**所在城市：北京**

**面试职位：渗透测试工程师**

面试过程：我是转岗的，往他家投了简历，然后就给我打电话了，电话面试，面试官还是蛮好说话的，问了比较基础的东西外加代码审计方面，反序列变量覆盖啥啥啥的。这里基本功做好就行，直接过了，话不多说 下面进入正题。

**面试官的问题：**

**HR：来个自我介绍吧**

答：渗透测试方面我是自学的 因为一直以来对信息安全有强烈的兴趣 从接触到现在差不多两年了 对系统的漏洞和web漏洞都有了解 能完成漏洞的查找 提交src 说明修复建议等（我觉得尽量说自学吧 因为自学的话在HR心中你能回答出很多问题代表你平时还是很努力学习的）

因为平时实战就是在漏洞盒子挖src来成长的对于挖这么久的src 挖的最多的那肯定就是属于漏洞之王sql注入 还有xss url重放 以及文件上传这些 其他漏洞虽然都有了解 有时候也会挖到 但是在实战中其实并不会太深入去做一些太过分的事情 毕竟的话渗透测试有限度 （委婉的表态我平时挖内网渗透比较少 求你别问 ） 平时会在论坛，博客先知社区 在B站看视频或者与朋友交流等等

**HR：那你平时在哪些论坛看呢？**

答：我……论坛方面….（早知道就不写论坛了），平时基本都在csnd上面看 我觉得上面知识很多的（尴尬回答）

**HR：你有博客么？你id多少？**

答：没得。 HR：那我建议你去注册个 多写点心得文章之类的 对你有帮助。

HR：我看你简历上写了xxe能详细说一下你实战咋做的么？

答：（直接回答靶场是怎么做的就行了，我记得我大概是这么回答的）  
我记得我上次xxe是一个cms 首先创建炮台1.xml 2.php 3.txt 然后抓包将1.xml数据从2.php发送到3.txt 那么数据就会从3.txt里面回显出来 可能有加密 把加密的数据解码之后就可以继续后面的渗透工作了。 hr：嗯 不错不错。

**HR：那waf绕过方面你说一下？**

答：sql方面的么？ HR：嗯  
大小写绕过 不过大小写绕过一般在比较老的waf才管用平时我不会怎么用

代替绕过 比如and -> & 其中符号是有相对应意义的这时候可以尝试对符号进行URL编码进行绕过

拦截union select可以考虑中间加个空值 union null select因为mysql里面的语句是比较粗糙的并不通用 如果写详细一点就要写union null select null，null，null 这样子

内联注释绕过 其实单纯的/\*\*/这种很少绕得过这时候就需要加版本号 内联注释版本号绕过 版本号用burp来测1000-99999如果加版本号还不行那么就加换行 、内联注释+%0a换行绕过 如果还不行那就换方法吧

容器特性-参数污染绕过 打个比方就是select 中间都加上% s%e%l%e%c%t 那么他执行之后就会变成select了

还有就是内存垃圾字符溢出绕过 这绕过很麻烦很难 但是我觉得效果比较好 麻烦就麻烦在你要知道每个waf的大概具体溢出字数 多了也不行 少了也不行都是拦截 就比如说我绕过的网站waf 他的字符数大概在4200多个

**hr：那你知道长亭的waf么？还有个xx waf （忘记他说的那个waf了映像中是个出名的waf）是多少字符？**

我：挖的时间太久了 忘记了 主要也不是天天都在绕waf用溢出方法不断测 其实这个方法是很费时间的 具体的可能要碰到的时候从新测。

hr：嗯。 某某waf是4万5千多个垃圾字符 长亭的是（这里我又忘记了多少字符）xx个字符。

**HR：那你了解过ssl绕过么？**

答：啥？csrf绕过？

hr：不是，是ssl绕过

我：我听不清 信号不好

hr：是！ S S L 绕过

我：哦 ssl啊！

hr：对的

我：不知道 没听说过

hr：………..

hr解答 ssl是证书绕过（这里给我解答了是啥原理绕过 不过我忘记了记性太差）

我：哦~ 嗦嘎原来是这样 那回头我得好好了解一下这个ssl绕过

hr：嗯，好的。

**HR:那说一下变量覆盖？**

答：我记得变量覆盖是必须白盒审计的 然后原理方面是 变量覆盖指的是可以用我们自定义的参数值替换程序原有的变量值

影响变量覆盖函数方面的话我记得是extract() parse\_str()

（在这里介绍函数的时候并不是直接说的 而是我不怎么会英语读不出来 然后一点点的拼出来 然后hr又说这个是这么读的….在这里有点小逗）

**HR：还有么？**

我：我目前所了解的就没有了 在这方面我了解的少 平时对于这方面不怎么审计 导致我在代码审计方面还是比较薄弱的因为平时挖src还是以前端深透为主

我对我自己的评价是 ，前端深透觉得中规中矩吧 代码审计因为不怎么实战所以很弱 ， 我主要还是想在工作以后着重的学习发展代码审计方面

hr：嗯 不错不错

（我为什么这样说大家可以自行体会一下话术中的奥妙）

**HR：那反序列化说一下？**

答：反序列化方面我知道原理 以及利用 以及防御方法等等只不过平时实战基本没怎么挖过而已 当然啦 我还知道java反序列化 因为我觉得现在java用的比较多嘛 所以也有去了解一下

hr顿时有了兴趣 那你说一下java反序列化？（面试方面hr其实问反序列化的话其实更想听java反序列化）

我：我java反序列化我只知道原理并不怎么深入。

hr：哦~ 意思是知道但是不怎么深入是吧

我：对的。 hr随后简单的说了一下java反序列化

（这个问题相当于我啥专业知识都没说 但是面试官又知道了，我会原理以及解决方案 只是不深入了解 就这么糊弄过去了你敢信？）

**HR：你这个简历上这个工具smf是个啥玩意？**

答：啊？不好意思 写错了 是msf

hr：哦~

我：那要不~ 我给你说一下？

hr:可以可以 你说一下吧。

我：咳咳~ 我酝酿一下哈

hr：嗯

我：首先呢 msf是kali里面的工具 这个工具说简单不简单 说难也不难 有了这个工具呢那些不懂的只要学msf就可以入侵别人的内网了 就变成了所谓的黑客了  
具体使用呢 首先就是扫端口咯 扫出端口以后然后msf里面是自带攻击模块的 好像是有一千多个还是两千个攻击模块 我的msf显示有1500多个 然后直接调用相对于的攻击模块来用就完事儿 比如我扫出445 那么我就调用一个永恒之蓝ms17的攻击模块然后直接打 不过呢这个永恒之蓝是真的猛 我上次直接把我建立的环境给主机电脑给打关机了 然后拿到shell之后再提权方面的操作 提权然后… 我记得我提权完事之后就没了 就这样。

hr：嗯 这个msf呢我的建议就是在项目不要用 特别是在公司域渗透 用这个会导致业务受阻（后面给我讲了一系列坏处）

**HR:我看你src有排行？ 能否说一下名字？我查一下？**

答：这里给他看就完事儿。

**HR：我看你之前做设计师好好的怎么想着转岗呢？**

答：主要是公司以及行业受到疫情的冲击…..（后面我就不说了 扯犊子就完事儿）

面试结束 HR：好的 我觉得你还是很不错的实战能力也挺强的 自己自学挺好  
src也有排名 那么你的一些基础挖漏洞能力还是证明有的 很不错 晚上人事方面再给你打电话 请留意一下 （具体的夸赞我忘记了 大概意思就是这样的）

**面试结果：通过**

**面试难度：简单**

面试感受：体验还不错，我这里面试难度—简单—是因为我一直带着面试官的思想走的 假如我被面试官一直带着走估计就不简单了 面试官不菜 我从跟他聊问题的时候我能感觉得到他各个东西都说的很深入 虽然我啥也没记住 哈哈哈哈

在面试的时候语气基本上跟两个很熟悉的朋友打电话一样  
你要是唯唯诺诺 回答问题不行 别人一听你就是个新手啥都不懂 像我的面试 我哪怕不会 不懂 我都能跟面试官聊的比较开心 如果你被动了 那么他就会出各种乱七八糟的问题 甚至是你的盲区问题给你 所以回答问题的时候如果会的东西一定要把回答问题的主权把握在自己手里 最好能够自问自答进行全方位的理解说明

很多东西你不会 但是你的态度方面以及回答问题的方式是很重要的 我这问答里面其实有很多心理问题 大家可以多多研究 其实我从头到尾并没有回答太多的问题但是面试官就觉得我很不错 为什么呢？ 大家可以仔细品。

**给大家的建议：**

建议大家在学完一个东西之后 把这个东西全方位给了解透

打个比方： 我sql注入我从基础注入各种原理到方法以及waf绕过 防护 写shell我各种我都了解的透透的 假如HR问说一下sql注入原理？

A回答：sql注入的原理是用户写入的数据被当做后端代码执行

B回答：sql注入的原理是用户写入的数据被当做后端代码执行，然后方式方面的话有 盲注 报错注入 偏移注入 DNS外带注入……..waf方面绕过的话…..在写shell方面首先有四个条件 要有写入权限…….有几种方法…..

最好是回答完了之后再说一下对sql注入的看法

假如你是HR 我就问了一个问题：你对于A B的回答你会觉得他们谁的能力更强？

是不是很多东西不用问了都心里有个底了？