**前言：**

和一些hr的交谈中我受益良多  
有一些人在职，即使不跳槽也会经常出去面试。为什么？我总结了如下几点：  
1、了解市场需求，明确自我定位和目标。特别是互联网行业发展迅速，市场对某个岗位的需求是发生变化的，通过对比，你才能知道自己的专业能力是否还能满足市场需求，还有哪些不足，找准定位和目标  
2、掌握薪资行情，判断现有能力与薪酬是否平衡 再来决定要不要跟领导提加薪或者是跳槽  
3、积累面试经验，提升自我营销能力

**渗透岗位\全职工作面试**

所面试公司：(学院内招)江西掌控者信息安全技术责任有限公司招聘  
薪资待遇：12k起  
所在城市：江西南昌  
面试岗位：Z1级辅导员  
面试官的问题：

1、自我介绍  
（略…..）  
2、你挖掘src的思路是什么？  
(略…..)  
3、在挖掘src的过程有遇到过什么有趣的站点吗？  
（在src挖掘的过程中我遇到一个比较有趣的站点，当我在前端测试sql注入时，爆出了一出一个框，说了一些带双亲的话。激起了我对这个站点更深层测试的欲望。在信息收集阶段发现目标站点下的子站存在一个cms，在漏洞文库中搜索了此cms站点的漏洞，发现存在文件上传就getshell了）  
4、给你一个目标，你的渗透测试流程是什么？  
（我会分为信息收集、漏洞测试、漏洞利用、权限提升）  
5、详细点的呢？  
（首先是信息收集，信息收集我会分为两块，第一块是网站：谷歌语法、找后台，铭感文件泄露，子域名、旁站、分站、C段，目录扫描、看是否是以恶搞cms以及站点都有什么功能点。到服务器信息收集这块：端口信息、服务器操作系统、中间件。到了漏洞利用，主要还是看信息收集到了什么样的信息，有什么样的功能就去测试什么样的漏洞。若是有测试到危害大一些的漏洞例如文件上传之类的getshell才有后续的权限提升）  
6、bypass有哪些手法  
(内敛注释加数据库的版本号、参数污染、缓冲区绕过)  
7、文件上传拿到shell之后，你的权限是什么权限?  
（一个低权限）  
面试结果：未通过  
面试难度：适中  
面试感受：其实还有一些没想起来，风哥给我说出了我自身的不足之处，与一些建议，修正了我未来错误的职业规划路线。着实让我受益良多。

所面试的公司：默安科技有限公司  
所在城市：北京  
面试岗位：安全服务工程师【应届生/实习生】

面试官的问题：

1、自我介绍  
（略…..）  
2、ssrf的原理是什么？  
(通俗易懂的说明是：利用一个服务器可以发起网络请求访问当作跳板来攻击内部其他服务)  
3、文件上传绕过的手法有哪些？  
(前端burp抓包绕过、后缀大小写绕过、后缀符号绕过、文件流绕过、双写绕过(pphphp)、00截断绕过)  
4、Mimikatz的常用命令是什么？  
（我平时喜欢在kali上用mimikatz。有Load mimikatz、mimikatz\_command -f samdump::hashes  
、mimikatz\_command -f sekurlsa::searchPasswords）  
5、能说说内网渗透的流程吗？  
（创建用户并加入到管理员组，登陆目标机器，用mimikatz看管理员密码这个时候就有白银票据了…因为这方面做的比较少，所有没答的上来多少）  
6、正向代理和反向代理的原理能说一下吗？  
（不太记得了，之前学习算是比较久远了）  
7、给你一个网站，你如果对其进行渗透测试？  
（信息收集、漏洞挖掘、漏洞利用、权限提升）  
8、MSF中的ms17\_010怎么打的？能简单的讲一下吗？  
（打ms17\_010、先搜索ms17\_010模块，直接选中模块，架设攻击载荷、设置目标地址和本机地址就能打）  
9、代码审计都复现过什么漏洞？都是什么cms？并且你是如果去审计发现它们的？  
（ThinkPHP-Shop、ThinkPHP3.0/5.0、dedecms、等。平时我都是全局锁定一个函数去寻找什么样的地方能被用户进行传参，哪些地方往往最容易出现问题）  
10、ThinkPHP什么样的版本都出现过什么样漏洞？  
11、>src挖掘是怎么样拿到名次的？思路是什么？  
(src拿到名次和思路不是一两句句话能说的完，三尺之冻非一日之寒，我有些过相关的文章，如果您要看我可以推荐给你)  
12、你认为你是一个什么样的人？  
（上进励志有志青年）  
13、你为什么要投我们公司？  
（朋友推荐的招聘信息，听朋友说还不错）  
14、和其他面试者相比，你认为你自身的优势是什么？  
（…还没思考过这一点）  
15、你可以接受加班吗？  
（愿意……）  
面试结果：未通过  
面试难度：适中  
面试感受：感觉问的问题都比较刁钻，兴许这也是我个人的不足之处。

所面试的公司：北京永信至诚科技股份有限公司  
所在城市：福建福州科技园  
岗位：安全服务  
面试官的问题：

1、自我介绍  
（….）  
2、owasp 漏洞都有哪些？  
(sql注入、xss、失效身份认证和会话管理、敏感信息泄露、安全配置错误、csrf…….)  
3、你有尝试过完整的渗透测试吗？  
(做过一次)  
4、有入侵过国外的网站吗？  
（没有）  
5、有做过黑产吗？  
（不做，以后也不会去做）  
6、你简单的说一下变量覆盖  
（变量覆盖一般都是代码审计出来的，是指原有已经被定义好的参数在程序中可以被用户去替换，用户可以去替换时就会出现一些问题。例如绕过登陆进入管理员后台）  
7、说一下反序列化原理  
(将php中对象、类、数组、变量、匿名函数等，转化为字符串 方便保存到数据库或者文件中,将状态信息保存为字符串)  
8、xxe实战遇到过吗？能说一下如何审计和利用吗？  
(xxe一般是代码审计出来的，就是XML外部实体注入攻击，DTD部分去读取敏感的信息、将读取到的信息赋值到实体当中、XML部分使用的过程中，将实体内容输出，危害是读取任意文件、执行系统命令、探测内网端口、攻击内网网站等)  
9、出差你能接受吗？出差的工作内容是去别家公司给他们做网络安全培训  
（我可以试试）

面试难度：适中

面试感受：海星

所面试的公司：有度网络安全技术有限公司  
所在城市：福州  
面试职位：渗透测试实习生  
面试官的问题：

1、你叫XXX对吧？你为什么会想到来福州工作呢？  
（略….）  
2、在线下awd攻防赛中，你在队伍是什么角色呢？  
（防御，巴拉巴拉说了很多我在比赛中的各种的防御手法……）  
3、在sql注入时遇到waf，怎么绕过呢？  
（内敛注释加数据库的版本号、参数污染、缓冲区绕过）  
4、mysql写文件需要什么条件？  
（root权限、绝对路径）  
5、sql注入写入文件都有哪些函数？语句是什么？  
（Union Select ‘一句话木马’ into outfile ‘路径’  
Uinon Select ‘一句话木马’ into dumpfile ‘路径’）  
6、如何防止CSRF？  
(验证referer\验证token)  
7、ThinkPHP框架有了解过吗？有复现过吗？  
（略…）  
8、了解过电子取证吗？  
(暂时还没有)

面试难度：适中

面试感受：感觉面试官是外行的，但是人很好，一边喝茶一边聊有说有笑。还不错没有紧张的心理。

**给大家的建议：**

面试是一个不断学习、不断自我提升的过程，有机会还是多出去面面比较好，至少能想到查漏补缺效果，而且有些知识点，可能你自以为知道，但让你说，并不一定能说得很好。有些东西有压力才有动力，而学到的知识点，都是钱（因为技术人员大部分情况是根据你的能力来定级、来发薪水的），技多不压身，学完咱学院的东西，一定要多扩展课外知识这点很重要！！