

# 一个Ctfer的自白

转载

[aoxiangzhi3576](#) 于 2018-08-04 11:44:00 发布 157 收藏 1

文章标签: [数据库](#) [游戏](#) [网络](#)

原文链接: <http://www.cnblogs.com/RM-Anton/p/9418129.html>

版权

一个巧合的机会,成为了CTF夺旗爱好者,一个ctf小白。从12年开始国内大大小小的CTF比赛我都看过,那会还没有统一叫CTF,都是叫网络攻防赛、信息安全赛之类的,目的就是为了通过技术手段找到最终的key(现在的CTF中叫做flag)。只是到了后来慢慢的可能受到DEFCON CTF的影响国内所有的安全竞赛也统一叫做CTF竞赛了。

国内外比较知名的比赛: XCTF联赛、DEFCON CTF、首都网络安全日

做为CTF小白用户,这四年跳过的坑真心不少。尤其是加密、隐写、逆向破解和web这几个方向的坑,基本是跳一个栽一个。

不过还是靠着:实验吧、决斗场等免费的线上模拟平台,终于成功脱坑,技术也越来越熟练。

在这四年的学习中,我总结了一些值得CTF新手和CTF刚刚入门爱好者,学习的干货。

## 一、首先推荐:常去的【学习交流站点】

实验吧[www.shiyanbar.com/courses](http://www.shiyanbar.com/courses) 安全类实操课程比较全,实验和CTF题库都可以免费学,做公益的平台真心不多见!

CTF领域指南 | IDF实验室 博译有道

百度信息安全吧 有时可以探到一些小道内幕

春秋 安全课程比较多,但能动手实操的少,课程收费有点小贵

XCTFtime 国内CTF联赛查询网站

Modern Binary Exploitation bin 干货区

吾爱破解·2016·安全挑战赛【2016安全挑战赛】

除了线上练习,看大牛们出的那些难解的题目,练手之外,加一些ctf的群(384182116、222359598、517164205),和别的朋友交流解题思路与经验,也是必不可少的,能让自己对CTF的解题思路更加广泛。

## 二、常去的一些ctf的【线上练习平台】

ctf夺旗训练\_CTF训练营 实验吧的决斗场,题库全更新快,基本每题都有WriteUP,免费练习的好地方

网络安全实验室 网络信息安全练习平台,很早的平台,近两年不怎么更新了

index of / ctf题目

梦之光芒/Monyer——Monyer's Little Game 梦之光芒的小游戏

黑客游戏 Let's Hack 习科黑客游戏

Jlu.CTF首页 Jlu.CTF

IDF实验室 CTF训练营 idf 实验室,比较早做CTF训练的平台,现在也不咋维护了

欢迎参加比赛~ 米安网ctf

黑吧安全网-红客闯关游戏 黑吧安全网-红客闯关游戏

<http://202.108.211.5/> 实训竞赛系统

信息安全铁人三项赛官网 训练营的内容很棒,期待早日开放出来

## 三、其他相关,挖洞人员【漏洞平台】

Offensive Security Exploit Database Archive

[www.sebug.org](http://www.sebug.org)

补天 - 企业和白帽子共赢的漏洞响应平台,帮助企业建立SRC,库带计划

SOBUG漏洞悬赏平台

Exploit-ID

CVE -

SecuriTeam.com

Computer Security vulnerabilities and exploits database

SecurityFocus

MARC: Mailing list ARChives

SecurityTracker.com

经常去漏洞平台，可以让你随时了解国内外那些漏洞大事件。也可以尝试着提交一些漏洞，既锻炼技术还有额外奖励。

#### 四、常用【在线类工具】

Objectif SÃcuritÃ 在线LMHASH破解

<https://www.hashkiller.co.uk/> hash破解

How people build software · GitHub 全球知名在线管理开发平台

ASTALAVISTA.BOX.SK 最好的注册码、注册机、序列号搜索引擎

s0ftpr0ject 意大利老站

<http://recover-weblogic-password.appspot.com/> 在线weblogic密文破解

Tools88.com Online Tools 在线VNC密文破<http://www.vpnhunter.com/> 在线查找VPN，mail接口

Mailinator 一次性邮箱

YOPmail: 临时、匿名的免费邮箱地址。 一次性邮箱

#### 五、国内外安全大牛的【个人博客】

Insecure.Org (Fyoderr的个人站点,即Nmap的老家)

georgi 安全专家Guninski的主页，有大量系统漏洞工具具及源代码

<http://blog.gentilkiwi.com/> mimikatz

<https://www.schneier.com/> Bruce,Schneier的博客（专业Blackhat会棍）

<http://an7isec.blogspot.co.il/> "整蛊小黑必备" 博客 发现了WVS8版本远程溢出漏洞

<https://fail0verflow.com/blog/index.html> 一个硬件牛的博客

<https://blog.0x80.org/> 破解过jeep车锁的大牛

<https://www.netspi.com/blog> 对MSSQL渗透有研究的大牛

<http://hakin9.org>

<http://websec.ca/blog> 渗透tips

<http://www.derkeiler.com/>

<http://www.xssed.com/>

<http://adsecurity.org/> 内网渗透、域渗透牛人

<http://securityxploded.com>

<http://www.devtys0.com/blog/> 国外路由器安全大牛

这些国内外大牛的个人博客，是一定要关注的，不管想当职业赛棍，还是仅仅是对ctf感兴趣，从中学些安全技术，这些是最宝贵的经验。

#### 六、最后给大家推荐一些【综合类型网站】

<http://www.blackhat.com/>

<http://shiyandar.com>（线上资源均免费，经常性的举办各种有奖活动）

<http://packetstormsecurity.com> (有大量exploit程序)

<http://www.ussrback.com/> 比较活跃的安全站

<http://www.attrition.org/> 内容全面的安全站（更新至2013年）

<http://www.social-engineer.org/> 社会工程学研究所

<https://www.soldierx.com>

[http://www.windowsecurity.com/\(windowsnetworking.com\)](http://www.windowsecurity.com/(windowsnetworking.com))包含论坛、博客、新闻、工具windowsnetworking.com

<http://www.blackmoreops.com>

<http://www.securitytube.net> 大量视频

发布于 2016-07-26 · 著作权归作者所有

转载于:<https://www.cnblogs.com/RM-Anton/p/9418129.html>