# 字节一面：

1. 介绍一下自己。
2. 问最近的XX漏洞是否熟悉
3. 介绍一下SDLC的流程；SDLC该怎么搞。
4. 拿到一个渗透的项目，要怎么搞。
5. SQL注入都有哪些类型。要怎么挖掘SQL注入漏洞。
6. 安全应急要怎么处理？来了一个漏洞要怎么排查？
7. 黑盒或者白盒的误判要怎么解决。
8. 经过防火墙的一段流量，没有检测的到攻击；但是产生了攻击，要怎么去找到攻击数据包。
9. 越权的漏洞在只有流量的情况下，没有其他的联动设备，的情况下是否能发现；要怎么去发现。
10. 网络攻击的检测方法。
11. 参与的项目未知流量攻击的检测方法。
12. 对于有签名的攻击要怎么回放。
13. APP的安全测试该怎么做（首先声明没搞过，然后说该怎么搞）
14. XXE漏洞要怎么防御。
15. SSRF漏洞要怎么防御。（没回答好）
16. 如何推动产品线去修漏洞。
17. 产品线不修漏洞有什么解决办法。
18. 自己有什么想问的吗？