> 在双十一大家都在购物的时候，我们在圈子里做了一个分享活动，这是几位小伙伴的学习经验分享，希望能对圈子里的同学有所帮助。

第一位：编号 001

看了前面几位表哥写的文章。我也来讲一下自己的入坑经历，可能和你们大部分人不一样，我既不是信息安全专业也不是和计算机相关的专业。苦逼工科男一枚，现在大三。

最开始接触到这方面的东西，是在吾爱破解论坛，当时也只是纯粹为了找资源，后面发现上面的一些技术帖子比较有意思，然后慢慢的就接触到了一些逆向破解方面的知识。当时也没想太多，在去年寒假陆续续的学了一点点破解方面的东西。能够简单的破解一些小软件。开学后，也就是大二的下学期，我有一个协会里面的学长他特别牛逼。有一天我看见他在看一本书，是张银奎写的软件调试。然后我就跟他说我是用 od 调试软件的。这一说就跟我打开话匣子了，整整讲了一个中午。那时候正是四月份左右，他跟我讲他怎么用影子经纪人的工具，在图书馆里面实战拿下两台 win7。我听得很入迷瞬间充满感兴趣。他说 web 渗透玩来玩去就那么点东西，让我直接学二进制。当时还完全是一个小白，我学长直接就扔给我一本逆向工程核心原理，让我去看。看了 200 多页吧，实在是太无聊，就没有看下去了。那段时间没学多少，最多也就只是用 ms08067 拿下了一台 xp。后面我发现自己基础实在是不行，搞不了二进制，就打算学 web 渗透。为了能多学点东西，上个暑假我没有回家。一直待在学校里，看这方面的教程。书看了六七本，视频教程看了一套。然而发现，自己还是什么都不会，主要是实践的太少了。现在想想暑假的那两个月有点耽误了。到了开学的时候，想了想，觉得以后能从事这一行就从事这一行，毕竟比现在的专业好多了。然后一切又是从头开始从最简单的注入学起。加了一些安全小组一起互相学习。和前面那位大佬一样，也是各种翘课。到现在吧，觉得自己会的东西也不多，漏洞原理基本了解，kali 工具会用几个感觉自己基础还是太薄弱了。

因为目前考试陆续的来了还有专业实习在这方面没太多的学习时间。打算在这个寒假好好的学下 PHP 和 python。

另外说一下群里的学习氛围真的还不错。加了很多个安全方面的群，咱们这个群学习氛围是最好的。能经常看到一些大佬的分享，有时迷茫的时候看一下这些文章，挺好。

愿自己在明年暑假的时候能成功找到一个安全方面的实习工作吧，然后就顺利转行了，哈哈哈。

感谢大佬抽出一点时间看我的入坑之路😊😊可以的话，交个朋友哟😊😊

第二位：编号 002

本人小白一枚，目前读职高还有一年升大专读嵌入式技术（连我自己也不知道是搞什么的）
刚开始学习 web 安全方面知识，前前后后几个月的学习时间，接触过 sqlmap，nmap，awvs，burp 等工具，只会基本操作，原理还没接触。暑假用了一个月在 sqli-labs 靶机里学习 sql 注入，看群里大佬推荐用 dvwa 靶机练习，自己前前后后搭了数十环境，真正玩透的没一个。由于有过一年自学 c 语言的苦逼经历，国庆七天学习 php 入门挺快，渐渐开始接触 Python，看 i 春秋教程，学习 kali，msf，arpspoof 的玩耍，在自己搭的靶机里各种自慰，让孤独苦逼的学习之旅增添一点色彩。
很想去实战一把，但是苦于真的不明白如何找洞，问过一两个大佬，不过都没回复我，只能自己继续好好打基础。自学是真特么累，也没缘分认识一些大佬，不懂只能找度娘。
路总得走下去，不过不知道怎么走，有点迷茫，希望有大佬带一把。目前在学 msf，Python，PHP，想学习怎么打 CTF。虽然开启多线程很累，但日子好像过得挺充足的。

第三位：编号 003

我也来随手写一写。
先说写背景，今年大二，计算机科学与技术专业，大一学了 C 语言，但二级考了两次没通过。以后专业课有 Java，HTML，数据库，但那个时候就到大三大四了。
我是今年 3 月份开始接触这方面的内容，在网上找了个群，交了 30 元，得到了一堆整理后的资料，加入了内部群开始看视频，看完一遍后也对 “黑客” 有了新的认识。同时，也感到了看视频和上手实践的重要性，看的视频再多，还不如实战一次来了解自己知识的薄弱点。第一次实践的也是和 “Hiton” 一样的 ms08-067 漏洞，不过我是虚拟机搭建的环境。

由于我个人感觉内部群得到的视频有点旧，就在网上找新的视频，这个时候接触到漏洞银行新手特训营，跟着倾旋车王学习，对渗透测试产生了浓厚的兴趣。与此同时，开始了 CTF 的学习，爱好 web 题，隐写题也不错，不过现在也就做做线上的题，比如实验吧，南邮什么的，最近也报名了安恒的 CTF 比赛，虽然就会做个签到题什么的。
说说现在，在 w3school 上学 PHP，但发现需要先具备 HTML、CSS、JavaScript，所以现在在学 HTML。同时，也在看其他的教程视频，感觉现在的知识面已经扩展开，但具体细分到一项上就有些模糊了。
想听听大佬们给我意见，如何更加有效的学习。信安之路，任重而道远。

第四位：编号 004

表述不清还请各位大佬、表哥见谅
过去的一年算是我正式接触到信息安全这一行吧，虽然我的专业就是信息安全，但是大一的时候完全是混过去的，室友在努力学习各种协议、linux 系统的时候我还在打游戏。
这一年算是我启航的一年，说说我学了些什么吧：owasp 漏洞，linux 基本操作，php (做不到代码审计，但能看懂程序的意思)，常见的几个工具(msf,empire,sqlmap,nmap 之类的)
掌握的很少，也不算精通，在打 ctf 和想做实战的时候都感觉有些力不从心，很难受。
感觉自己处在一个瓶颈期，基础的东西都会一些，想往高处走又找不到方向，最重要的可能是心境的宽广问题。之前暗暗的想和室友比(毕竟他离我最近)，但是一年的时间就被拉开不少差距，追逐他的脚步让自己很累很迷茫，所以决定和自己较劲，要做得比以前好，让自己满意。面对最重要的上升期，如何突破瓶颈让我很苦恼，心境的狭窄让我把自己绑起来了，信息安全太广，找不到自己的领域而无处使力，请问各位表哥在打下基础之后是如何突破瓶颈期的，还请各位表哥多多赐教。
说说这一年剩下的两个月的计划吧：《白帽子》，《 web 实战篇》，《 python 黑帽子》这三本书认真阅读一下，powershell 攻击原理，中间穿插点实战。欢迎各位表哥对我的学习路线做出建议批评

第五位：编号 005

原来以为分享 pa 要干货才可以分享呢，看了前面两位大佬的入坑历程，决定也分享一下自己的~
目前大四，专业是开发方向的。
其实一直以来都对信息安全很感兴趣，奈何之前失足跌进了召唤师峡谷，迷了路，没走出来，浪费了大好光阴。不知道在座的各位有没有跟我一样的路痴~
咳咳~
今年 6 月，学校安排到一家公司进行开发技能培训（ Java 的 SSM 框架什么的），培训完以后准备找实习。一开始是想先做一年开发，然后再研究安全的。
后来一位很厉害的同学直接找到了渗透的实习工作 ?!!!
还有这种操作
原来对安全感兴趣，但是可以说完全不了解
他和我关系好，跟我说:“其实你想做安全的话，现在也可以的”，然后跟我说还有其他的小菜鸡也找到了安全的工作。
于是我下了决心，也要试一试。
然后就开始入坑了~
然后他借我一本书 《 Web 安全深度剖析 》 ，还给我推荐了一些他觉得比较好的公众号，网站和群（我加这个群就是他推荐的）
书看完以后原理大概都懂，玩了一下 dvwa 靶机。再看了一下那些招聘要求。还要会白盒测试，所以又看了《代码审计》，就有点跃跃欲试了
我同学那家公司有个大牛，很中意很想去，为此准备了很久也等了很久。终于去面试了。失败。原因是公司刚起步，需要有经验的人。那时候很失落，很灰心丧气，但是没有后悔。因为这是自己选的路，而且这么年轻，刚走出社会就不敢试一下，这样我记几都会看不起我记几了
因为完全不了解安全行业的现状，就以为需要的都是有经验的人，很绝望，觉得实力不够很难找到工作。一度想过回家修炼，明年春后再来。然后女朋友一顿噼里啪啦骂了一顿，说还有其他公司，让我去投简历，面试。
好吧，破罐子破摔。投就投，谁怕谁
然后第二次面试，运气好，过了。就有了现在这份工作
回想起两个月前（ 9 月 15 的样子）我还在玩 LOL，打排位，想新赛季拿个好框。
搞安全对我可以说是从入门到卸载游戏
从开始（ 9 月 16 日的样子）花时间研究渗透到找到工作（ 10 月 18 日），花了大概一个月。

上班以后发现很多的不足，比如没用过 sqlmap、还有很多比较弱的漏洞都没见过、圈子太小（ msf 是什么都不知道，kali 的界面都不知道）、没有用过扫描工具等等。现在基本上可以胜任工作内容，也加了好多个群扩大圈子（发现其他群好多人搞黑产）。唔，大概这样。工作以后眼界宽阔了好多，实战就还需要多加努力啦。
最近买了不少书，上周买了 kali 的，kali 无线的和 msf 渗透测试实践指南。今天双十一，看了猪猪侠的学习路线买了 TCP/IP 和汇编。觉得工具要会用，但原理才是核心。稳扎稳打的学，多点实战。希望尽快达到我那位同学的水平，然后超过他，再有自己的 0day。咳哼，我又做梦了不好意思。
说完经历再说一下想法吧。
喜欢安全原因很简单。因为安全脑洞大，并且自由
目前学习计划是想先尽快尽量接触多一些，更了解这个圈子。迟些对各种漏洞都比较熟悉以后就研究一下 waf 的防御原理，然后回归底层，写写代码。Web 这块做好以后研究搞无线和移动渗透。
如果有刚入门没多久的朋友，我有个小建议
一定要有圈子！
一定要有圈子！
一定要有圈子！
圈子可以给你带来什么？
1， 知识面。有圈子你可以看他们聊天，从中了解到各种各样的东西，扩大知识面，然后才有可能将这些一一击破。否则自己一个人就像打人机一样，真的玩不转
2， 学习资源。有圈子可以带来很多学习资料。原来我是只有这个渗透群的（信安之路），当我发现我同事 qq 一直在闪，都是渗透群的人在聊技术。我一下加了十几个，然后在群文件里面发现好多的学习资源。
3， 有人指路。运气好的话说不定可以找到大牛教你。反正现在我同学教我绰绰有余 2333
唔，大概就是这样。
各位大佬有什么意见或者建议都可以跟我聊一下，为我指条明路
因为可以进知识星球，所以重新修改了一遍。
麻烦投我一票。我很想进知识星球呢。谢了哈~

第六位：编号 006

本萌新已经大三了，最近学习的重心在编程和审计上，大佬们带带我。

其实我是在初中就开始玩的，那时候玩过灰鸽子，火蚁的加壳，阿D，木马的捆绑工具也玩过。在那个时候，那些老牌的小工具那么轻轻的一扫，就会有不少的收获。后面学习了一部分的汇编语言的免杀，搞了花指令，记得我当时初中，假期去上成人夜校，学习了算是网络工程师的课程，顺手学习了数据库（微软小狐狸），然后打算玩，但是家乡（ XINJIANG ）出现了断网事件，断了一年。后来，还是没有继续这类的爱好了，高中家里自然也断了网，网吧也只能滑滑水，玩毒奶粉。

重拾这方面的爱好，是大二下的时候，电脑下载软件，多了个奇怪的进程，猜测了下被中招了，重启电脑，那个小东东还在。。。贼气，没百度到方法，只能重装电脑。装完以后，我想到，自己如果有什么重要的资料，被窃取了，那岂不是很火大。我以前上冰河，也就看看摄像头，然后默默删掉木马，离开。没办法，我只能重新开始了学习，入坑的第一本书是 《 metasploit 魔鬼训练营》，真是让我读了个痛快，让我重新认识到了还有比 C/S, B/S 玩法更有意思的东西，然后我找到了玄魂大大的 kali 教程，看了个痛快，我用着 meta 的靶机，把那里的工具和 metasploit 的攻击手法，研究了好几遍。但是真的玩实战，我玩不通呀，我看了黑麒麟的视频，也找了些网站去试了下手，没错 waf，但是也有成功的案例。

我也从中失败以及成功中思考过一下问题：

1、如何去测试得知有漏洞的产生（高效的渗透思路）

2、如何对一个漏洞进行攻击到 getshell 到提权（渗透攻击手法的展开）

3、如何渗透内网

4、如何对木马免杀，绕过 UAC 防御（二进制领域和诸多的知识）

我不会的究竟是太多了，我认真学习了 burp,学习了 sqlmap 好几个常见的工具，但是我到了需要有人帮我把那层窗户纸捅开的时候，我找了玄魂群里的大佬，问他如何挖掘漏洞的（我那时还真的不会挖SRC,现在会挖但是懒得动），他让我找了 HWC（你们去 CNVD，看着个人贡献能找到他），那个骚气的白帽黑阔（花了一笔，现在觉得真的比较值）。暑假，开始了我的 web 实战挖漏洞的学习，好了，常见的 web 漏洞挖了一大波，感觉入门了。但是我们都是玩的 win 的工具，开学的时候，思路突然开了，学的常见工具不都在 kali 上吗，于是我开始去研究下国外的网站安全性，很多的工具用法，我也是在 freebuf 和习科，i 春秋那里看的，我看免费的，也渐渐的发现自己的不足，阅读那些被推荐的 web 书籍，最后找到了自己的短板：编程。所以我开始了写 php 代码，学习审计，希望成为法师那样的大牛，自己也努力练习 python，希望能写出扫描器，毕竟国外有什么新鲜货，我这里自行组装好，去补天刷一波。

当然，我自己只是把这个作为兴趣来玩，不太会当成职业去做，现在学习 yii 框架，学习代码。毕竟现在都是讲究的使用框架来开发，安全性高，先学习开发，同时看书，知道开发的流程和思想，然后再来玩挖洞，这样有新的漏洞利用的技术，你才能更好的把他的挖掘思路变成你的，关键是要打牢基础，多看几本基础的协议和原理的书，弄懂了，真的不耽误你去花什么论坛币学习新的漏洞 getshell 姿势的时间，底子足了，才更好理解，“二次开发”。几个月前你让我去看乌云的知识库，我真的很多不能理解，但是现在，好多了，但是我发现了我更大的知识空白。我看到了猪猪侠的学习之路，我只希望不急不躁，尽力去学好那些基础，再去看那些“姿势”。每个阶段都会有新的思路和新的漏洞等新事物的产生，基础不变，当然想想那些东西很多人不懂，自己花时间搞懂了，岂不是能装逼了，是不是特别的爽。
我也只是一个入门不久的新人，还希望能够多把基础打扎实了，把编程好好练习了（不是每一个程序员都是黑客，但是每一个厉害的黑客都是炒鸡厉害的程序员），刷刷 SRC，攒一笔钱，把那个 PTE 证书考了，大佬们，要是我有审计方面没弄明白的，多带带我。我也是个萌新。群里的萌新们，一起加油学习吧。

第七位：编号 007

看到群里的大佬都有写这个，我也写写自己的菜鸡之旅，刚开始接触网络安全大概就是阿里的月饼事件，某程序员写脚本抢月饼，然后知道了学校有个实验室是专门搞这方面的，这下激发了我的兴趣，俗话说学计算机的不想当黑客那不是好程序员，于是一开始接触的 sql 注入，也硬着头皮刷完了 sql-lab ，但是我还是喜欢做 ctf 中的隐写，misc 之类的题目，然后不久前觉得自己不适合搞 web，于是转手二进制，学到现在有点收获，但感觉自己还是很菜，想找一些志同道合的二进制小伙伴创个群，天天刷题，分享经验撒的，这样带动学习的积极性，希望有师傅能带带我，自己一个人学确实很累

第八位：编号 008

我大学专业是信息安全，但在学校里面并未真正去学习安全类相关知识，只是自己学习了有关 PHP、Python、Mysql 的知识，然后在实验吧、i 春秋上刷了一些 CTF 题目、也曾参加过一些 CTF 比赛，但技术不够。

进公司实习后，首先就是结合 Burpsuite+Sqlmap 以及 Kali 去完成 DVWA 的题目，但在做的时候还是参考了 Freebuf 里面某位大牛写的内容。由于自己之前学习过 php，因此我更能知道 DVWA 漏洞产生的原理。

也通过一些网站，博客学习了有关信息安全的相关术语，比如你知道POC的完整意思是什么嘛？我觉得在安全业它指的是概念性验证（ Proof Of Concept ）【余弦大大说的是：观点验证程序】，也就是通过代码可以验证漏洞可以被利用或者说可以被证明存在。

在学习了 DVWA 后，我学习了 OWASP Top 2013 和 OWASP Top 2017 RC1 (现在有 RC2，正在学习)。 OWASP 每隔一段时间就会更新当下 10 个最关键的 Web 应用安全问题清单，即 “OWASP Top 10” ，这是针对 Web 应用安全问题的一个影响力极大的清单。我建议大家也去学习领会下，对自己的见识成长肯定也会有帮助。

由于在公司一般都是弄安全测试，因此与开发人员之间的交流并不多，后来我们部门给开发人员开展了安全开发培训，我负责讲 A2 -失效的身份认证和会话管理、 A8-CSRF 、 A10 - 未受保护的 APIs。在准备 PPT 的过程中，我又进一步的了解了漏洞的原理，产生原因，以及如何从开发阶段就去避免这些漏洞的产生。

比如对于 CSRF，我给的建议是：

一、严格验证Referer来源，必须是 http://www.xxx.com/ 开头

二、可以通过设置随机 Token，然后与 Cookies 里面的或者 Session 中的对比

“<?=csrftoken()? ” />

三、在 HTTP 头中自定义属性并验证，XMLHttpRequest 这个类，可以一次性给所有该类请求加上 csrftoken 这个 HTTP 头属性，并把 token 值放入其中。

现在我在学习有关 Python、GO、Docker 相关知识，我认为以后企业肯定会用到许多 Python、Go 语言（人工智能、AI ），也会用到许多 Docker 容器，因此我觉得这里面的安全隐患肯定会像之前众多 PHP 语言框架产生的漏洞一样多。

信息安全知识很多，我也是个小白，下面推荐大家一些我觉得可以汲取知识的站点。

> http://www.freebuf.com 【Freebuf】
> https://www.ichunqiu.com/【i春秋】
> https://www.t00ls.net/ 【土司】
> http://www.shiyanbar.com/ 【实验吧（在线CTF，渗透测试实验）】
> https://www.shiyanlou.com/【许多视频、实验】
> https://chybeta.github.io/2017/08/19/Web-Security-Learning/ 【Web-Security-Learning 学习资料大礼包，强烈推荐】

最后送给大家一句话“会当凌绝顶，一览众山小”。