

CTF学习经验分享（Web方向）

原创

Bit0 已于 2022-04-07 17:22:31 修改 3135 收藏 17

文章标签：[web安全](#) [经验分享](#) [网络安全](#)

于 2021-10-11 21:06:21 首次发布

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/Baian_Gu/article/details/120709851

版权

本人Web安全初学者，记录分享一下学习历程，推荐评价仅代表个人观点，不足之处欢迎各位表哥指正.....

CTF基础知识：



分类：[基础知识](#) | [CTFHubEnjoy your's CTF](#)

<https://writeup.ctfhub.com/categories/Skill/%E5%9F%BA%E7%A1%80%E7%9F%A5%E8%AF%86/>

CTFH

这里讲得很全面了，题目类型、比赛模式都有，不了解的话可以看一下~

学习视频：

1. [i春秋渗透测试工程师就业班-基础篇vm和Linux上_视频教程_i春秋_培育信息时代的安全感!](#)

<https://www.ichunqiu.com/course/68627> i春秋出品的渗透测试工程师就业班第一个月的内容，主要讲解了vm虚拟机与Linux系统的使用，Linux与Windows基础命令，计算机网络基础知识以及Web开发的基础方法（HTML，JS，CSS，PHP，Mysql），讲得十分详细，很适合小白补充Web方面的基础知识。（不是广告，讲得确实不错，还免费，不过我没报正式的就业班...太贵了）

2022.04.07更新：现在收费了.....想看的话等等看以后有没有机会白嫖吧

2. [i春秋渗透测试工程师就业班-体验课【渗透测试工程师（体验课）】_实战教学_名师面授_培训认证_i春秋](#)

i春秋致力于Web安全工程师培训，面向零基础想从事Web安全工程师的安全行业求职者；IT从业者转Web安全工程师；对Web安全工程师感兴趣的在校和毕业大学生。i春秋已与百度、360、知道创宇等知名互联网公司取得战略合作，建立长期人才输出渠道，培养互联网行业新贵。

<https://www.ichunqiu.com/train/course/40?i=2> 需要花1元购买，开放了基础篇以外章节的部分课程，讲解了Webshell的使用，sql注入基本手法（报错注入、布尔盲注、时间盲注，但没有联合注入，建议先自学这个），Python爬虫等，都是做CTF题中经常涉及到的技术点，讲得很细，比较适合初学。

3. [涅普计划-ctf入门课涅普计划-ctf入门课_哔哩哔哩_bilibili](#)

涅普计划-ctf入门课涅普计划-ctf入门课_哔哩哔哩_bilibili涅普计划公益活动，每晚七点，课程表在宣传

视频最后。课程附件地址<https://ctf.hzyxxl.com/nep>课程练习题<https://camp.hackingfor.fun/>
<https://www.bilibili.com/video/BV1VA411u7Tg> Nepnep联合战队出品的课程，每个方向都有讲解，Web部分讲得比较好，把大部分题中涉及到的知识点、工具的使用都做了讲解，Misc部分稍微有点乱，但也介绍了很多工具和题型，值得一看。（我只看了这两部分.....

线上靶场：




1. 攻防世界<https://adworld.xctf.org.cn/>

<https://adworld.xctf.org.cn/> xctf出品的靶场，界面炫酷，花里胡哨的挺多（不是贬义），新手练习区的题挺浅显易懂的，适合入门，高手进阶区的题多为比赛真题，站内Writeup质量挺高，表哥们会分享很多自己的思路，很适合参考学习。（我大部分时间都在这刷的）



2. We Chall[WeChall] Challenges <https://www.wechall.net/challs>
逐步递增，据说很多大佬都是从这里刷题成长起来的

国外的靶场，题型比较杂，难度



New Sites

PWN.TN 247CTF
 PromptRiddle Énigmes À Thématiques
 PyDéfis LordofSQLi
 CryptoHack MysteryTwister

New Users

Tateusz his_dudeness
 Yolel z1595303605
 luser marking
 biter001 overrider88

66 Online

Guest, Guest(x46), a0x4dbeddedbabe, asteris, ath0, Deep_Thought, Elius, hassanno, hoaiquoc, IBSONE2017, Ketza, livinskull, lordOric, luochengbie, lxf42, overrider88, planetlane, sifmuna, Yolel, zhukeni

All(153), Audio(4), Coding(14), Cracking(9), Crypto(25), Encoding(11), Exploit(57), Forensics(1), Fun(9), HTTP(10), Image(8), Java(3), Linux(9), Logic(6), Math(5), MySQL(15), PHP(27), Programming(1), Python(1), Realistic(6), Regex(2), Research(7), Shell(2), Simulated(1), Special(8), Stegano(22), Storyline(4), Training(33), Unknown(2), Warchall(11), Windows(1), XSS(2)

All Solved Open

Challenge(s) Overview for Deep_Thought

Score	Title	Author	Solvers	Age	Votes	Difficulty	Education	Fun	Forums
1	Training: Get Sourced	by Gizmore	17462	13y 190d	1629	0.47	1.69	2.12	
1	Training: Stegano I	by Gizmore	12047	13y 89d	800	1.08	2.55	2.56	
1	Training: Crypto - Caesar I	by Gizmore	11411	10y 320d	764	1.19	2.47	2.71	
1	Training: WWW-Robots	by Gizmore	10062	10y 291d	720	1.22	3.51	3.40	
1	Training: ASCII	by Gizmore	11720	10y 204d	758	0.54	1.79	1.62	
1	Encodings: URL	by Gizmore	10607	10y 204d	655	0.80	2.03	2.39	
2	Prime Factory	by ch0wch0w	7304	13y 190d	541	1.99	2.80	3.36	
2	Training: Encodings I	by Gizmore	4815	13y 117d	306	3.32	4.30	3.85	
2	Training: Programming 1	by Gizmore	4734	13y 89d	230	2.88	4.62	4.80	
2	Training: Regex	by Gizmore	2869	11y 35d	293	4.14	6.15	5.14	
2	Training: PHP LFI	by Gizmore	4627	11y 6d	303	2.89	5.20	4.91	
2	PHP 0817	by Gizmore	5728	10y 336d	385	1.59	3.78	3.49	
2	Training: Crypto - Transposition I	by Gizmore	3650	10y 320d	239	2.42	3.30	4.10	
2	Training: Crypto - Substitution I	by Gizmore	2964	10y 320d	175	3.03	3.56	4.30	
2	Training: Crypto - Caesar II	by Gizmore	2388	10y 320d	164	2.93	3.62	4.65	
2	Training: Crypto - Digraphs	by Gizmore	1140	10y 320d	122	4.21	4.38	5.24	
2	Training: MySQL I	by Gizmore	5503	10y 320d	407	2.13	4.16	4.31	
2	Training: MySQL II	by Gizmore	2806	10y 320d	200	4.81	5.98	6.00	


CSDN @Deep_Th0u9ht


3. [Hacker101Home | Hacker101](https://www.hacker101.com/) 朋友推荐的国外靶场，也有视频课（没有字幕，但b站有翻译过的，我还没看），题型主要以Web为主，难度还可以。

LEARN TO HACK

Hacker101 is a free class for web security. Whether you're a programmer with an interest in bug bounties or a seasoned security professional, Hacker101 has something to teach you.

Start Hacking!






Capture the Flag

Put your skills into practice with CTF levels inspired by the real world

Check out CTF



Video Lessons

Learn to hack with our free video lessons, guides, and resources

Explore free classes

CSDN @Deep_Th0u9ht

4. [CTFHub](https://www.ctfhub.com/#/index)

也是朋友推荐的，题目分类比较清晰（在技能树那挨个点进去可以循序渐进的学习），很适合初学，而且查找近期赛程特别方便，赛程表清晰明了。（后悔没有早发现.....

正在进行

2021年湘潭市首届“莲城杯”网... 2021-10-11 10:00

暂无

暂无

暂无

暂无

即将开始

“长安杯”网络安全极客挑战赛... 2021-10-12 08:30

广东省第四届“强网杯”网络安... 2021-10-12 09:00

2021浙江省第二届工业控制网... 2021-10-12 09:00

广东省第四届“强网杯”网络安... 2021-10-13 09:00

近期赛程

2021年10月

周日	周一	周二	周三	周四	周五	周六
下午9时 Tamil CTF 2021						
3日	4日	5日	6日	7日	8日	9日
TSG CTF 2021 Sacramento TastelessCTF 2021 下午3时 RuCTF 20...					上午9时 首届“鹤城” 上午8时 pbctf 202...	上午10时 Digital C...
10日	11日	12日	13日	14日	15日	16日
pbctf 2021 Digital Overdose 2 上午9时 第二届“第... 下午5时 SPbCTF's Student CTF 2021 Q...	上午10时 2021年第...	上午8:30 “长安杯” 上午9时 2021浙江... 上午9时 广东省第...	上午9时 2021年第... 上午9时 广东省第...	上午9时 2021年工...	下午10时 DEADFACE CTF	上午1时 iCTF 上午1:30 Reply Cy... 上午8时 第七届全... 上午9时 ByteCTF 2... 上午9时 “天府杯”2... 上午9时 第五届“强... 下午3时 首届“鹤城...
17日	18日	19日	20日	21日	22日	23日
DEADFACE CTF Reply Cyber Securi... ByteCTF 2021 - 初... “天府杯”2021国际... 第五届“强网杯”全... 首届“鹤城杯”CTF网...	上午9时 2021第二...	上午9时 2021 车辆事故深度调查技能大赛	上午9时 2021 智能网联汽车安全测评技能大赛		下午8时 Collegiate SECTF 下午11时 ASIS CTF Quals 2021	上午8时 Fweefwop... 上午8时 BuckeyeC...
24日	25日	26日	27日	28日	29日	30日
Collegiate SECTF						下午7时 M*CTF 20...

5. [sqli-labs GitHub - Audi-1/sqli-labs: SQLi labs to test error based, Blind boolean based, Time based.](https://github.com/Audi-1/sqli-labs) <https://github.com/Audi-1/sqli-labs> 需要自己搭建的sql注入练习靶场，相当经典了，各种注入技巧都可以练习到，不过自己搭建可能会出问题（可能需要切换PHP版本，我在kali里就没整明白），所以建议在docker中搭建，仅需安装docker后运行

```
sudo docker run -it -d -p 12345:80 acgpiano/sqli-labs
```

再访问127.0.0.1:12345就可以了。

后记

暂时先分享这些，发现更好的学习资源再来补.....目前感觉学习CTF没有什么系统的方法，就是从兴趣入手，对哪方面感兴趣就先学习哪方面，基础知识掌握后就多做题，每弄懂一道不会的题就会多掌握一部分的知识，Web题涉及到的知识很杂，sql注入、源码泄露、文件上传、文件包含、反序列化、Python框架漏洞、命令执行、各种函数的漏洞、各种绕过等等等等...只能自己一点一点积累，如果有兴趣，过程就不会那么枯燥。即使因为环境所迫未来没有机会好好的参加比赛或是拿不到什么名次，我依然相信这过程中学到的技术技巧总会有用武之地。（我们学校完全没有CTF学习的环境与资源，更没有战队，哎...总之，先一起加油吧！