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

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/ CTFHu
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生和毕业大学生。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/

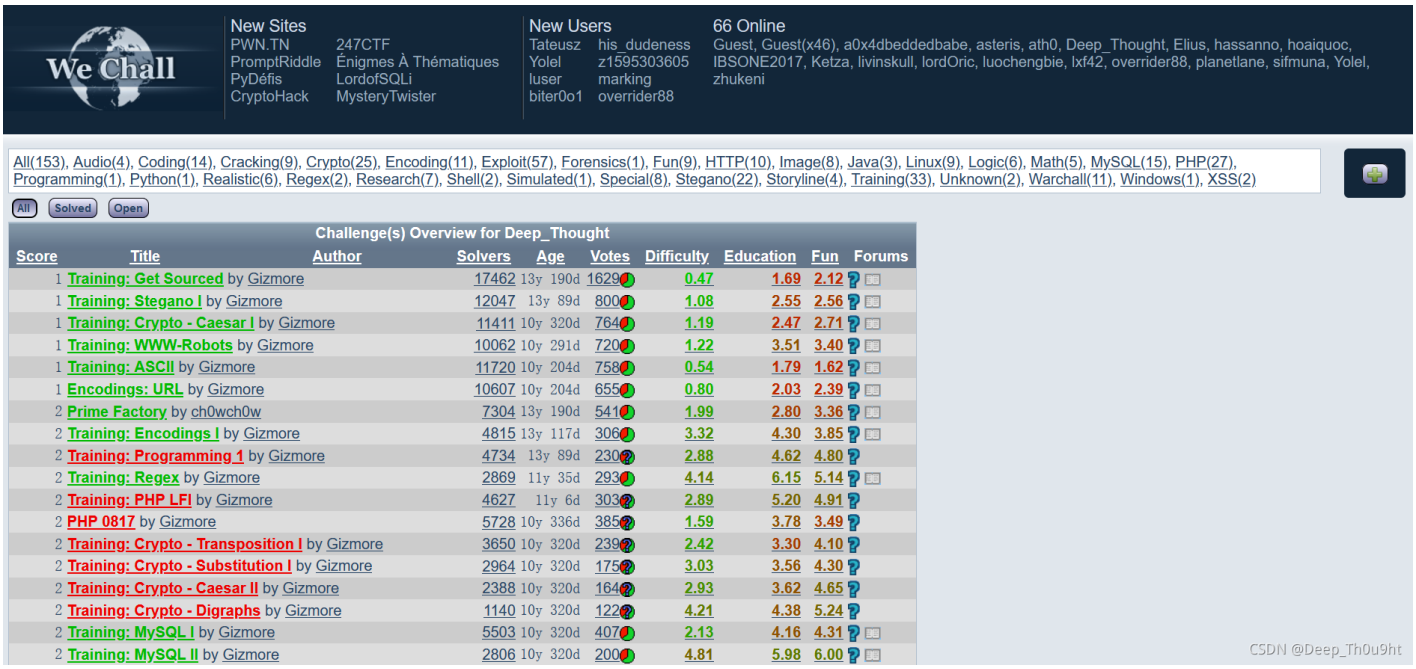
https://www.bilibili.com/video/BV1VA411u7Tg Nepnep联合战队出品的课程，每个方向都有讲解，Web部分讲得比较好，把大部分题中涉及到的知识点、工具的使用都做了讲解，Misc部分稍微有点乱，但也介绍了很多工具和题型，值得一看。（我只看了这两部分……

线上靶场：

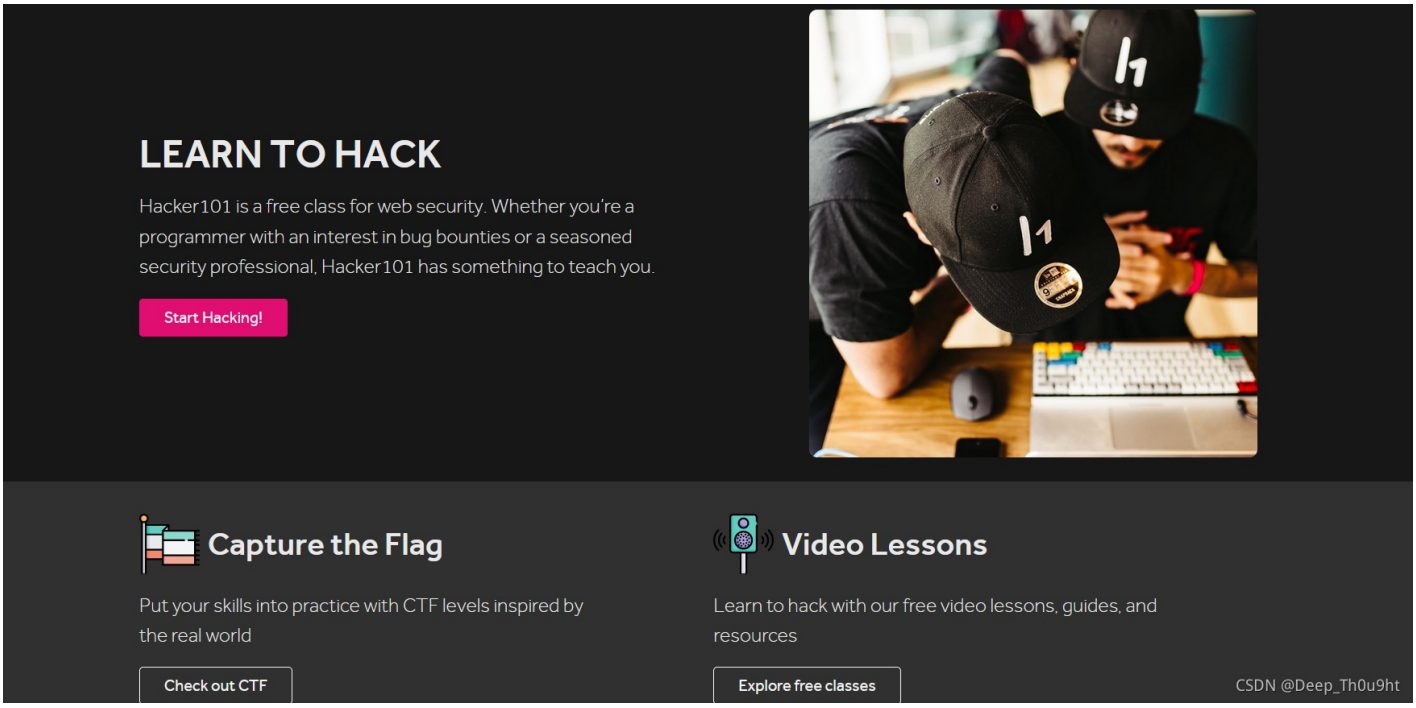
1. 攻防世界https://adworld.xctf.org.cn/

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 国外的靶场，题型比较杂，难度逐步递增，据说很多大佬都是从这刷题成长起来的

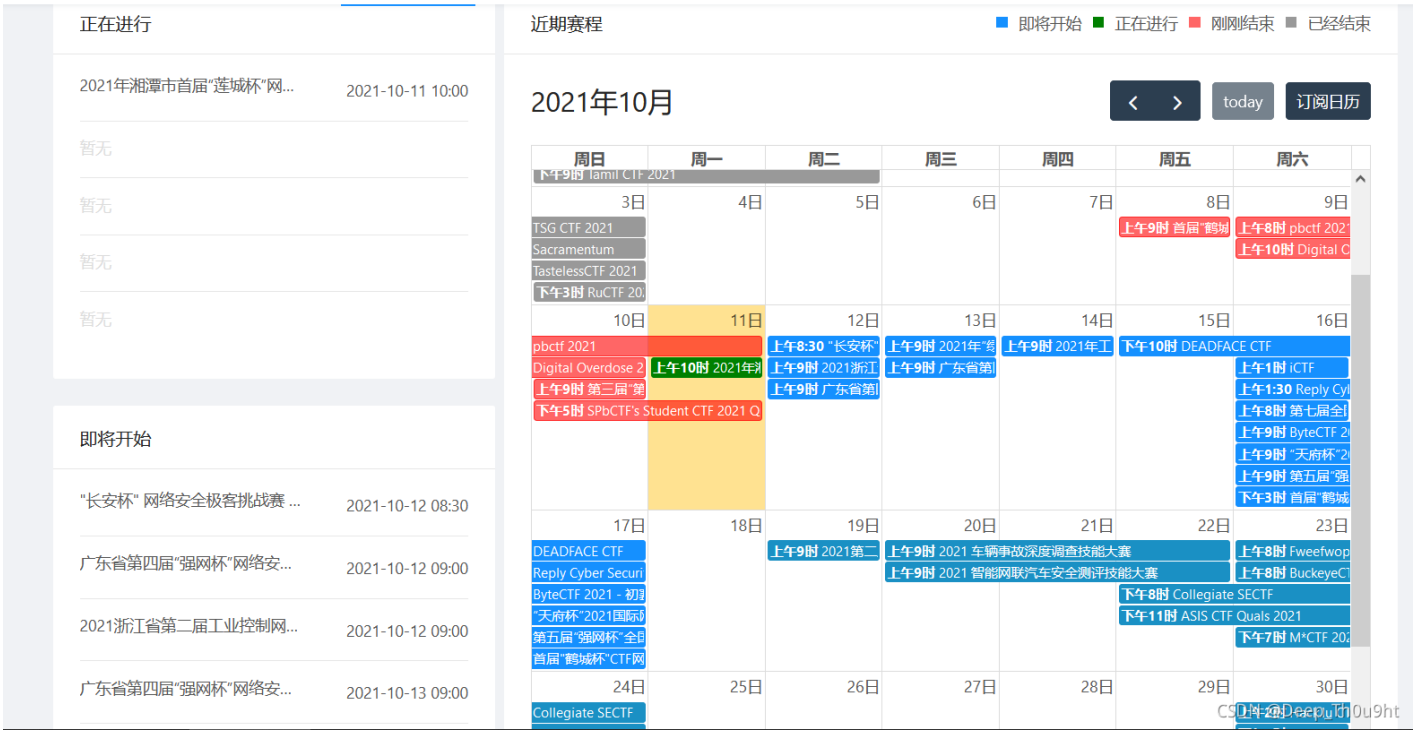


3.**Hacker101**Home | Hacker101 https://www.hacker101.com/ 朋友推荐的国外靶场，也有视频课（没有字幕，但b站有翻译过的，我还没看），题型主要以Web为主，难度还可以。



4. **CTFHub**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……



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 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！