

# ctf比赛/学习资源整理，记得收藏！

原创

网络安全研究所 于 2021-05-09 15:52:21 发布 939 收藏 32

文章标签：[编程语言](#) [信息安全](#) [安全](#) [微软](#) [xss](#)

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/zjqxzhj/article/details/116574565>

版权

猛戳  蓝色小字，关注我们！


























最近CTF比赛很多，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编码

 <b>Base编码</b> Base64, Base32, Base16 ctf.ssleye.com <a href="#">进入</a>	 <b>Hex编码</b> Hex, 十六进制编码转换 ctf.ssleye.com <a href="#">进入</a>	 <b>URL编码</b> Url ctf.ssleye.com <a href="#">进入</a>	 <b>Quoted-printable编码</b> Quoted-printable ctf.ssleye.com <a href="#">进入</a>
 <b>Mimetypes</b> 获取http消息头应用类型 ctf.ssleye.com <a href="#">进入</a>	 <b>HTML编码</b> Html ctf.ssleye.com <a href="#">进入</a>	 <b>Escape编码</b> Escape ctf.ssleye.com <a href="#">进入</a>	 <b>敲击码</b> Tap code ctf.ssleye.com <a href="#">进入</a>
 <b>莫尔斯电码</b> Morse code ctf.ssleye.com <a href="#">进入</a>	 <b>哈希计算</b> Hash ctf.ssleye.com <a href="#">进入</a>	 <b>AES加密</b> 支持5种模式, 5种填充 ctf.ssleye.com <a href="#">进入</a>	 <b>DES加密</b> 支持5种模式, 5种填充 ctf.ssleye.com <a href="#">进入</a>
 <b>Triple DES加密</b> 支持5种模式, 5种填充 ctf.ssleye.com <a href="#">进入</a>	 <b>RC4加密</b> 多种字符集, Base64输出 ctf.ssleye.com <a href="#">进入</a>	 <b>进制转换</b> ASCII, 任意进制转换 ctf.ssleye.com <a href="#">进入</a>	 <b>Base36编码</b> Base36, 支持整数 ctf.ssleye.com <a href="#">进入</a>
 <b>Base58编码</b> 字符表, 支持中文编码 ctf.ssleye.com <a href="#">进入</a>	 <b>Base62编码</b> Base62, 整数与字符串互转 ctf.ssleye.com <a href="#">进入</a>	 <b>Base91编码</b> Base91, 整数与字符串互转 ctf.ssleye.com <a href="#">进入</a>	 <b>公钥解析</b> 获取加密类型, n, e等参数 ctf.ssleye.com <a href="#">进入</a>
 <b>RSA私钥解析</b> 提取私钥的n, e, d, p, q ctf.ssleye.com <a href="#">进入</a>	 <b>Base92编码</b> Base92在线编码、解码 ctf.ssleye.com <a href="#">进入</a>	 <b>Base85编码</b> Base85在线编码、解码 ctf.ssleye.com <a href="#">进入</a>	 <b>ASCII编码转换</b> Unicode, UTF-16, UTF-32 ctf.ssleye.com <a href="#">进入</a>

# CTF算法


















 <p><b>ADFGX密码</b> ADFG Cipher</p> <p>ctf.ssleye.com <a href="#">进入</a></p>	 <p><b>ADFGVX密码</b> ADFGVX Cipher</p> <p>ctf.ssleye.com <a href="#">进入</a></p>	 <p><b>仿射密码</b> Affine Cipher</p> <p>ctf.ssleye.com <a href="#">进入</a></p>	 <p><b>自动密钥密码</b> Autokey Cipher</p> <p>ctf.ssleye.com <a href="#">进入</a></p>
 <p><b>埃特巴什码</b> Atbash Cipher</p> <p>ctf.ssleye.com <a href="#">进入</a></p>	 <p><b>博福特密码</b> Beaufort Cipher</p> <p>ctf.ssleye.com <a href="#">进入</a></p>	 <p><b>双密码</b> Bifid Cipher</p> <p>ctf.ssleye.com <a href="#">进入</a></p>	 <p><b>凯撒密码</b> Caesar Cipher</p> <p>ctf.ssleye.com <a href="#">进入</a></p>
 <p><b>列移位密码</b> Columnar Transposition Cipher</p> <p>ctf.ssleye.com <a href="#">进入</a></p>	 <p><b>恩尼格玛密码</b> Enigma M3 Cipher</p> <p>ctf.ssleye.com <a href="#">开发中</a></p>	 <p><b>四方密码</b> Foursquare Cipher</p> <p>ctf.ssleye.com <a href="#">进入</a></p>	 <p><b>Gronsfeld密码</b> Gronsfeld Cipher</p> <p>ctf.ssleye.com <a href="#">进入</a></p>
 <p><b>便携式机械密码</b> M-209 Cipher</p> <p>ctf.ssleye.com <a href="#">开发中</a></p>	 <p><b>普莱菲尔密码</b> Playfair Cipher</p> <p>ctf.ssleye.com <a href="#">进入</a></p>	 <p><b>波利比奥斯方阵密码</b> Polybius Square Cipher</p> <p>ctf.ssleye.com <a href="#">开发中</a></p>	 <p><b>Porta密码</b> Porta Cipher</p> <p>ctf.ssleye.com <a href="#">进入</a></p>
 <p><b>栅栏密码</b> Railfence Cipher</p> <p>ctf.ssleye.com <a href="#">进入</a></p>	 <p><b>Rot13密码</b> Rot13 Cipher</p> <p>ctf.ssleye.com <a href="#">进入</a></p>	 <p><b>简单换位密码</b> Simple Substitution Cipher</p> <p>ctf.ssleye.com <a href="#">进入</a></p>	 <p><b>维吉尼亚密码</b> Vigenere Cipher</p> <p>ctf.ssleye.com <a href="#">进入</a></p>
 <p><b>猪圈密码</b> Pigpen Cipher</p> <p>ctf.ssleye.com <a href="#">进入</a></p>	 <p><b>培根密码</b> Baconian Cipher</p> <p>ctf.ssleye.com <a href="#">进入</a></p>	 <p><b>滚动密钥密码</b> Running Key Cipher</p> <p>ctf.ssleye.com <a href="#">进入</a></p>	 <p><b>希尔密码</b> Hill Cipher</p> <p>ctf.ssleye.com <a href="#">开发中</a></p>
 <p><b>关键字密码</b> Keyword Cipher</p> <p>ctf.ssleye.com <a href="#">进入</a></p>	 <p><b>A1z26密码</b> A1z26 Cipher</p> <p>ctf.ssleye.com <a href="#">进入</a></p>		

## CTF杂项

 <b>XXencode</b> XXencode ctf.ssleye.com <span>进入</span>	 <b>UUencode</b> UUencode ctf.ssleye.com <span>进入</span>	 <b>PPencode</b> PPencode ctf.ssleye.com <span>进入</span>	 <b>AAencode</b> AAencode ctf.ssleye.com <span>进入</span>
 <b>JJencode</b> JJencode ctf.ssleye.com <span>进入</span>	 <b>核心价值观编码</b> 社会主义核心价值观，学习一下 ctf.ssleye.com <span>进入</span>	 <b>JSfuck</b> JSfuck，玩一下 ctf.ssleye.com <span>进入</span>	 <b>Brainfuck</b> Brainfuck，玩一下 ctf.ssleye.com <span>进入</span>
 <b>BubbleBabble</b> BubbleBabble ctf.ssleye.com <span>进入</span>	 <b>Handycode</b> Handycode ctf.ssleye.com <span>进入</span>	 <b>Punycode</b> Punycode ctf.ssleye.com <span>进入</span>	 <b>Poemcode</b> Poemcode ctf.ssleye.com <span>开发中</span>
 <b>WebSocket测试</b> WebSocket链路测试，发送数据 ctf.ssleye.com <span>进入</span>	 <b>HTTP(S)响应头查看</b> 查看请求的响应头信息 ctf.ssleye.com <span>进入</span>		

2、CTF加解密工具箱：<http://www.atoolbox.net/Category.php?id=27>

### 加密解密

 Base64 Base64编码/解密	 Base7 Base7编码/解密	 Base100 Base100编码/解密	 Base91 Base91编码/解密	 Base85 Base85编码/解密	 Base62 Base62编码/解密
 Base58 Base58编码/解密	 Base32 Base32编码/解密	 Base16 Base16编码/解密	 随机密码和密钥生成器	 自动密钥加密/解密	 同音替代密码加密/解密
 ADFGX ADFGX密码加密/解密	 ADFGVX ADFGVX密码加密/解密	 A1Z26 A1Z26密码加密/解密	 密码本密码加密/解密	 希尔密码加密/解密	 波利比奥斯方阵密码加密/解密

## 加密解密



首页 上一页 1 2 3 下一页 尾页

## 加密解密



首页 上一页 1 2 3 下一页 尾页

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

E

### ExelInfoPE

打包、压缩壳检测工具，可以支持 Symbian/Android/Linux/macOS/Window...

macOS Linux Windows Reverse

👁️ 🔗 ⬇️

D

### Detect it Easy(DIE)

Detect It Easy缩写为DIE，是一个用来确定文件类型和查看保护壳的程序。...

macOS Linux Windows Reverse

👁️ 🔗 ⬇️

B

### Bytecode Viewer

一个开源轻量级的Java反编译工具，使用多种反编译引擎进行反编译，支持...

Android Reverse Misc

👁️ 🔗 ⬇️



### SageMathCell

SageMathCell是SageMath的基于WebUI制作的在线运行Sage脚本的Web站点。它...

Website Crypto

👁️ 🔗 ⬇️



### SageMath

SageMath是根据GPL许可的免费开源数学软件系统。它基于许多现有的开源软件...

Crypto

👁️ 🔗 ⬇️

S

### StegOnline

图片隐写工具 StegSolve 的 Web 版。真香。

图片 Website 隐写 Misc

👁️ 🔗 ⬇️

C

### cRARK

cRARK是一款跨平台的RAR压缩包密码破解工具，可以使用GPU (CUDA/OpenCL) ...

Linux 压缩包 Windows 暴力破解 Misc

👁️ 🔗 ⬇️



### brainfuck

Brainfuck，是一种极小化的编程语言，它是由Urban M&uuml;ller在1993年创造的...

Website Crypto

👁️ 🔗 ⬇️



### jsfuck

JSFuck (或为了避开脏话Fuck写作JSF\*ck) 是一种深奥的JavaScript编程风格。以...

Website Crypto

👁️ 🔗 ⬇️



### MATLAB

MATLAB是美国MathWorks公司出品的商业数学软件，用于算法开发、数据可视...

Crypto

👁️ 🔗 ⬇️



### wolfram

wolfram是一个用于各类密码算法分析的在线工具

Website Crypto

👁️ 🔗 ⬇️

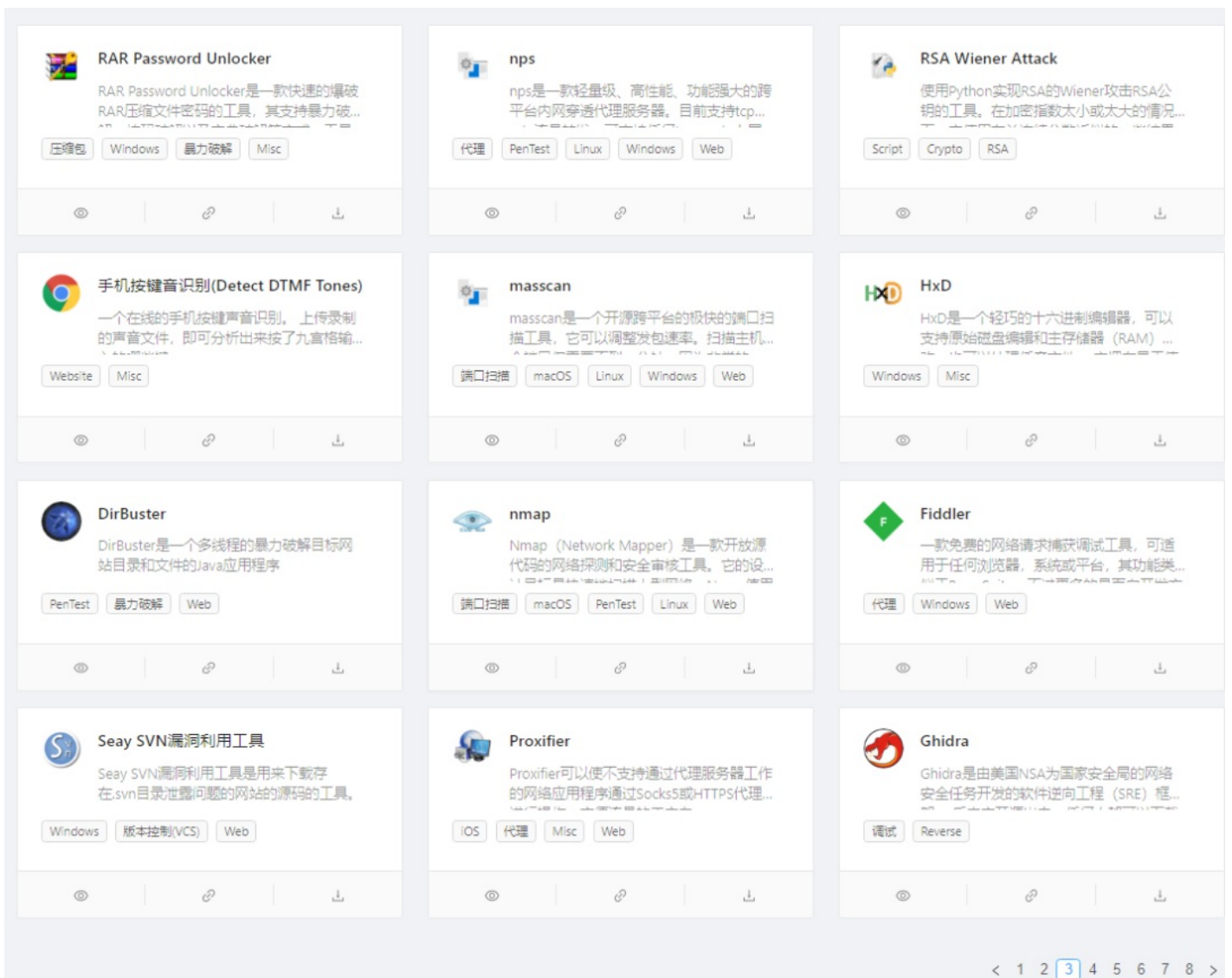


### dcode

DCODE是一个在线的密码解码的工具，包含了常见的密码加密解密小工具

Website Crypto

👁️ 🔗 ⬇️



#### 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/charsetuencode>

URL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.php>

MIME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.html>

JJencode: <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/cryptaes>

ADFGVX密码: <http://www.atoolbox.net/Tool.php?id=917>

AAencode: <https://utf-8.jp/public/aaencode.html>

## 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>

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](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](https://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，从启动虚拟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>

如果觉得有用，记得关注公众号、收藏文章哦！

往期招聘

---

网络安全，有编制，省委直属单位招聘

安全招聘——深信服安全岗位校园招聘

[安全招聘——启明星辰安全岗位社会招聘](#)

[安全招聘——奇安信安全岗位招聘，大专可报](#)

[安全招聘——亚信安全岗位招聘，学历不限](#)

[安全招聘——绿盟科技安全岗位社会招聘，大专可报](#)

[大型央企招人！全国有岗！工资过万！六险二金！](#)

[安全招聘——拼多多安全岗位社会招聘](#)

[安恒信息社会招聘](#)

[想进安全大厂么！快来看面试题及经验](#)

## BugKu CTF

---

[BugKu CTF\(杂项篇MISC\)—想要种子吗](#)

[BugKu CTF\(杂项篇MISC\)—社工-进阶收集](#)

[BugKu CTF\(杂项篇MISC\)—善用工具](#)

[BugKu CTF\(杂项篇MISC\)—隐写2](#)

[BugKu CTF\(杂项篇MISC\)—只有黑棋的棋盘](#)

[BugKu CTF\(杂项篇MISC\)—隐写](#)

[5月全球CTF比赛时间汇总来了！](#)

[更多CTF比赛信息、writeup请点击公众号菜单栏CTF](#)



END

扫码关注

网络安全研究所

更多精彩等着你



网络安全研究所