2020/2/21 深信服北京攻防一面

2020/2/21-面试-问的问题比较宽泛，主要是让你自己描述

一、实习时间-地点

我投的北京攻防，不知道为啥短信给的是深圳的，然而面试官又是北京的，有点晕-去北京

二、学了安全多少年-在大学学了哪些东西

三、实战发现的问题描述一下

四、sql注入利用方式

五、数据库的一些提权姿势

mysql-redis-sqlserver一个个来慢慢讲

六、python熟不熟

七、ctf的经历

八、nmap你对哪些端口敏感

3306 6379 3389 21 22 80 8080 443 7001
然后问了445端口-局域网中轻松访问各种共享文件夹或共享打印机的-知识盲区
用过永恒之蓝么

九、分析过公开组件的漏洞

weblogic-tp5-shiro反序列化

十、http协议refer字段-有什么安全问题

refer的意思就是跳转来源的意思，也就是说refer:https://www.baidu.com就是用来添加百度网站的跳转
其他字段的安全
X-forwarded-For
Remote Address