```
https://www.freebuf.com/articles/neopoints/190895.html
```

总结：

1. 浏览器Fuzzer学习，可以在Win和Linux下Fuzz浏览器，

我最先接触到的是fuzzing，它所带来的自动化，让我陷入痴迷。

我从网上疯狂的查询资料（因为我之前见识过浏览器0day的威力，只需要点击一下链接，那么你的机器便会被控制）

地址：

```
https://github.com/MyselfExplorer/hackingLibrary/blob/master/fuzzing_four.rar
```

2. 拿到Crash，申请CVE，申请报告模板样例参考：

```
Report(CVE-2018-11396:https://bugzilla.gnome.org/show_bug.cgi?id=795740 )
```

3. twitter

twitter搜索关键字，比如：fuzz，fuzzing，fuzzer，看相关最新资料 ，右键翻译成中文，都是最新的技术点

可以在Twitter上面搜索诸如”fuzz”、”fuzzing”、”fuzzer”等关键字；或者在关键字前面添加”#”，例如”#fuzzing”，那么将会限制为只搜索fuzzing话题。

4. Youtube

使用Youtube视频学习，看各种大牛视频，把中文字幕切换上全都可以看懂，语言从来都不是问题，这些订阅号都很好：

```
”Defcon”、”BlackHat”、”OWASP”、”CernerEng”、”hacktivity”
```

还有Bugcrowd的bugcrowd university，hackerone的hacker101；他们会教你如何挖掘web漏洞，并且获取漏洞赏金

在Defcon搜索“APT”：分享者分享了一个被称为”TGXF”、”TKXF”/”TCXF”的技术。它可以实现脱离网络传输文件的效果，只需要扫描二维码便可以在手机和电脑之间传输任意文件；更酷的是甚至还可以通过摄像头在电脑与电脑之间传输任意文件

搜索”how to find bug”：作者现场演示了如何一步一步挖掘一个0day，从开始到结尾，从无到有，可以完整见证一个0day的诞生；在视频的最后，可以看到全场掌声如潮。

在Defcon

如果你想学习漏洞挖掘，那么推荐”Bug Bounty Public Disclosure”这个订阅号，尽管里面全都是已经修复的漏洞，但是并不影响对我们的帮助。

当然，也可以直接搜索”bug bounty”关键字，然后筛选你需要的。

5.WriteUp

pentesterland：如果你是渗透测试人员，那么这个站点对你的作用将是巨大的。

https://pentester.land/list-of-bug-bounty-

writeups.html ：这里面收集了过去到现在的所有经典的挖洞过程。

Bug Bounty Reference：里面几乎囊括了所有与web安全相关的技术点。

PayloadsAllThings：不管你是红队，渗透，ctf 玩家，你都可以在里面获得你想要的资料

6.新闻

```
Thehackernews：https://thehackernews.com/
文章的最后还可以看到参考文章，这些都非常有价值

Freebuf：https://www.freebuf.com/
```

大佬的学习方法：1.在Youtube上看视频 2. Google查询相关资料 3. 实战操作

7.工具

不要相信”脚本小子论”。除了尽快的学习最新的

1day/nday，学会利用它们相关的工具也可以让你快速成长。

Kitploit:里面介绍了很多的黑客工具。

```
https://www.kitploit.com/
```

如果只看文章，对于工具的操作仍旧不是很明白，那么此时可以去Youtube上搜索这个工具的相关关键字。通过查看分享者，可以让你收集很多分享黑客工具的人，你可以关注他们，随时跟进。

搜索关键字：

```
Kitploit，RAT，rat fud，bypass av
```

RAT：远程控制工具；bypass：绕过

只要对自己有用的，都应该记到自己的笔记里面，不用顾及会不会太多。

如果你想进一步提高自己，你还可以阅读这些工具的源码，他们大部分是Python、Ruby、Perl语言编写的。

windows平台下的黑客工具包，太多了，你随便一搜便会找

到很多，像：扫描、暴力破解、间谍软件、EXP等都可以找到

Connect-trojan：这是一个RAT下载器，可以找到A-Z大概几百款国外的RAT，很多APT组织都会进行大量的利用这些。里面的很多开源工具都可以进行二次开发，定制为自己的专属工具。

```
http://www.connect-trojan.net/
```

这是两个黑客论坛：

Offensive Community:http://offensivecommunity.net/

Cracking:https://cracking.org/forums/cracking-tools.16/

强烈建议：千万不要去百度上搜索”黑客”、”黑客教学”、”黑客论坛”、”黑客排行榜”、”黑客教父”等这些东西，它害了多少中国热爱 hacker 的孩子，让他们还不知道什么是 hacker 精神的时候，就迷失在了恶作剧、违

法、金 钱、虚荣、交智商税的怪圈里；强烈的抨击那些混蛋们。

1/nday&Exploit

关于漏洞的利用Metasploit是效率最高的工具。

在这里能获得最新的漏洞利用：https://github.com/rapid7/metasploit-framework/pulls

Twitter和Youtube在这里仍旧是有效的工具。

如在twitter上面搜索”#exploit”、”#0day”。

在Youtube上面搜索 “CVE+年份”

除了黑客大会上的分享，Youtube上的结果也需要筛选，不要直接搜索什么黑客教程，因为有很多傻子在黑”hacker”这个东西。

知识来自于网络世界，也服务于网络世界，因为是宝贵知

识，所以需要你花费努力才能筛选出自己需要的结果，不要相信不劳而获的东西，不然你会 上当受骗。

8. 一些其他的东西

二进制入门：

```
https://www.youtube.com/playlist?list=PLhixgUqwRTjxglIswKp9mpkfPNfHkzyeN
```

逆向工程：

```
https://www.youtube.com/results?sp=EgIQAw%253D%253D&search_query=reverse+engineering
```

里面都是一些很好的课程，像”linux”，”macos”的逆向，也有101 to master系统的学习。

下面是一个我在搜索”fuzzing”关键字时找到的一个fuzz浏览器的视频。

```
https://www.youtube.com/playlist?list=PL00QFekqLCCLvF4iaP8FLuUuot2OIsiqq
```

中文站点强烈推荐 Bilibili，它也可以帮助你成为强大的黑客

这里面有”操作系统原理”、”计算机编程语言”、”计算机科学”、”算法基础”等很多优秀课程，甚至是国外的知识，并且都是翻译好的，你只需要坐下来学习就可以了。

汇编、 C、Python、Javascript，这些你都能在里面找到，操作系统原理，哈佛的 cs50，计算机科学等就像内功一样，它们太重要了。

当你看透二进制世界的时候，可能便不仅仅限于hacking了，人工智能，大数据，还有更多的东西，你都可以在里面找到，非母语的问题到此便可以解决了。

漏洞搜索引擎，可以最快的帮你找到公开的漏洞：

```
https://sploitus.com/
```

非常好的搜索漏洞平台：

```
https://media.ccc.de/
```

海量数据搜索：

```
https://cdn.databases.today/
```

跟其他安全人员交流：

在Twitter，微博，知乎上，你可以直接分享你的经验给那些开启私信功能的安全研究人员们。

即使名头很大粉丝巨多，或者一些安全公司甚至某些专家、黑客书籍的作者，亦或者出名的大牛还是一些低调独立的漏洞猎人（Bug Hunter），只要开启了私信功能，那么你便可以发送你确切具体的问题，90%的人都会答复你。

千万不要害怕交流和询问，每次尝试你都终将会获得帮助。

9. 结尾

“心能转物，即同如来”，在任何困难的时候，别无他法的情况下，改变自己的心境，才能改变现状；

“天上天下，唯我独尊”，你已经来到这个世界，便是独一的，别人的成功与否与你关系并不大，不要羡慕和追捧它人，那只是消磨你的时间，专注于完成你自己的生命修行，遵照你的内心，更少的不受外物所扰，活成一个传奇。

10. 自己收集积累的资源：

最全的浏览器漏洞分析文章：

```
https://github.com/wnagzihxa1n/BrowserSecurity/blob/master/%E5%AD%A6%E4%B9%A0%E8%B5%84%E6%96%99.md
```

Pwn学习资料：

```
https://etenal.me/archives/972#B1
```

各种文件结构：

```
https://github.com/corkami/pics/tree/master/binary
```

CTF WriteUp

```
https://www.xctf.org.cn/
https://github.com/Kung-Pao-Chicken/ctf
看雪
```

非常牛逼的漏洞技术博客

```
http://angelboy.logdown.com/
https://whereisk0shl.top/

```

非常牛逼的安全前沿论文

```
https://securitygossip.com/blog/
```