

# 【总结】今日采访·对话：平杰。

今日采访·对话：平杰。

1、暑假该干什么？：



↑与其在互联网上屎里淘精，不如线下约谈学长，获取黄金经验信息差🤔

他的建议：建议我们码代码。

平杰自己的经历：玩（个人理解为疲惫后的放松休息方式）

证据：

2023年

09<sub>7</sub>月

北京市·天安  
门广场



可以勉强拍到兵哥哥🐧看  
升旗太不容易了

08<sub>7</sub>月

北京市·前  
门大街景区  
(北门)



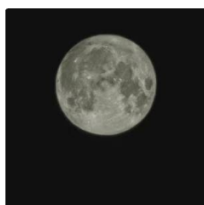
那叫一个地地地地地地道~

↑ 准大三暑假去北京打蓝桥杯网安国赛

实赛兼旅，两难自解

2022年

14<sub>7</sub>月



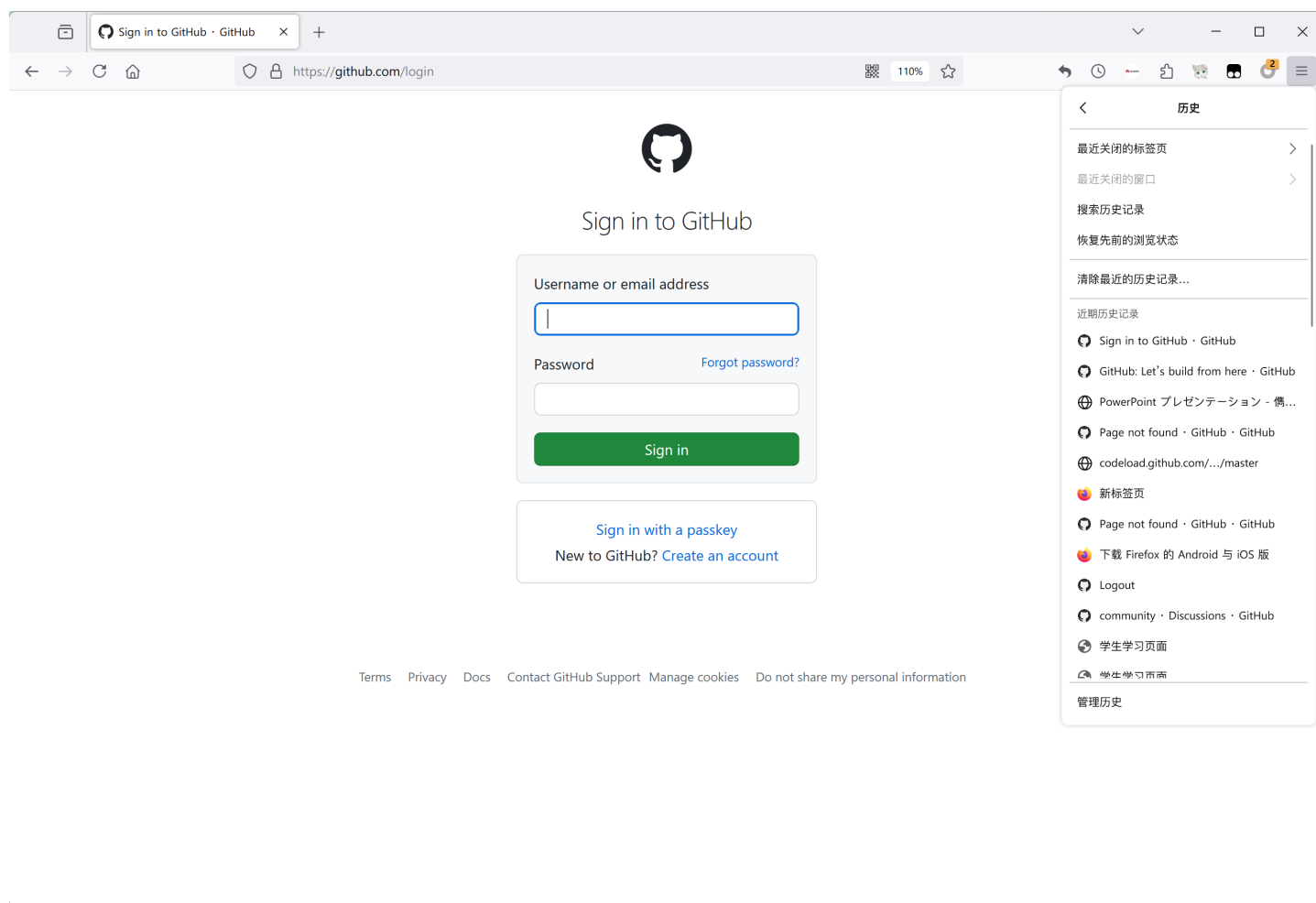
今晚是超级月亮呢

↑ 准大二暑假：休息（猜测）。

极旱极涝，韬光养晦

注：平杰自大三开始备战考研，猜测其余大三学长多为实习党。

2、然后他登录了GitHub，下载了脚本，开始刷阳光长跑（他朋友委托的）：



3、然后他聊起来一个他的同学，之前还是个小白，看了几个月的安全课程之后能力就差不多可以了。



**【小迪安全】web安全 | 渗透测试 | 网络安全 (6个月线上培训全套)**

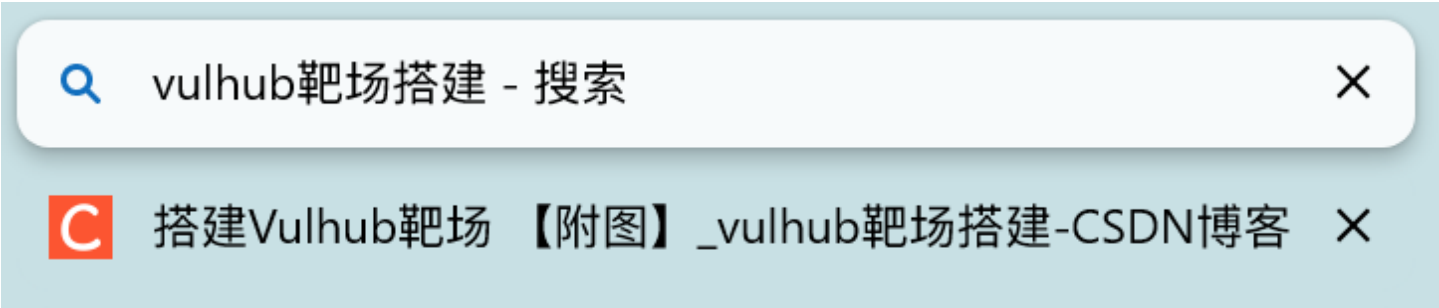
UP 逆风微笑的代码狗 · 2021-4-2

几个月的安全课程

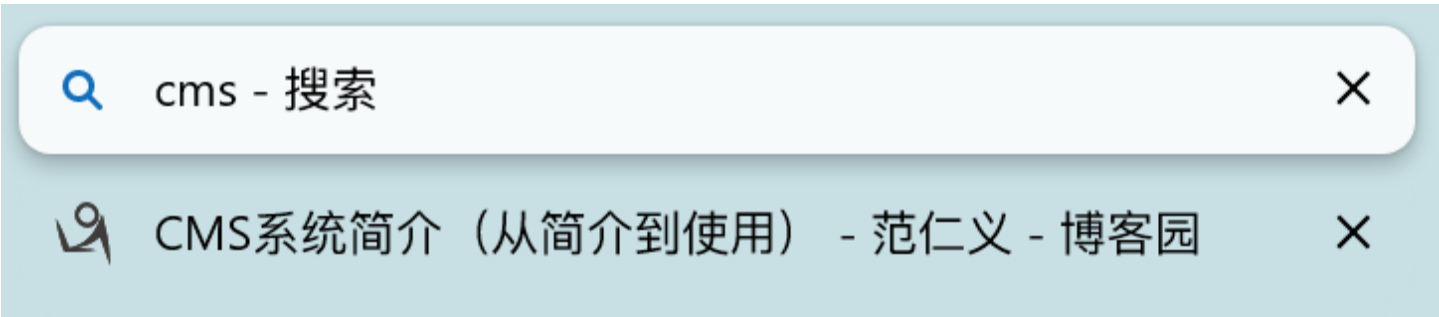
指路：小迪安全，B站、闲鱼百度云 有全套课程；其次，学长也指出了市面上几千几万的课程虽然割韭菜，但确实可能有干货；最后，学长指出兴趣第一位，之前大二的时候都差不多熬到凌晨两三点（没有早自习就是这么嚣张😁）。



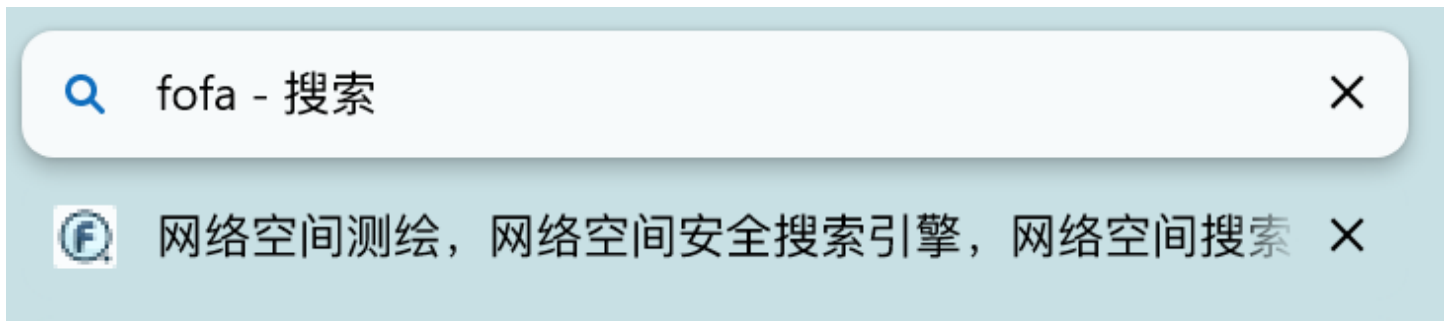
↑ 先是检查了一下我的做题情况，问了我团队里的web手



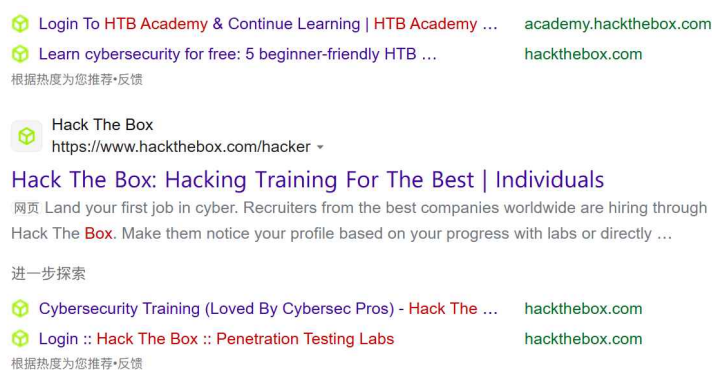
↑ 然后讲解了一下靶场（他大二的兴趣点，经常以复现为乐），0day/1day/n day漏洞



↑ 然后又讲了他之前护网的一次经验，查查web当中的CMS系统，然后在利用1day漏洞攻击，嘎嘎上分



↑ 之后又讲到这个fofa——网安搜索引擎，漏洞扫描用的



网页 2022年8月29日 · Hack The Box是国外的一个网络安全在线平台，允许用户实践渗透测试技能，并与其他类似兴趣的成员交流想法和方法。它包含一些不断更新的挑战，其中一些模 ...

↑ 最后讲到了这个hack the box

4、还是之前发的那些东西（[CTF-web安全/红队渗透路线（1）](#)，[CTF-web安全/红队渗透路线（0）——「路线整理」](#)），只不过这个学期课业压力有点大，被迫吃不了画好的饼，我相信在较高自由度的下学期，我能够施展宏图，大展拳脚，吃上大饼😁

## 前置知识

协议

## 信息收集

网络

域名

公开信息

HTTP

工具

指纹

## 漏洞挖掘

WEB漏洞（原理搞懂，靶场实践几次）

通用漏洞披露

漏扫工具

## 后渗透

操作系统

内网

虚拟化

## 社会工程

书籍

水坑攻击

供应链攻击

钓鱼

工具

## 综合靶场

## 前置知识

- ☐ ☐ 掌握操作系统使用
- ☐ ☐ 熟练重装系统
- ☐ ☐ 什么是web网站?
  - <https://baike.baidu.com/item/web/150564>
- ☐ ☐ HTML/CSS/JS
  - <https://www.w3schools.com/>
  - <https://developer.mozilla.org/zh-CN/docs/Web>
  - <https://www.runoob.com/tags/ref-standardattributes.html>
- ☐ ☐ Golang（未来趋势，良好的跨平台、优秀的多线程和网络处理）
  - [【坤哥力荐】4星期速成学会poc，摆脱脚本小子](#)
- ☐ ☐ Python（社区庞大，入门简单，可以作为初学语言）
  - <https://www.bilibili.com/video/BV1qW4y1a7fU>
- ☐ ☐ Java（后端开发主流语言，通用漏洞发现几乎是最多的语言，学习难度大，不推荐）
- ☐ ☐ 数据库（一种类型选择一个了解）
  - Sql
    - ☐ MySQL（推荐）
    - ☐ Oracle
    - ☐ MSSQL
  - NoSql
    - ☐ Redis（推荐）

↑ 红队渗透线



## HelloCTF

## 快速开始

## 前言

## 环境设置

## MISC | 杂项

## Web | 网络攻防

## Crypto | 密码学

## Reverse | 逆向工程

## Pwn | 二进制安全

## AWD | 攻防模式

## AI | 人工智能安全

## blockchain | 区块链安全

## 附录



## 欢迎来到新手村x

## 注意

在学习CTF前我们希望您具备一些CS领域的基础知识，我们推荐您先阅读 JAN1ittle师傅写的CS入门资料 ([点此跳转](#)) 大致具备CS领域的基本技能后再开始CTF的学习。

这篇教程会引导你大致的了解CTF，并且尝试教会你如何入门CTF。

当然，文档可能不是那么完善，如果你觉得文档缺少什么东西或者有什么不足的地方，欢迎在下方的评论区留言，我会尽快回复。

在开始之前，我想你可能会有些许疑惑，希望下面的 Q&A 能够帮助到你。

## 常见问题 Q&amp;A

## Q: 什么是CTF

A: 「CTF Capture The Flag」中文一般译作夺旗赛，在网络安全领域中指的是网络安全技术人员之间进行技术竞技的一种比赛形式。CTF起源于1996年DEFCON全球黑客大会，以代替之前黑客们通过相交发起真实攻击进行技术比拼的方式；其将安全相关的知识点抽象出来并加入到题目中，我们通过对知识的理解认知，具体地进行实践来攻克题目。

## Q: 什么是Flag?

A: 参赛团队之间通过进行攻防对抗、程序分析等形式，率先从主办方给出的比赛环境中得到一串具有一定格式的字符串或其他内容，并将其提交给主办方，从而夺得分数。为了方便称呼，我们把这样的内容称之为“Flag”。

## Q: CTF竞赛模式?

## 目录

## 欢迎来到新手村x

## 常见问题 Q&amp;A

## Q: 什么是CTF

## Q: 什么是Flag?

## Q: CTF竞赛模式?

## Q: CTF的竞赛方向?

## Q: 我只是个萌新，为什么他们叫我师傅?

## Q: 什么是WriteUp?

## 其他名词解释

## Q: 学习CTF有什么要求么?

## 从哪开始?

## 「网络攻防 WEB」

## 「杂项 MISC」

## 练习平台 &amp; 使用指南

## 比赛平台

## 刷题指南

## 新手引导

## 「杂项 MISC」

## 「网络攻防 WEB」

## 「密码学 CRYPTO」

## 「逆向工程 Reverse Engineering」

## 「二进制漏洞利用 Pwn」

## 消除信息差

## ↑ CTF入门指南

https://xp0int-team.feishu.cn/wiki/wikcnWbXXGLt1xHky8HvdQKrh

General

Xp0int@Feishu (测试中) > 入入入入门 (fén) 综述

最新修改时间为10月23日

入入入入门 (fén) 综述

2023年5月7日创建

大一新生请来这里

1. 编程相关

1.1 如何选择编程语言?

1.2 如何练习?

1.3 用什么写?

1.3.1 Visual Studio

1.3.2 VScode

1.3.3 Pycharm

1.3.4 PhpStorm

1.3.5 IDEA

2. 遇到问题怎么办?

2.1 学会阅读错误提示

2.2 学会使用搜索引擎

2.3 学会翻阅文档

2.4 学会正确提问

3. 做好磁盘管理

4. 你可能需要科学上网

5. 可能需要学习的工具和网站

5.1 下载与安装需要注意的...

5.2 Everything

5.3 Git

5.4 GitHub

5.5 Markdown

5.6 Latex

入入入入门 (fén) 综述

2023年5月7日创建

大一新生请来这里

欢迎各位新生加入计算机地狱大家庭，尤其是十八层地狱的安全方向。无论你是怀着对成为带黑客的憧憬，抑或是觉得计算机相关方向有前景，又或者是随便选了个专业，我都想说计算机从来都不是一个简单的学科，很多人在本科四年啥也没学到（当然入大学前就学过计算机的人可能没什么感觉23333）。不过，我们这里将会尽可能地讲述一些基本和入门的东西，帮助你尽可能地进入计算机的学习进程，减少大家的痛苦过程~

首先，这个计算机自学网站烦请收藏，你在后续的学习中可以去里面取取经：[CS自学指南](#)

其次，相信你的自学能力，你的自学能力远远超过大学老师的讲课速度，请坚持自学，不要仅仅等待老师讲课；

最后，这篇综述字比较多，希望你能够耐心看完，学会阅读长篇文章，也是计算机的必修课。（番外篇之单方面发站：<https://0xffff.one/>）

1. 编程相关

无论如何，只要是计算机相关方向，你就绝对跟写代码脱不开关系，绝不是只有开发才会天天跟代码打交道。相反，唯有相当牢固的代码基础和丰富的代码经验，才能让你在安全的道路上走得更远，当然开发更是如此了。另外，也希望各位不要害怕编程，编程不是一件痛苦的事，相反，编程是为了让计算机来帮助我们解决问题而存在，大家在后续的生活中遇到问题，多思考是否可以通过编程来解决问题，相信我，计算机将会是你提高生产力最重要的工具。所以我们希望大家，最开始的起步，请从坚持不懈地写代码开始。

1.1 如何选择编程语言?



要编程，我们首先简单认识下编程语言。所谓“编程语言”，说白了就是跟计算机交流用的语言，使用“编程语言”，驱使计算机帮你干活。可能很多人听说过世界上有很多编程语言，令人眼花缭乱的，但其实，只要“语言是“图灵完备的”，那它就几乎能让计算机做它能做到的任何事情！那既然如此，为什么世界上还有那么多

## ↑ CTF线

当然啦，大一阶段夯实(代码能力)基础是很重要的。

以下附上访谈录音（前半段不敢录，只有后半段的）文件：

6月15日 18点10分.m4a

 6月15日 18点10分 

- 1 简易转文字：
- 2 加油站未来是有前景大一打基础大二就可以展宏图代码就可以自己的能力发挥的能力去在安领域大展宏图事业怎么代码能力就是没有方面练习练习代码平时多扩展一些兴趣点扩展一些安全这个概念当然如果学习学习学习学几个月就能对这个大概前面那个二十一还是打开反正我不想留下十天时间都会扩展一下自己的兴趣那还有那个学习学习学习学习哦这个这个这个是网络安全学习路线漏洞漏洞挖掘漏洞要更当然可以时间时间暑假没问题奋斗奋斗不要再摆烂了要奋斗一个人奋斗也没有我们一起团队一起奋斗不能自己形式我觉得我也不知道有什么可以让团队一起奋斗前面我们就学的差不多前面课上已经叫前段三千套很长的一条线这够愿意听的够远跟开始一样电脑重启你你打算在暑假怎么学习在家链接在家里学习然后后面的课程基本上就是学校担心生态让我摆脱不了上课可以那就可以摆脱跟这个一样公司这个的话数据规律暑假相互咨询什么自学这些东西但具体我也没想清楚因为现在没了怎么办现在都不清楚你怎么看刚刚开始今年学长做什么给我们讲了一遍这东西怎么打渗透怎么互网的之前大二的时候打了很多靶场挖了很多洞这个说法播放是一个搜索引擎网络漏洞是否写写过对但是其实大一太忙看看我写写写写写过之前写过他说的这些治疗怎样搜一下靶场靶场是有的说法也是有的播放也是有的靶场佛法还有什么互联网行业业内都知道评价他说学校里的课其实不能不能教不了你就不能把你教的精通只能把你交基础只能这些基础的内容但是你交钱一个精通的工程学校课的定位要不要把这个命扎到学校课程说可否一定要多咨询你一定要形成自学能力要不要把这个不要把这个命拿到学校的课上刚才跑步他们各个都经常阳光他的账号上浏览器自己官网管理我不敢用电脑不能电动车阳光你帮我清一下浏览器我知道自觉意识打开热点任务栏这个评分类型不可全部选择同意评分项是什么意思完全不同在位置评价教学观永久永久永久不是移动是永久破解版不能让你给老婆100分之回复覆盖覆盖是否政策直接领很不符合还有两个学生对老师教学工作满意我真的很难评价那你直接干嘛他能看到是谁写的备份不要看我刚刚根本没有备份第三方软件怎么分还是这个进入已经重新关注我给他评论的他不会给我万一有些人不会除非你给他完成了我怎么才能提交啊你为什么他要他提示我我他妈的逼我就是就是你可以靠全都打给他打打到这个来了确实你买这些东西他能看到吗