开发的一款自由和开放源码的 Web 应用程序。其中包含了丰富的渗透测试项目，如 SQL 注入、跨站脚本、clickjacking、本地文件包含、远程代码执行等.

链接地址：http://sourceforge.net/projects/mutillidae

- SQLol

SQLol 是一个可配置得 SQL 注入测试平台，它包含了一系列的挑战任务，让你在挑战中测试和学习 SQL 注入语句。此程序在 Austin 黑客会议上由 Spider Labs 发布。

链接地址：https://github.com/SpiderLabs/SQLol

- hackxor

hackxor 是由 albino 开发的一个 online 黑客游戏,亦可以下载安装完整版进行部署,包括常见的 WEB 漏洞演练。包含常见的漏洞 XSS、CSRF、SQL 注入、RCE 等。

链接地址：http://sourceforge.net/projects/hackxor

- BodgeIt

BodgeIt 是一个 Java 编写的脆弱性 WEB 程序。他包含了 XSS、SQL 注入、调试代码、CSRF、不安全的对象应用以及程序逻辑上面的一些问题。Exploit KB

该程序包含了各种存在漏洞的 WEB 应用，可以测试各种 SQL 注入漏洞。此应用程序还包含在 BT5 里

链接地址：http://exploit.co.il/projects/vuln-web-app

- WackoPicko

WackoPicko 是由 Adam Doupé.发布的一个脆弱的 Web 应用程序，用于测试 Web 应用程序漏洞扫描工具。它包含了命令行注射、sessionid

问题、文件包含、参数篡改、sql 注入、xss、flash form 反射性 xss、弱口令扫描等。

链接地址：https://github.com/adamdoupe/WackoPicko

- XSSeducation

  XSSeducation 是由 AJ00200 开发的一套专门测试跨站的程序。里面包含了各种场景的测试。

  链接地址：http://wiki.aj00200.org/wiki/XSSeducation

- Google XSS 游戏

  Google 推出的 XSS 小游戏

  链接地址：https://xss-game.appspot.com/

- **Metasploitable**

  著名的渗透框架 Metasploit 出品方 rapid7 还提供了配置好的环境 Metasploitable，是一个打包好的操作系统虚拟机镜像，使用 VMWare 的格式。可以使用 VMWare Workstation（也可以用免费精简版的 VMWare Player ）“开机”运行。

  链接地址：

  https://information.rapid7.com/metasploitable-download.html

  下载地址：

  http://downloads.metasploit.com/data/metasploitable/metasploitable-linux-2.0.0.zip

- **OWASP Broken Web Applications Project**

跟 Metasploitable 类似，这也是打包好的虚拟机镜像，预装了许多带有漏洞的 Web 应用，有真实世界里的流行网站应用如 Joomla, WordPress 等的历史版本（带公开漏洞），也有 WebGoat, DVWA 等专门用于漏洞测试的模拟环境。

链接地址：https://code.google.com/p/owaspbwa/

- **XCTF_OJ**

XCTF-OJ （X Capture The Flag Online Judge）是由 XCTF 组委会组织开发并面向 XCTF 联赛参赛者提供的网络安全技术对抗赛练习平台。XCTF-OJ 平台将汇集国内外 CTF 网络安全竞赛的真题题库，并支持对部分可获取在线题目交互环境的重现恢复，XCTF 联赛后续赛事在赛后也会把赛题离线文件和在线交互环境汇总至 XCTF-OJ 平台，形成目前全球 CTF 社区唯一一个提供赛题重现复盘练习环境的站点资源。

链接地址:http://oj.xctf.org.cn/

- **PWNABLE.KR**

以上都是网页服务器安全相关的靶场，再推荐一个练习二进制 pwn 的网站：Pwnable.kr。pwnable 这类题目在国外 CTF 较为多见，通常会搭建一个有漏洞（如缓冲区溢出等）的 telnet 服务，给出这个服务后端的二进制可执行文件让答题者逆向，简单一点的会直接给源代码，找出漏洞并编写利用程序后直接攻下目标服务获得答案。这个网站里由简到难列出了许多关卡，现在就上手试试吧。

链接地址：http://pwnable.kr/%3Fp%3Dprobs