**常见面试题**

介绍一下自认为有趣的挖洞经历（或CTF经历）

你平时用的比较多的漏洞是哪些？相关漏洞的原理？以及对应漏洞的修复方案？

你平时使用哪些工具?以及对应工具的特点?

如果遇到waf的情况下如何进行SQL注入/上传Webshell怎么做？

谈谈Windows系统与Linux系统提权的思路？

列举出您所知道的所有开源组件高危漏洞

描述一个你深入研究过的 CVE 或 POC

php/java反序列化漏洞的原理?解决方案?

如果一台服务器被入侵后,你会如何做应急响应?

介绍 SQL 注入漏洞成因，如何防范？注入方式有哪些？除了数据库数据，利用方式还有哪些？

常见的中间件解析漏洞利用方式

Windows、Linux、数据库的加固降权思路

如何绕过CDN获取目标网站真实IP，谈谈你的思路

如果给你一个网站,你的渗透测试思路是什么?

你实际的渗透测试经历等等

反弹 shell 的常用命令？一般常反弹哪一种 shell？为什么？

SSRF漏洞的成因 防御 绕过？

有哪些反向代理的工具，有没有实际的内网渗透经历？

**SQLi**

发现 test.jsp?cid=150 注入点，你有哪几种思路获取 webshell?

以下链接存在 SQL注入漏洞，对于这个变形注入，你有什么思路？

mysql注入点，用工具对目标站直接写入一句话，需要哪些条件？

Mysql的网站注入，5.0以上和5.0以下有什么区别？

sqlmap如何对一个注入点注入，sqlmap如何注入一个post的包?

你都了解哪些SQL注入的bypass技巧?

介绍 SQL 注入漏洞成因，如何防范？注入方式有哪些？除了数据库数据，利用方式还有哪些？

宽字符注入的原理？如何利用宽字符注入漏洞，payload如何构造及修复方案？

如何判断SQL注入，有哪些方法，说说你最常用的?

**浏览器知识**

如何设置可以跨域请求数据？jsonp是做什么的？

如果子域名和顶级域名不同源，在哪里可以设置叫他们同源，解释一下什么是同源策略？

同源策略，哪些东西是同源可以获取到的？

JSON和JSONP的区别？

JSONP劫持利用方式及修复方案？

JSON注入如何利用？

Ajax是否遵循同源策略？

CSP是什么？如何设置CSP？

不同浏览器之间，安全策略有哪些不同，比如chrome，firefox，IE

说说HTML5有哪些新的安全特性？

**XSS**

如何防范 XSS 漏洞，在前端如何做，在后端如何做，哪里更好，为什么？

黑盒如何检测XSS漏洞？

如果给你一个XSS盲打漏洞，但是返回来的信息显示，他的后台是在内网，并且只能使用内网访问，那么你怎么利用这个XSS？

如果叫你来防御蠕虫，你有哪些方法？

在社交类的网站中，哪些地方可能会出现蠕虫？

XSS持久化？

如果给你一个XSS漏洞，你还需要哪些条件可以构造一个蠕虫？

xss的发生场景？

XSS是什么，修复方式是？

**CSRF/SSRF**

CSRF、SSRF和重放攻击有什么区别？

防御CSRF都有哪些方法，JAVA是如何防御CSRF漏洞的，token一定有用么？

CSRF漏洞的本质是什么？

CSRF是什么？修复方式？

SSRF漏洞原理、利用方式及修复方案？Java和PHP的SSRF区别？

XML注入

XXE是什么？修复方案是？

**逻辑漏洞**

说出至少三种业务逻辑漏洞，以及修复方式？

越权访问(水平/垂直/未授权)

谈谈水平/垂直/未授权越权访问的区别?

越权问题如何自动化检测？

**Java考察**

java的MVC结构都是做什么的，数据流向数据库的顺序是什么？

了解java沙箱吗？

ibats的参数化查询能不能有效的控制sql注入？有没有危险的方法可以造成sql注入？

说说两次struts2漏洞的原理

ongl在这个payload中起了什么作用？

\u0023是什么字符的16进制编码？为什么在payload中要用他？

java会不会发生执行系统命令的漏洞？java都有哪些语句，方法可以执行系统命令？

如果叫你修复一个xss漏洞，你会在java程序的那个层里面进行修复？

xss filter在java程序的哪里设置？

说下java的类反射在安全上可能存在哪些问题

Java反序列化漏洞的原理?解决方案?

你都了解哪些java框架？

**PHP考察**

php的LFI，本地包含漏洞原理是什么？写一段带有漏洞的代码。手工的话如何发掘？如果无报错回显，你是怎么遍历文件的？

php反序列化漏洞的原理?解决方案?

php webshell检测，有哪些方法

php的%00截断的原理是什么？

php.ini可以设置哪些安全特性

php里面有哪些方法可以不让错误回显？

**常见中间件**

Redis未授权访问漏洞如何入侵利用？

说说常见的中间件解析漏洞利用方式

JAVA有哪些比较常见的中间件容器？

tomcat要做哪些安全加固？

如果tomcat重启的话，webapps下，你删除的后台会不会又回来？

常见的网站服务器中间件容器。

**数据库安全**

mysql表权限里面，除了增删改查，文件读写，还有哪些权限？

mysql安全要如何做？

sqlserver public权限要如何提权

Windows、Linux、数据库的加固降权思路，任选其一

mysql的用户名密码是存放在那张表里面？mysql密码采用哪种加密方式？

mysql数据库默认有哪些库？说出库的名字

mysql UDF提权5.1以上版本和5.1以下有什么区别,以及需要哪些条件?

**Linux操作系统**

简述Linux系统安全加固需要做哪些方面？

你使用什么工具来判断系统是否存在后门？

Linux的Selinux是什么？如何设置Selinux？

iptables工作在TCPIP模型中的哪层？

如果无法升级内核，那么如何保证系统不被已知的exp提权？

syslog里面都有哪些日志？安装软件的日志去哪找？

如何查询ssh的登录日志？如何配置syslog的日志格式？

syslog可不可以使用vi等工具直接查看？是二进制文件吗？

如果一台Linux服务器被入侵后,你会如何做应急响应?

反弹 shell 的常用命令？一般常反弹哪一种 shell？为什么？

**应急响应**

有哪几种后门实现方式？

webshell检测有什么方法思路？

Linux服务器中了木马后，请简述应急思路？

遇到新0day(比如Struts2)后，应该如何进行应急响应？

新业务上线前可以从哪些方向进行安全评估？

现有系统可以从哪些方向进行审计发现其中的安全风险？

**渗透测试**

判断出网站的CMS对渗透有什么意义？

如何清理入侵日志

总结渗透报告及修复方案

在渗透过程中，收集目标站注册人邮箱对我们有什么价值？

如果给你一个网站,你的渗透测试思路是什么? 在获取书面授权的前提下

DNS在渗透中的作用？