大厂安全工程师实习面试题

笔记本：	web安全		
创建时间：	2019/8/27 18:51	**更新时间：**	2019/8/27 18:52
作者：	guihuozhiling		

大厂安全工程师实习面试题

绿盟：

1.解释一下对SQL注入的理解以及防御的手段
2.ssrf听说过吗？xxe呢？

知道创宇：

1.介绍一些后台拿shell常见的场景
2.SQL注入拿shell的方式
3.SqlMap会用么？怎么通过Sql注入写基本Sql命令？
4.Ssrf了解么？可以怎么判断有没有这个漏洞？
5.溯源能力
6.获取知识的手段
7.有没有内网渗透的经验
8.各大SRC的排名，是否挖到过高危
9.介绍一个挖到的最有趣的漏洞

长亭科技

1.SQL注入怎么拿shell
2.Xss怎么绕waf
3.waf和ips的绕过区别和一些技巧
4.对于平时爆的漏洞会去复现吗？有没有代码审计的基础
5.内网渗透怎么样，怎么反弹命令。

360：

1.PHP中命令执行的函数以及会出现的问题
2.PHP中系统执行的函数以及会出现的问题
3.变量覆盖问题
4.有没有审计到什么漏洞
5.问了一些漏洞的名字和问了下形成原因

6.渗透中常见的端口以及是什么应用
7.Ssrf中怎么拿shell、还有一些绕过方式
8.Xss的一些绕过方式，如果在href中可以用什么编码绕过以及网页渲染中他对不同编码的渲染前后顺序。
9.记忆中比较深刻的渗透经历
10.内网渗透怎么样
11.如果打到内网怎么反弹shell
12.打到内网会干什么
13.扫端口用什么扫
14.扫什么端口为什么这样
15.memcache放大攻击聊了下。

阿里云：

1.tcp的一些细节，然后ddos tcp洪水攻击和防护的一些问题
2.linux中的一些命令，问了下怎么看一个进程他都调用了什么文件
3.linux中密码文件在哪里
4.为什么普通用户（非Root权限）可以修改密码 因为修改密码需要修改/etc/passwd或者/etc/shadow文件，可是这两个文件都是需要root权限才能修改的
5.http2.0和1.0的区别。
6.xss浏览器的防护头。csp
7.怎么检测Sql注入和Xss漏洞的
8.Ssrf了解么。一些绕过技巧，rebind听说过么。gopher的原理。怎么拿shell
9.怎么绕waf
10.代码审计怎么样
11.ssrf应该怎么检测

腾讯：

1.怎么检测SQL注入、xss
2.平时复现漏洞吗，讲几个
3.命令执行的一些绕过方式
4.ssrf的绕过
5.xss的防护手段
6.输入过滤和输出过滤哪里好
7.SQL给了一个场景怎么注入
8.SSRF怎么检测、怎么防御
9.xss生成原因
10.SQL注入怎么防御