# 渗透学习

转载

weixin_30735745 于 2016-11-30 19:40:00 发布 47 收藏 3
文章标签： php 数据库 python
原文链接：http://www.cnblogs.com/Oran9e/p/6119391.html

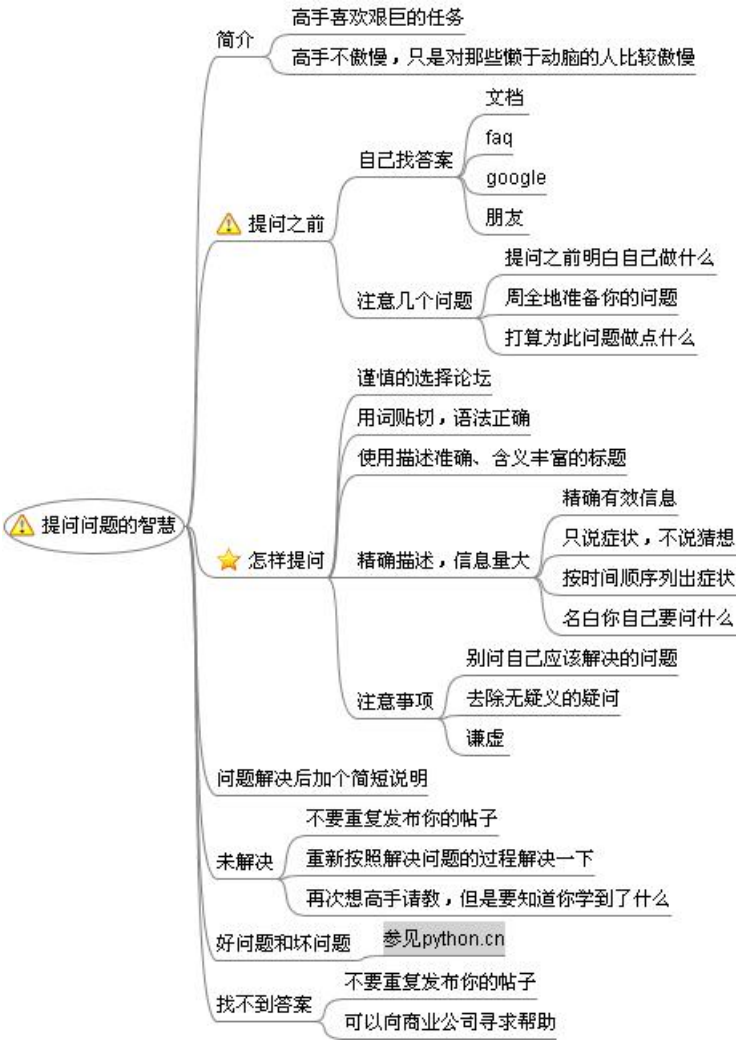

## 前言

近日被几位同学询问怎样去入门,我作为一个稍微接触这方面的小白,尽我所能整理总结一下,希望能帮助到一些同学。

## 学习能力的培养

自我感觉在课堂上所学的知识完全是不够的，更多的是需要课后的自我学习，所以学习能力的培养是最重要的。

提问的智慧(http://www.guokr.com/post/90225/)
1，在遇到问题的时候,可以先去搜索一下,你遇到的问题,网上可能就有人也遇到过这样的问题,暂时不要急于去问他人,学会自己处理问题.是在解决不了的,可以去询问他人。具体见下图。



2，学会搜索
利用网上的强大资源,比如bing,google,维基百科..,为了更加精准的获取到资料,要学会一些搜索引擎的语法：google hacking (http://baike.baidu.com/view/336231.htm?fr=aladdin)
对于怎么样访问google，大家可以去FQ或者替换hosts文件(https://github.com/racaljk/hosts)

3，学会总结
学的东西多了,很容易就忘记以前学习的知识,推荐用一些笔记软件去总结自己学过的知识。
比如：印象笔记,马克飞象，写博客记录。

4，多动手
看书是一方面,动手却又是另外一方面,多动手才能加深印象,不然就是纸上谈兵。

**入门流程**

下面是针对完全0基础的同学

1. 了解一些基本名词以及意义
   这本书,《黑客攻防---web安全实战详解》,感觉用来入门很不错(但是内容有些偏老)

另外几本本书是
《安全之路：Web渗透技术及实战案例解析（第2版）》 看目录是一本详细而又偏实战的书，我只是感觉目录写的很棒
《Web安全深度剖析》 与上面有些相对立，原理稍微多了一些
两本结合起来很棒。

> 实际的去了解渗透是什么(看视频)
> 因为大家完全不知道从何下手,最快的办法就是看别人的视频,自己去模仿,但是一定要记住,看完要去明白,**为什么要这样做,原理是什么,如果我是运维应该怎么去防御**
>
> 视频推荐：
> 暗月渗透视频：
> http://115.com/lb/5lbdbgrw5wb
> 暗月原创网站入侵渗透视频(共三十一节上).zip115网盘礼包码：5lbdbgrw5wb
> http://115.com/lb/5lbdbgrdy8h
> 暗月原创网站入侵渗透视频(共三十一节下).zip115网盘礼包码：5lbdbgrdy8h
> http://115.com/lb/5lbb9qtwclp
> 暗月一些视频.zip115网盘礼包码：5lbb9qtwclp
> http://115.com/lb/5lbaw6oj44s
> 暗月原创提权视频.zip115网盘礼包码：5lbaw6oj44s
> ps:这些视频可能有些老了,但是我觉得还是可以用来入门的,更多的需要大家自己去寻找了。
>
> 了解漏洞原理
> http://wiki.wooyun.org/enterprise:web
> http://wiki.wooyun.org/enterprise:pentest
> 这wooyun的wiki已经包含了很多,别纠结某个名次,重点在于你是不是知道这个漏洞,毕竟名词是人定的,显得高大上只是装逼用的。
>
> 针对性的研究
> 再知道一些漏洞原理后,可以补充更多最基本的知识来理解。
> 比如sqli:因为对数据控制不严,导致可以在数据库中执行语句
> 这时候就可以去学习一波数据库原理。

**编程之道**

基础语言
c

web方面需要掌握的一些东西
html javascript php(不一定是php,但是个人感觉php比较好些)

然后平时可以用来解放双手的一个强大编程语言
python

**注意：编程的重要性,很多大牛都是推荐从一个程序猿转到做安全是更好的,多写代码对漏洞理解会更深**

**ctf**

作为学生党,最习惯的还是那种做题的感觉,所以大家也可以通过一些ctf的比赛做题来学习,以及验证自己的学习成果.
附上一些关于ctf：
综合：
http://wargame.kr/
西普学院
http://www.simplexue.com/CTF.html
http://canyouhack.it/
http://fun.coolshell.cn/
网络信息安全攻防学习平台
http://hackinglab.cn/
idf实验室
http://ctf.idf.cn/
wechall
http://www.wechall.net/
合天
http://erange.heetian.com/
jctf
http://ctf.3sec.cn/
http://oj.xctf.org.cn/

渗透:
米安网
http://ctf.moonsos.com/pentest/index.php
http://webhacking.kr/
四叔叔写的一个
http://hackit.sinaapp.com/

xss:
http://prompt.ml/0
http://xss.pkav.net/xss/

sql:
http://redtiger.labs.overthewire.org/

逆向:

http://reversing.kr/
http://pwnable.kr/
http://exploit-exercises.com/
http://overthewire.org/

各种writeup
https://github.com/ctfs/
bin干货区
http://security.cs.rpi.edu/courses/binexp-spring2015/

各种赛事预告
https://ctftime.org/event/list/upcoming
来自：http://bbs.secbox.cn/thread-38-1-1.html

参考文章

Web新手入门：
http://blog.sycsec.com/?p=166

转载于:https://www.cnblogs.com/Oran9e/p/6119391.html