



## 《K哥谈：白帽子转型养成之路》

孔韬循 ( K0r4dji ) | 北京丁牛科技有限公司-首席安全官 ( CSO )





## 个人简介

2019

**姓名籍贯：**孔韬循，籍贯内蒙古-赤峰市，93年，网络ID：K0r4dji（小K）

**项目经验：**拥有多年国家级党政军信息安全服务经验

**接触时间：**2008年左右接触（15-16岁期间）

**所在职位：**北京丁牛科技有限公司-首席安全官（CSO）

**安全团队：**国内信息安全研究团队-破晓团队（Pox Team）创始人

**个人名言：**没有高手和菜鸟，只有玩的多和少！

**相关书籍：**

- 1.中国工信出版集团-电子工业出版社《Web安全深度剖析》原稿审核/修改人
- 2.中国工信出版集团-电子工业出版社《Python带我起飞》专家书评撰写人
- 3.中国工信出版集团-人民邮电出版社《Windows黑客编程技术详解》专家书评撰写人

.....





- 1.中央企业-中国电子CEC-可信华泰教育事业-技术专家顾问
- 2.中国工信出版集团-人民邮电出版社-IT专业图书专家顾问
- 3.中国Python开发者大会-特邀讲师
- 4.国家教育部-第九届全国大学生信息安全竞赛-嘉宾/评委
- 5.广州大学-网络信息安全CTF夏令营-方滨兴院士班-高级讲师
- 6.赛宁网安-白帽子学院-资深专家顾问（院长：诸葛建伟）
- 7.北京蓝森科技-15PB二进制安全实地培训机构-特邀讲师
- ....





# 目录

01

过去的成长轨迹

02

目前心理与状态

03

未来发展与规划

04

K哥的综合建议





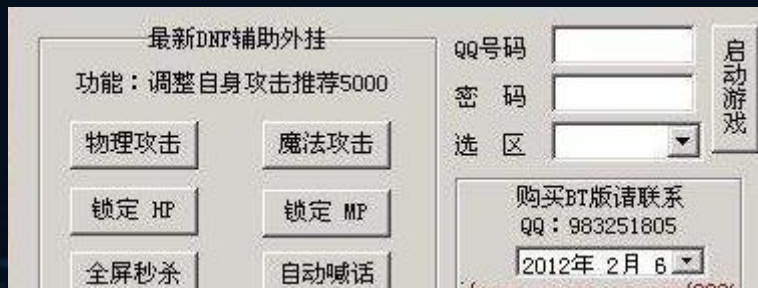
## 虚拟世界财产被盗取

2019

游戏账号：大话西游/热血江湖/梦幻西游/天龙八部/CF穿越火线/DNF地下城与勇士...

社交账号：QQ

....



我会迅雷  
下载QB







拜师收徒，只要8.8，寒暑假冲刺班

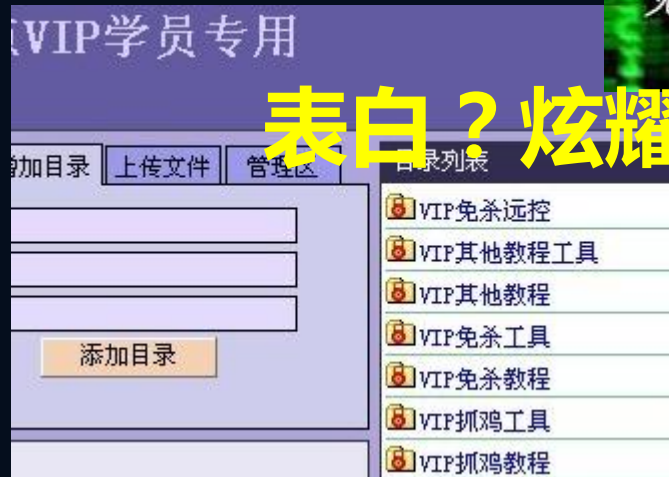
2019

免费网络安全培训原创语音教程

弘扬黑客文化，普及安全知识



表白？炫耀？虚荣？装X？...



交钱就拉黑！



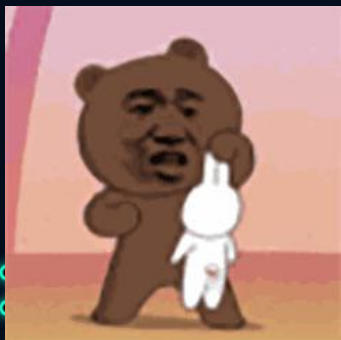
招人：XX负责人、XX导师、XX讲师、

开班：WebShell提权班、渗透班、DDOS抓鸡班、免杀班、编程班、外挂辅助班....

名字：中国XX家族、中国XX黑客联盟、中国XX小组、中国XX安全团队...

搞事：Hacker By Helen（梗）、教父-郭某华、此站/此号/此群被社....

惹事：你很牛逼嘛？求社！求D！我大哥是XX，不服你来打我！....（调侃）



年轻气盛，希望  
最后能有真正意  
义的成长与发展！



## 看眼眼熟的工具....

2019







## 看眼眼熟的工具....

2019





# 看眼眼熟的工具....

2019

花刺代理验证 (P Cheat Engine 5.6.1)

地址栏: D:\

SQL连接

IP地址 127

上传步骤

本地文件

SHELL

DOS 命令

命令: dir c:

恢复

DLL路径

中国代理

中国代理2

中国代理3

国内代理

台湾

上海

西藏

湖北

国内

中国代理

世界

文件(F) 编辑(E) 进程(P) 帮助(H)

00001454-Lingoes.exe

找到: 1, 905

地址	值
001212E4	11
001213F3	11
0012142D	11
00122283	11
001223FD	11
0012412D	11
00124C04	11
00124C1C	11
00124CE7	11
00124D34	11
00124D4C	11
00124E97	11
00124EE7	11
00129954	11
0012A2B0	11
0012AA03	11
0012AA5D	11
0012AB73	11

新的扫描 再次扫描 撤消扫描

数值:

☐ hex 11

扫描类型 精确值

数值类型 4 个字节

内存扫描选项

☒ 用户模式 ☐ 所有

从 目

00000000 77F7FFFF 显示

☐ 同时扫描只读内存

☐ 快速扫描 ☐ 深层扫描

☐ 在扫描时暂停游戏

☐ 禁止随机

☐ 启用速度修改

查看内存

手动添加地址

锁定	说明	地址	类型	数值
<input type="checkbox"/>	无说明	001213F8	4 个字节	11



## 眼熟的课程...

2019

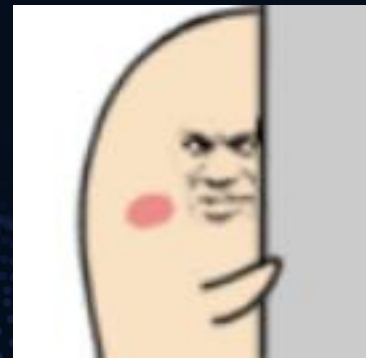
- 饭客黑客之免杀教程.rar
- 饭客黑客之入侵教程.rar
- 饭客黑客之基础教程.rar
- 饭客黑客之提权教程.rar
- 饭客黑客之网赚教程.rar
- 饭客黑客之脱壳破解教程.rar

- 黑客基地软件破解特训班1-19.rar
- 黑客基地软件破解特训班20-38.rar
- 黑鹰破解教程.iso
- 甲壳虫脱壳破解班.rar
- 中华隐士黑客联盟软件破解及解密系列

- YES黑客联盟初级免杀培训教程.rar
- 暗组Gh0st编译免杀系列教程.rar
- 暗组免杀教程.rar
- 饭客Gh0st源码免杀VIP教程.rar
- 红色黑客联盟免杀教程.rar
- 华中红客基地菜鸟学习MianS系列教程.rar
- 小七VIP\_2013年无特征高级技巧处理(主要针对)
- 新世纪网安VIP高级免杀班1-16.rar
- 新世纪网安VIP高级免杀班17-31.rar
- 夜鹰海盗盟初级免杀培训教程.rar

- 冰客安全网渗透系列.rar
- 饭客脚本入侵.rar
- 黑客动画吧Web入侵班1-16.rar
- 黑客动画吧Web入侵班17-31.rar
- 黑客动画吧之网易学院新手脚本系列
- 黑客防线2009脚本课程.rar
- 红黑脚本攻防20课全.rar
- 华夏入侵.rar
- 华中红客入侵.rar

一个没学会







不是我们太年轻，而是没有人愿意正确引导

2019

引导不足



不用搭理他们，都是小学生

诱惑四起



老板日站嘛，1个10万

肆无忌惮



无所谓，别人入侵我看也没事，我也不能有啥事情

根深蒂固



你不GetShell提权拿服务器脱裤，还学什么网络安全？



# 目录

01

过去的成长轨迹

02

目前心理与状态

03

未来发展与规划

04

K哥的综合建议







## 目前的状态，CTF+刷漏洞平台

IT 2019



哪个师傅带  
带我？



## IT技能充电-培训方式补充营养

IT 2019

- 1.现在的渗透跟以前不一样了
- 2.现在的二进制也跟以前不一样了
- 3.现在的公司企业岗位需求跟以前不一样了
- 4.现在的求职门槛也不一样了
- 5.现在的技术门槛跟以前也不一样了

慌

15PB®

十五派信息安全教育  
15PB Information Security Education

LanOu  
蓝鸥





## 目前的心理活动

2019

### 初级(0-1)

- 拜师学艺
- 八方看看
- 结实伙伴

### 中级(2-4)

- 技艺实战
- 四处游荡
- 团队组建

### 高级(5-8)

- 技艺娴熟
- 目标锁定
- 团队发展

哎哟给你呱呱呱呱



优秀





# 白帽子内心弹幕墙！

2019

你厉害你  
牛逼

这个人绝对  
是大佬

一群SB

这个小姐姐  
好漂亮

他还不如  
我呢

呵呵

都是大佬

这哥们技术  
屌的一匹

凭啥他就比  
我牛逼

我要当大  
佬

我就是不服

去哪找个工  
作呢

好像不适合做  
安全哎..

SRC坑爹

漏洞审核SB

我就鄙视你  
了咋地吧

我娱乐圈了  
咋地吧

不服你咬我啊



阔怕





# 白帽子团队-破晓团队 ( Pox Team )

IT 2019

**灵魂创建**：2013年10月，2014年中旬开始运营

**团队文化**：路虽远，行则必达。事虽难，做则必成！

**官方网站**：<http://www.SecBug.org>

**团队人数**：60-70人

**成员组合**：CETC中国网安、腾讯安全应急响应中心、美图秀秀、联想、安天、安恒、国家电网-电力科学研究院、中国电子、德国电信、银行、中国农科院、360集团、360企业安全集团、启明星辰ADLAB实验室、天融信阿尔法实验室、知道创宇、T00ls多板块/多位版主、Python开发者组委会核心、中国石油、国家队...等，安全研究经验3-20年不等。

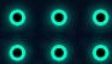
**相关书籍**：《Web安全深度剖析》/《Python带我起飞》/《Windows黑客编程技术详解》

**团队日常**：SRC漏洞/书籍编写/技术切磋/心情分享/CTF/职位内推/活动合作/企业辅助...等

**成员职位**：工程师->组长->经理->总监->首席安全官->CEO首席执行官...阶段不等。

**行业贡献**：人才输送、人才中转、人才培养、课程分享、文章分享、其他扶持...等

**组建意义**：让大家有归属感，有喜欢的事情自由研究并实现出来，分享更多的事物。



理念：SRC/CTF刷的再牛逼，有困难了不去帮忙，这支队伍的灵魂是有问题的！





## 如何做好一名白帽子？

2019

**白帽子-DM**：在遵守法律的前提下，对安全知识能做到刨根问底，追求理论和实战相结合，不拘泥于工具的使用。要有一门自己很熟练的编程语言，把自己的想法付诸于行动，用代码实现它。肯花时间去钻研，不要把时间浪费在没有意义的事上。作家格拉德威尔说过：要成为某个领域的专家，需要10000小时，按比例计算就是：如果每天工作八个小时，一周工作五天，那么成为一个领域的专家至少需要五年。自己对于一个事物的认知程度取决于自己对这个事物花了多少时间。当然前提是这个时间是属于有效时间。

**白帽子-岩少**：做自己该做的事情，接自己力所能及的东西，坚决不能触碰红线。

**白帽子-Simple**：保持激情上进的态度，不断探索学习新兴技术，实践多于理论。

好强的骚气！





## 如何做好一名白帽子？

2019

**白帽子-红客十年：**首先我们要了解白帽子存在的意义，只有了解了白帽子存在的意义，才能去做好白帽子，白帽子是一个黑灰产业时代诞生出的新生群体，这个群体的存在是为了守护安全，但现在在利益的驱使下和圈子文化的感染下，已经没有纯粹的白帽子了，我们应该属于这个安全时代的先驱者，看到身边很多朋友都在利益和圈子文化里沉下去了，希望后起的白帽子要记住你成为白帽子的初心是什么，不要跟着利益和圈子文化去改变自己，要做到真正的不忘初心！

**白帽子-Saviour：**Emmm.....

为啥你们  
这么优秀！





# 目录

01

过去的成长轨迹

02

目前心理与状态

03

未来发展与规划

04

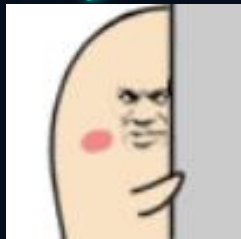
K哥的综合建议





## 未来发展与规划-生活与学习

FIT 2019



取个媳妇生个娃，老婆  
孩子热炕头



富婆 抱抱我

我要买一个大房子



我要把某个领域的技术  
学的很得心应手，像某  
师傅一样优秀

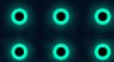
装了逼就跑，真刺激

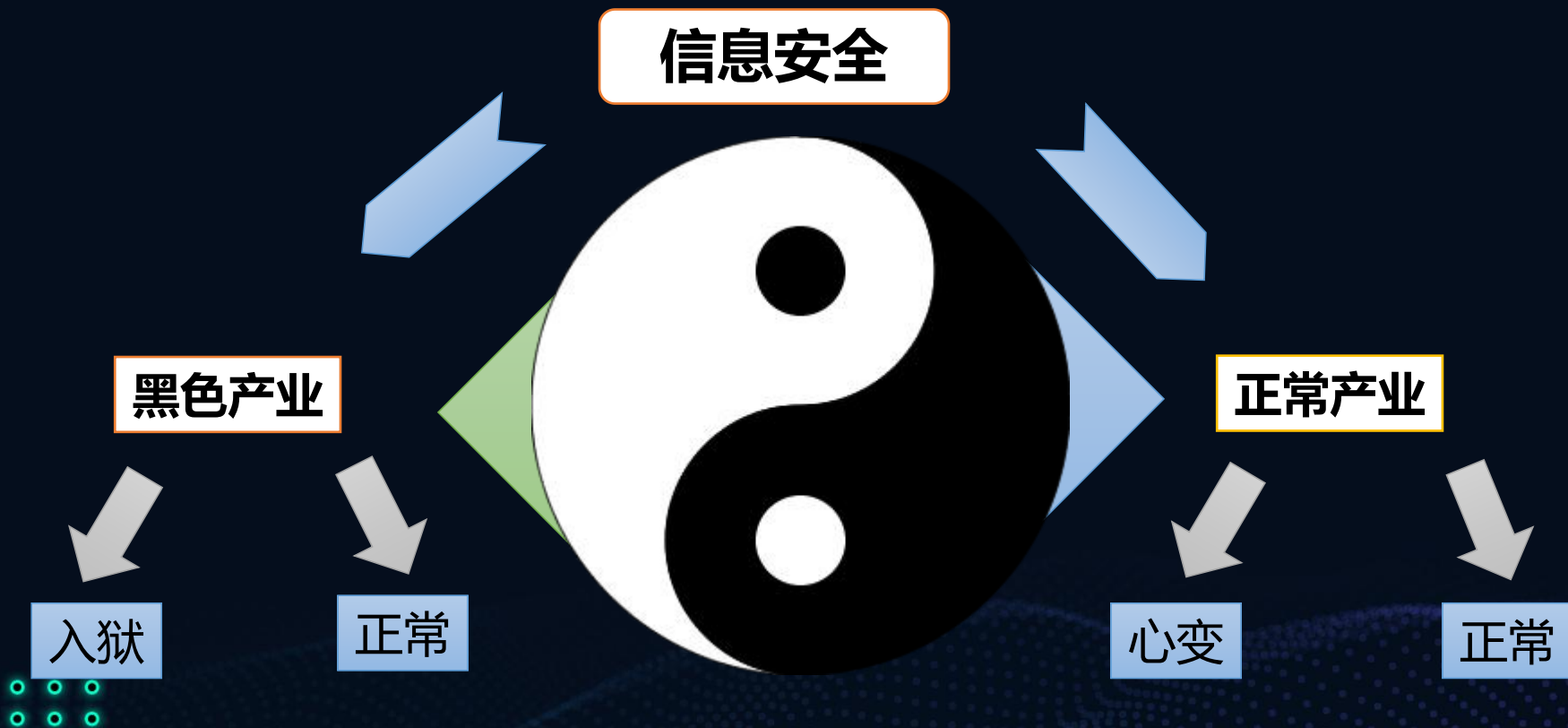


多把基础打扎实点，以  
后还想做管理呢



规划是个啥玩意？



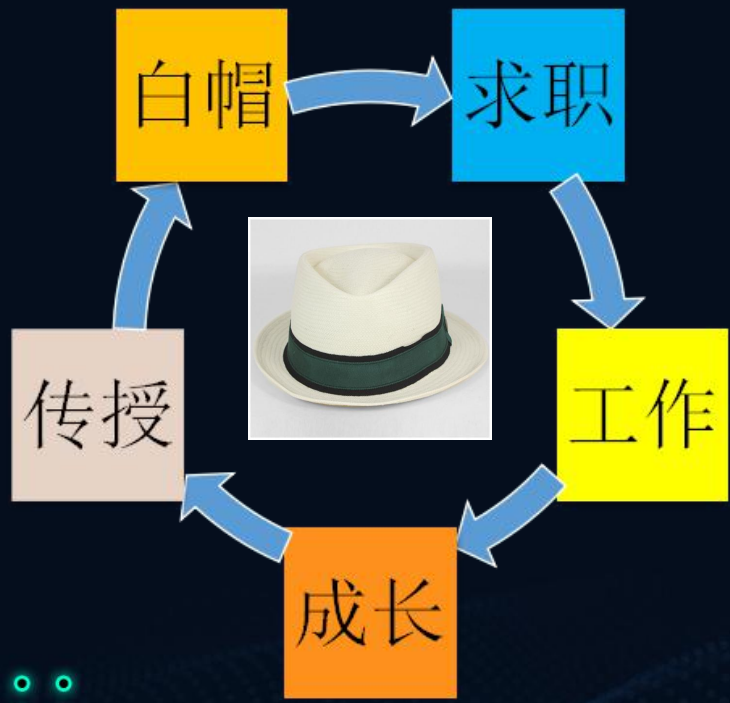






# 未来发展与规划-骑驴找马，让伯乐自动送上门！

FIT 2019



我驴在哪？怎么骑？



怎么让驴加速？



我的千里马在哪？



伯乐？来一斤....





# 目录

01

过去的成长轨迹

02

目前心理与状态

03

未来发展与规划

04

K哥的综合建议





## 白帽阶段转化引导

2019

### 初级

- 对方喜欢玩啥，就让他玩啥
- 因为对方根本不知道有啥

### 中级

- 基于兴趣尝试一段时间的深度学习
- 因为对方不知道到底适不适合自己

### 高级

- 技术方向抉择，规划辅助，转型
- 因为对方经历的多就知道了



你给了建议，对方以为你在坑他。【有木有深有感触？】



建议一：人无完人，用全力，迎接你的职场

建议二：比你牛的人，一定汗水很多

建议三：谦虚谨慎，多低头学习做事情

建议四：要学会体现你的成果

建议五：急躁是解决不了问题的

建议六：成长是无限的，学习是首要的

建议七：别人的建议要去尝试验证和体会

建议八：扬长避短，查缺补漏





## 我的联系方式

2019

邮件：[admin@secbug.org](mailto:admin@secbug.org)

微信二维码



看你们吹牛装逼电脑都烧了







| REEBUF | TIT

THANKS