**面试公司：某汽车公司**

**所在城市：北京**

**面试职位：渗透测试工程师**

**面试官问题：**

**1.自我介绍**

答：自我介绍面试必问问题，多介绍自己项目上突出的地方以及你以后的发展方向。

**2.CSRF和SSRF的区别以及修复方式**

答：**原理：**CSRF为客户端的请求伪造，他是通过攻击者构造恶意Payload诱骗在登录状态下的管理员去点击触发，最常见的就是XSS+CSRF打组合拳。SSRF为服务器端的请求伪造，产生原因是由于服务器端对参数的过滤不严格，导致攻击者可以构造恶意Payload去访问外网无法访问的资源。一般用来探测内网服务、开放端口或者是使用伪协议读取 本地文件。  
**区别**：CSRF与SSRF的主要区别就在于发起请求的目标不同，一个为客户端，一个为服  
务器。而且SSRF主要利用与内网探测。  
**修复方式**：CSRF：首先是验证求中的referer值（不推荐）或者是在关键GET或POST；请求中加入随机Token校验。 SSRF：限制请求只能是http或https、限制不能访问内网IP再者就是限制后端打印返回信息。

**3.说一下你在实战中遇到的比较典型的漏洞。**

答：这种问题可以回答你在项目或者SRC上挖到的比较有意思的漏洞或者自己认为很有成就感的挖洞经验。

**4. 说一下绕WAF的常见手段**

答：常见绕WAF的方法有关键字大小写绕过、URL编码或二次编码、双写绕过、注释绕  
过、参数污染或者使用一些不常见的函数、cookie注入。然后拓展说一下waf机制……

**5. SSRF如何进行绕过**

答：对内网IP地址进行编码或者是缩写例如10.0.0.1地址就可以写成10.1、对url解析不当可以使用@符拼接IP地址进行绕过、通过生成短链接绕过、伪协议绕过。

**一面主要是技术面，面试难度很基础，感觉甲方还是愿意培养一些爱学习爱专研的同学。二面就是人事问了一些具体情况。**

**面试结果：通过**

**面试难度：简单**

**面试公司：启明星辰**

**所在城市：北京**

**1. Nginx解析漏洞了解多少？**

答：Nginx解析漏洞是由于Nginx配置中匹配到.php结尾的请求，就会发送给Nginx  
的cgi解析器进行解析。我们可以通过空格和截断符上传.php小马来绕过检测，从而拿到shell。然后拓展说了一下Nginx存在的其他漏洞，Nginx还存在CRLF注入（在请求包中构造恶意的\r\n实现Cookie伪造或者是构造XSS等）；还有整数溢出造成的信息泄露。

**2. Weblogic、solr、tomcat中间件漏洞了解吗？**

答：WebLogic（是用于开发、集成、部署和管理大型分布式Web应用、网络应用  
和数据库应用的Java应用服务器。）  
Weblogic在使用T3协议加载远程资源，通过绕过反序列化黑名单，攻击者通过T3协议远程执行命令。一般通过nmap或者一些第三方扫描工具查看7001端口和对应服务版本。要不就是通过Poc先盲打，探测存在在使用exp进行利用。再者就是使用JAVA的一些weblogic漏洞利用工具。  
**修复方式：**打补丁或者升级到较高的版本。或者通过黑名单禁用特殊的类。  
Tomcat（小型轻量级Web应用服务器）7.0版本存在PUT方法可直接写文件到目标服务器。  
**绕过方法：**后缀名+空格绕过、后缀名+/绕过、文件流绕过::$DATA（Windows把上传的文件当做文件流进行处理从而不会检查文件名后缀是否合法）。  
Tomcat 9.X、8.X、7.X因配置文件打开了AJP协议（8009端口）导致根目录下任意文件读取，也可通过文件解析将任意文件解析为.jsp文件，但须配合文件上传进行利用。  
Tomcat弱口令 通过弱口令直接登录管理后台，通过后台上传wai文件功能直接getshell。  
Solr（Java开发的开源搜索服务器）反序列化是由于低版本的solr中ConfigAPI接口存在不安全的配置，使Solr中反序列化函数可以通过构造payload来达到远程命令的执行。  
修复方式：禁用ConfigAPI（disable.configEdit=true）、配置访问控制策略只允许受信任的IP进行访问。最好的方法还是升级到较高的版本。

**3.反序列化了解吗？**

答：序列化相当于相当于存档，将当前的运行状态保存到硬盘方便下次直接调用，  
而反序列化相当于读档，通过反序列化函数将保存的状态读取出来。产生漏洞的原因就在于反序列化函数参数可控，导致一些魔术方法(**construct()、**wakeup()、\_\_destruct())被调用，从而执行一些危险函数。

**4.Phpmyadmin弱口令登录后getshell的几种方法？**

1)包含日志文件getshell  
2)Into dumpfile 或into outfile 写马  
3)数据库慢查询日志（简单的说就是在mysql中，查询超过10秒的语句会被写到慢查询日志文件中去，一般默认是不开启的]）  
条件：目标站点存在phpMyAdmin和l.php探针;知道mysql登录密码;secure\_file\_priv未开启  
4)使用错误日志getshell  
5)利用phpmyadmin4.8.x本地文件包含漏洞getshell

**面试官主要问了一些当前主流的一些中间件漏洞，当时对这些中间件还不是太了解，所以回答的并不是太好，上述这些答案是自己私下自己查资料总结到的。**

**面试结果：未通过**

**面试难度：中等**

这几次面试总结出来一些经验，感觉基础一定要打好才可以，业余时间一定要多看风哥的回放，多做笔记，面试前一定要多看笔记加深映像！