Sec-Interview-4-2023

一个2023届毕业生在毕业前持续更新、收集的安全岗面试题及面试经验分享~

写在最前面

快一年没更新了。。。身份也从求职者转变到了打工人，刚好这段时间也不少师弟来问求职的问题，所以想着要不更一下吧，目前应该有80多篇面经了，有人想让我写个面经问题的答案，这个倒是有点偏离我一开始建这个仓库的目的了。。因为一开始就没想着“教人”面试，以后也不会有这个打算，这个仓库主要还是用于收集最真实的面试问题，展示面试都会问啥，而不是我应该答啥（关于公司投递链接的，我随便点了几个发现很多都改了，也有些是不收人了，我就不再更新链接了吧= =大家自行寻找投递方式）

写在更前面

和铺天盖地的研发、产品等校招宣讲和内推通知不同，安全岗位虽然在大多数公司中都属于“研发”下的一个分类，但是宣讲时很少会提到。。这就不得不我们自己去挖掘了，同时我也希望能有更多的招聘人员（或者有了解的直接发issue）能介绍一下自己公司的安全部门、部门平时的业务，对于学生来说也更容易找到适合自己技术特点或者自己感兴趣的部门。

写在前面

1. 个人强烈感觉面试因人而异，对于简历上有具体项目经历的同学，个人感觉面试官会着重让你介绍自己的项目，包括但不限于介绍一次真实攻防/渗透/挖洞/CTF/代码审计的经历 => 因此对于自己的项目，面试前建议做一次复盘，最好能用文字描述出细节，在面试时才不会磕磕绊绊、或者忘了一些自己很得意的细节
2. 面试题会一直更新（大概，直到我毕业或者躺平为止吧...）包括一些身边同学（若他们同意的话）和牛客上扒拉下来的（若有，会贴出链接）还有自己的一些经历
3. 还有一点很想说的，就是面试题/面经，本质上只是一种“见识”，他并不能实质上提升自己的水平，还是希望大家（包括我自己）不要太局限于面经，可以查缺补漏但没必要面经问什么自己就一定要学什么，按自己的节奏学就行了，毕竟每人的技术特点不一样，面试的过程和问题也会不一样

最后欢迎大家fork项目！xdm自己有面试经验的话也欢迎发pr！有分享就有收获！

若有不方便公开的内容请联系本人第一时间删除！

安全岗目录

有最新的公司校招信息可以随时issue，我会第一时间更新

以安全为主业的公司我就不放了（360、深信服、奇安信等），主要放不以安全为主业但有安全业务的公司

公司及投递链接	base	岗位	部门
字节跳动	北京、深圳、杭州	渗透测试工程师 安全研究工程师 安全工程师	安全与风控 无恒实验室
华为	基本全覆盖	网络安全与隐私保护工程师	基本覆盖
SHEIN	南京	安全工程师	无
大疆	上海、深圳	嵌入式系统安全工程师 功能安全工程师 安全技术开发工程师	研发团队 车载团队 信息管理团队
联想	北京、天津、厦门	安全工程师	IDG Lenovo Research
oppo提前批	深圳、成都	终端安全工程师（二进制、安卓、逆向类）	
网易雷火	杭州	游戏安全工程师（游戏、安全、二进制）	雷火事业群
蔚来	上海、北京、合肥	岗位较多，覆盖面大	
科大讯飞	合肥	安全工程师	
米哈游	上海	信息安全工程师（客户端） 安全运营	
Shopee	深圳（Sg暂未上线hc）	安全工程师	研发中心
百度	北京、成都	安全工程师 数据安全研究员 人工智能安全算法研发工程师	
网易	杭州	IOS安全开发 Android安全开发 安全运营专员（产品岗）	
网易游戏（互娱）	广州	安全工程师	

公司及投递链接	base	岗位	部门
海康威视	杭州	网络安全工程师 安全开发工程师 安全研究员（博士学历） 安全方案工程师	
4399	广州	信息安全工程师	
美团		安全工程师	
Garena	上海、杭州	信息安全工程师 安全逆向工程师	
AutoX	北上广深	信息安全合规工程师 安全开发运维工程师 嵌入式开发-安全工程师 后台开发工程师-安全服务	网络安全团队
快手	北京	安全工程师	工程类-安全
字节跳动正式批	北京、深圳、杭州	安全研究工程师 安全工程师 隐私计算研究员 渗透测试工程师	安全与风控 无恒实验室
完美世界	北京-朝阳区	安全分析工程师（提前批） 安全分析工程师	
京东	北京	安全工程师	
中国电信天翼云	北京、成都、厦门、广州	信息安全工程师（北京要求硕士及以上）	
拼多多		安全工程师	仅开放内推
阿里巴巴	杭州、北京、上海	安全工程师	
Zoom	苏州、杭州、合肥	应用安全工程师	
远景科技	上海	信息安全工程师	远景能源
贝壳找房	北京	安全研发工程师 安全工程师	
竞技世界	北京	安全工程师	
地平线	上海	安全工程师（信息/功能方向)-Auto	
小红书REDstar	上海	java开发工程师-安全 [机器学习算法工程师-安全技术	

公司及投递链接	base	岗位	部门
度小满	北京	信息安全工程师	
兴业数金	上海、福州、成都	信息安全工程师	
oppo	深圳、成都	终端安全工程师 互联网安全工程师 信息安全工程师	
小米	北京、南京	安全研发工程师 安全工程师 安全操作系统工程师	
vivo	深圳、东莞	安全工程师	
小鹏	广州、上海	信息安全培训生 系统安全软件工程师	
Momenta	深圳	信息安全工程师	
TCL	深圳	软件开发工程师（安全方向） 信息安全工程师	鸿鹄实验室（提前批） 软件工程中心
吉利	杭州、宁波	信息安全工程师 功能安全工程师 氪学家-信息安全/攻防方向 信息安全开发工程师 氪学家-车联网安全研究员	多个下属组织分开收
中兴	南京、长沙、西安、深圳	网络安全工程师	
滴滴	北京	安全工程师（密码开发、容器开发、接口安全、反入侵、移动安全） 安全算法工程师	CTO线 国际化事业部
顺丰科技	深圳	信息安全工程师（顺丰科技）	
微众银行	深圳、武汉	信息安全工程师（应用安全、信息安全管理、后端开发C++、反欺诈、安全攻防）	
腾讯音乐	深圳	安全策略	
TP-Link	深圳	网络安全算法工程师 信息安全工程师（深圳）	
携程	上海	基础安全工程师	
海尔	青岛	信息安全工程师	

公司及投递链接	base	岗位	部门
荣耀	北京、南京、深圳	网络安全工程师	
中国人寿	很多	很多	
格力	珠海	信息安全	
传音控股	上海、重庆	系统安全工程师（web、安卓、安全开发） 安全合规 安卓隐私安全开发	
美的	深圳、佛山、武汉	信息安全技术研发工程师 信息安全工程师	
西云数据	北京	信息安全工程师	
工商银行	北京、广州、杭州、珠海	科技菁英-安全技术	
欧科云链	北京	安全开发工程师	
建信金科	北京	信息安全工程师（实施管理中心）	
阳光保险	北京	信息安全工程师（安全运维/安全开发）	
奕斯伟	北京	信息安全工程师	
58同城	北京	安全工程师	
金发科技	广州	信息安全工程师	
东方财富	上海	信息安全岗位 信息安全开发工程师 信息安全咨询师	
中金所	上海	运维工程师-网络安全技术方向	硕士+
中国电信天翼云	北京、成都、厦门、广州	信息安全工程师	北京需要硕士+
浩鲸科技	南京	安全工程师	
商汤科技	北京、深圳		
三一重工	长沙	信息安全工程师	硕士+
经纬恒润	较多	较多	
理想	北京、杭州	安全研发工程师 安全运营工程师 安全测试工程师 信息安全合规专员	

公司及投递链接	base	岗位	部门
中国一汽	长春	车联网安全工程师 信息安全工程师 电子电气网络及安全软件工程师	
中国系统	北京、武汉	安全工程师 数据安全工程师	
蚂蚁集团	北京、上海、杭州、重庆、成都	安全工程师	
联易融	深圳	信息安全工程师	
海信集团	佛山、青岛	网络安全工程师	
人保寿险	福州、上海、佛山、南京	信息安全、基础安全、应用安全、数据安全	
途虎养车	上海	信息安全工程师	
零跑科技	杭州	信息安全工程师 信息安全开发工程师	
腾讯	深圳、北京	安全技术	

好文分享

我的秋招安全之路

作为安全工程师，都有哪些可选择的公司？

安全岗笔试题

部分安全岗汇总（牛客）

部分牛客安全岗面经

一个双非安全菜鸡的秋招总结

目录

- 0x00 字节跳动-渗透测试实习生
- 0x01 阿里云安全实习
- 0x02 深信服-漏洞研究员实习
- 0x03
- 0x04 字节跳动-安全研究实习生
- 0x05 长亭科技-安全服务工程师
- 0x06 天融信面试复盘
- 0x07 腾讯-安全技术实习生
- 0x08 小鹏汽车-安全工程师
- 0x09 阿里巴巴-阿里云安全
- 0x0A
- 0x0B 字节跳动-无恒实验室
- 0x0C 58同城-安全工程师

- 0x0D 腾讯-玄武实验室
- 0x0E 360-安全工程师
- 0x0F 快手-安全实习生
- 0x10 华顺信安-安全服务工程师
- 0x11 奇安信面试复盘
- 0x12 京东-安全研发
- 0x13 安恒面试复盘
- 0x14 浙江东岸检测
- 0x15 360-安全工程师实习
- 0x16 某一线实验室实习
- 0x17 腾讯-科恩实验室实习
- 0x18 某四字大厂面试复盘
- 0x19 某四字大厂实习面试复盘
- 0x1A 某两字大厂面试复盘
- 0x1B 某安全公司-安全研究员
- 0x1C 腾讯-科恩实验室实习
- 0x1D 长亭科技 安全服务工程师实习
- 0x1E PingCAP 安全工程师
- 0x1F shopee
- 0x20 深信服
- 0x21 华为
- 0x22 360
- 0x23 深信服-深蓝攻防实验室
- 0x24 B站
- 0x25 shopee-红队-Singapore
- 0x26 长亭
- 0x27 奇安信 安全研究员 实习
- 0x28 美团 安全岗实习
- 0x29 美团 安全工程师实习
- 0x2A 京东 安全研究
- 0x2B 百度
- 0x2C 腾讯
- 0x2D 奇安信 A-TEAM
- 0x2E 快手 安全工程师
- 0x2F 快手 安全实习生
- 0x30 快手 安全工程师
- 0x31 快手 安全工程师
- 0x32 蚂蚁 安全工程师 实习
- 0x33 蚂蚁 安全工程师 实习
- 0x34 商汤科技 安全开发工程师
- 0x35 海康威视 网络安全工程师
- 0x36 度小满 信息安全工程师
- 0x37 长亭 安全开发工程师
- 0x38 小米 安全工程师
- 0x39 携程旅游 基础安全工程师
- 0x3A 欧科云链 安全开发
- 0x3B 大疆 安全技术开发工程师
- 0x3C 经纬恒润
- 0x3D 微众
- 0x3E 百度

- 0x3F 米哈游
- 0x40 传音控股
- 0x41快手 安全工程师
- 0x42 腾讯
- 0x43 海尔
- 0x44 4399
- 0x45 滴滴
- 0x46 海康威视
- 0x47 字节跳动 安全工程师
- 0x48 美团 安全工程师
- 0x49 vivo
- 0x4A 小米
- 0x4B TCL 鸿鹄实验室 软件开发工程师（安全方向）
- 0x4C 京东 安全工程师
- 0x4D 阿里-菜鸟
- 0x4E 完美世界 安全分析工程师
- 0x4F 深信服 漏洞研究员
- 0x50 联想
- 0x51 商汤
- 0x52 竞技世界
- 0x53 度小满
- 0x54 绿盟 梅花K
- 0x55 中兴-未来领军-软件开发工程师-网络安全
- 0x56 美团
- 0x57 安恒-卫兵实验室
- 0x58 白帽汇-安全研究
- 0x59 极氪-安全研究
- 0x5A 奇安信-观星实验室
- 0x5B 沥泉科技-红队安全研究
- 0x5C 二进制安全面经汇总
- 0x5D 忆享科技面试 北京渗透岗
- 0x5E 悬镜安全 成都安全开发
- 0x5F 中安网星面试 红队攻防开发
- 0x60 重庆绿盟面试 红队攻防开发
- 0x61 北京微步在线 安全开发
- 0x61 成都卫士通 物联网安全研究
- 0x61 成都数默科技(科来) APT研究
- 0x62 传音控股上海 安全开发
- 0x63 绿盟成都-安全服务国际部 安全服务
- 0x64 成都360 安全研究
- 0x65 成都360 车联网安全
- 0x66 杭州极氪科技 安全研发
- 0x67 成都四叶草安全 安全研发
- 0x68 成都民生银行
- 0x69 亚信安全 安全分析
- 0x6A 头条
- 0x6B 腾讯-云鼎实验室
- 0x6C 腾讯云安全
- 0x6D 蚂蚁金服
- 0x6E 360企业安全

- 0x6F 58集团
- 0x70 海康威视
- 0x71 顺丰科技
- 0x72 平安科技
- 0x73 360
- 0x74 哔哩哔哩
- 0x75 百度
- 0x76 腾讯
- 0x77 360
- 0x78 华顺信安
- 0x79 某步
- 0x7A 绿盟
- 0x7B 360
- 0x7C 奇安信
- 0x7D 深信服
- 0x7E 大疆
- 0x7F 华为

致谢

感谢 `PolarPeak` 、 `lalalashenle` 、 `4ra1n` 、 `底层群员` 、 `TARDIS` 、 `Theoyu` 、 `hurricane618` 师傅的分享！

0x00 字节跳动-渗透测试实习生

> 字节直接找朋友内推的效率很高，当天上午投简历，下午就约了面试，裸面挺痛苦的建议复习一下再去

1. 自我介绍
2. 渗透的流程
3. 信息收集如何处理子域名爆破的泛解析问题
4. 如何绕过CDN查找真实ip
5. phpinfo你会关注哪些信息
6. 有没有了解过权限维持
7. 说一个你感觉不错的漏洞，展开讲讲
8. 输出到href的XSS如何防御
9. samesite防御CSRF的原理
10. CSRF防御
11. json格式的CSRF如何防御
12. 浏览器解析顺序和解码顺序
13. 过滤逗号的SQL注入如何绕过
14. 过滤limit后的逗号如何绕过
15. fastjson相关漏洞
16. 说一个你知道的python相关的漏洞（SSTI原理，利用过程,payload相关的东西）开放性问答

0x01 阿里云安全实习

时长：20分钟

1. 自我介绍
2. 看你简历上说擅长java、php代码审计，也没有类似的经历能够分享一下，比如说独自审的一套代码或者开源项目，从中发现的一些比较高危的问题
3. 在审项目的时候，比如一个web网站，简单说说思路
4. 简单描述一下什么是水平越权，什么是垂直越权，我要发现这两类漏洞，那我代码审计要注意什么地方
5. 解释一下ssrf
6. 怎么防御ssrf，场景：`http://ip/?url=image.jpg`
7. 常见的内网段有哪些，他们的掩码是什么
8. 教育系统攻防演练，分享一个渗透的例子
9. 除了学校，有没有试过渗透别的系统
10. 像这样的场景（给内网靶标），渗透内网系统的思路
11. 反问环节（问了工作内容）
    - 岗位做的是阿里云云平台安全，内部安全保障，保障阿里云自身的安全不出问题，整个系统的上线前中后过程，每个方向都有人

0x02 深信服-漏洞研究员实习

时长：15分钟

1. 自我介绍
2. 在xx实习的时候做什么东西
3. 渗透测试的思路简单说一下
4. 护网在里面担当一个什么样的角色
5. 红队的一些思路
6. 拿下系统后有没有做横向
7. 前段时间那个log4j有研究吗，可以简单说一下吗
8. （继上一个问题）有哪些混淆绕过的方法
9. 内存马有没有了解过
10. 冰蝎、哥斯拉这些工具有没有了解过
11. 做攻击队的时候有没有研究过什么攻击，比如研究一些工具还是魔改什么的
12. 那么多漏洞和攻击，比较擅长哪一个
13. 说一下shiro反序列化的形成原因、利用链
14. 对一些bypass的方法有没有了解过，有什么姿势可以简单介绍一下
15. 反问

0x03

0x04 字节跳动-安全研究实习生

一面

时长：50分钟

1. 你投的岗位是安全研究实习生，你了解我们这边主要是做什么的吗
2. 自我介绍

3. 现在有什么比较想做的方向吗，比如你写的代码审计、攻防演练、你在学校的研究方向（密码学）其实是三个大方向，现在有什么比较想做的吗
    - 说了代码审计、安全研究
4. 有没有审过开源框架、cms、中间件之类的
5. 面试官介绍了工作内容
6. 我看你简历上有几段实习经历和项目经历，先聊一下实习经历吧，在A主要做什么的
7. 详细聊聊入侵检测主要在做什么，遇到的问题
8. 关于入侵检测产生大量误报的原因，有没有分析过，有没有比较好的解决方法
9. 和A比起来，B的应该就比较偏攻击方对吧，有打仗（雾，面试官好像确实是这么说的）有代码审计，聊一下在B主要做了些什么
10. 审表达式引擎的步骤和思路
11. 刚刚你说的审计听起来好像和普通开发的审计差不多，都是通过程序流、文档去做，有没有从安全方面入手审计一些项目
12. xxe是怎么造成的，从代码层面来看
13. 我看你简历有很多攻防演练经历对吧，这几段攻防演练经历有没有哪一次印象比较深刻的，挑一个聊一聊
14. 你的这次攻击好像更多的是利用弱口令，有没有一些更有技巧的方法
15. 这个头像上传的webshell是怎么上传的
16. 还有什么其他的检验方式？要怎么绕过？
17. 这两天log4j漏洞很火，有没有去了解一下
18. 面试官最后介绍业务
19. 反问环节

一面plus-安全研发实习生

> 很奇葩的剧情，一面面试官面完告诉我有base北京base深圳问我是不是想要深圳的，我说是，结果过了一个多星期hr告诉我因为我一面面试官是北京的，然后我选了深圳，所以一面不作数，重新约了一面
>
> 接着一面这天中午又收到了感谢信，然后看官网状态是流程已终止，本以为没得面了没想到还是正常进行....

> 等到二面才发现原来已经变成安全研发了，本来我投的是安全研究的...

时长：45分钟

1. 自我介绍
2. A护网做了什么
3. 做哪一层的处置，waf？ids？
4. 遇到的问题是什么，有什么印象深刻的处置
5. 怎么解决误报过多的情况，有做过什么规则能解决这个情况的
6. 他的内网误报是在办公网还是生产网
7. 比如mysql也会执行powershell，怎么做防护（前面说了很多内网误报是因为有人写了ps脚本触发的）
8. 有没有挖过src
9. 在做攻防的时候，资产收集这块有没有什么经验介绍的
10. 一个单位的一级域名可能不止一个，怎么收集某个单位的所有域名，注意不是子域名

11. 还有没有其他的资产收集的经验
12. 除了信息收集，有没有什么漏洞方面的攻击案例
13. 聊一下sql注入
14. 怎么防御
15. 遇到order by时怎么防御
16. 用转义字符防御时，如果遇到数据库的列名或是表名本身就带着特殊字符，应该怎么做
17. 宽字节注入
18. ssrf了解吗
19. 怎么修复
20. 基于黑白名单的修复，现在的生产基本都是用的docker，ip是随时变的，而且docker重启后可能什么都不一样了，怎么做一个修复
21. fastjson反序列化
22. redis的漏洞
23. mysql的提权
24. shiro反序列化
25. 最近很火的log4j，聊一下原理
26. jndi的解析流程和原理
27. 有没有什么你做的比较好的地方我没有问到的，可以聊一聊
28. 惯例介绍部门的主要业务
29. 惯例反问

二面

> 紧接在一面plus后，就隔了10分钟，一面复盘写一半就开始二面了

时长：25分钟

1. 聊攻防演练中比较得意、印象深刻的一次经历
2. 安全领域比较擅长什么
3. 审的一般是什么，java？python？
4. csrf了解吗，怎么做一个修复
5. 在拿到java系统的代码时，审计的流程是怎样的
6. java系统中的sql注入怎么做一个防御和修复
7. 在浏览器中输入一个域名去访问时，浏览器做了什么
8. 一个系统的登录页，通常可能出现什么漏洞
9. 云安全了解吗
10. 有做过安全工具的开发吗，比如waf或者扫描器之类的
11. 惯例介绍业务
12. 惯例反问

0x05 长亭科技-安全服务工程师

一面

时长：30分钟

1. 自我介绍
2. web渗透测试有没有过实战
3. 讲一下sql注入原理
4. 有没有从代码层面了解过sql注入的成因（反问代码层面指的是不是sql语句，答是）
5. 了不了解xss，有没有从代码层面了解xss的原理
6. 对owasp top10漏洞哪个比较了解

7. 讲一讲怎么防御sql注入
8. sql注入怎么绕过过滤
9. 问了护网时xx有没有成为靶标，有没有对攻击队行为做过研判
10. 在xx护网时的工作内容，有没有做过流量包、数据包的研判
11. 学校攻防演练时担任的角色，主要工作内容，渗透测试的思路，有什么成果（这个问的还是挺细的，具体到分配的任务、有没有拿下主机或者域控、攻防演练的形式和持续时间等都聊了）
12. 平时ctf打的多不多，有什么成绩
13. 平时会不会关注一些新颖的漏洞，会不会做代码审计，比如shiro漏洞等有没有做过漏洞复现
14. 对钓鱼邮件这些有没有什么了解（因为上面聊xx护网时说了钓鱼邮件和微信钓鱼的事）
15. 目前学习的方向是什么
16. 最后介绍人才需求
17. 反问环节

二面

时长：34min

1. 自我介绍
2. 学代码审计偏哪个语言？擅长哪个语言
3. 拿到一份php代码做审计，审计的流程大概是怎样的
4. 对php开发框架熟吗？比如ThinkPHP这些
5. 给的源码是ThinkPHP框架的话，审计起来和没有使用框架的有什么不同，从流程上或者从关注的点上有什么不同
6. php原生的敏感函数有哪些，比如搜关键字的话会搜哪些
7. 反序列化漏洞了解吗
8. 反序列的时候，unserialize()反序列一个字符串的时候，对象会有一些魔术方法会被自动调用到，在找反序列化的链时，有哪些魔术方法是可以作为一个入手点去找的
9. 有没有审计过实际的项目，比如github上一些开源cms
10. java审计可以聊一下吗
11. 之前做渗透时有没有做过完整的项目，除了ctf
12. 能不能说一些找到的漏洞，怎么找到的
13. ssrf这类的漏洞熟悉吗，说一下原理和利用方式
14. 我们利用ssrf可以做什么，达到什么效果
15. 在php环境下，怎么最大程度的利用ssrf，拿到shell或者进内网
16. 怎么利用内网的机器请求内网中的服务
17. ssrf漏洞的修复建议，修复的时候需要注意哪些细节
18. 如果用白名单策略修复ssrf，从用户输入的变量里拿出要访问的目标，这个要注意哪些，因为一些url会通过特殊的字符做白名单绕过，对取变量这个操作有哪些要注意的细节？
19. php中三个等号和两个等号有什么区别
20. php代码常见入口函数怎么找
21. 有一些php的开发框架可以帮我们做一些url路由，对这些路由的方法熟悉吗
22. 介绍下PHP的变量覆盖
23. 有一个php的程序，本身就允许文件包含的操作，同时想要避免文件包含漏洞，写代码的时候要注意哪些
24. 远程文件包含和本地文件包含，这两种涉及的php设置有什么
25. 本地文件包含能不能通过php配置限制文件包含的路径（不通过代码直接通过配置项来解决）
26. php、java代码审计对哪个漏洞特别熟悉
27. php在做sql注入防御时有哪些方法
28. java做sql注入的防御
29. sql的二次注入了解吗，能介绍一下吗
30. 写代码的时候怎么防止二次注入

0x06 天融信面试复盘

时长：15~20分钟

1. 有没有做过现实环境的渗透测试？有没有提交过src？
2. 对免杀技术了解多少，制作的木马能不能过360
3. ctf的成绩？擅长什么方向的题？
4. 攻防演练有什么成果？
5. shiro漏洞了解吗，讲一下原理
6. 在linux下，现在有一个拥有大量ip地址的txt文本文档，但是里面有很多重复的，如何快速去重？
7. 在内网渗透中，通过钓鱼邮件获取到主机权限，但是发现内网拦截了tcp的出网流量，聊一下这个时候应该怎么进行通信？
8. 代码能力怎样，平时有没有做过代码审计？
9. 目前对什么方向感兴趣？

0x07 腾讯-安全技术实习生

时长：15分钟

1. 自我介绍
2. sql注入了解吗，讲一讲二次注入的原理
3. 二次注入要怎么修复
4. sql注入过waf了解吗，若一个sql注入过滤了information关键词，怎么绕过
5. Redis未授权访问
6. 渗透测试的一个完整流程
7. 打ctf的时候有没有遇到什么印象特别深的题目
8. 文件下载漏洞有没有什么比较好的利用方式
9. 利用文件下载漏洞找文件名具体是找什么文件名（读取文件一般会读取哪些文件）（ctf中？实战中？）
10. 命令执行漏洞，http不出网有什么比较好的处理方法（发散一点说）
11. 接上一题，通过隧道通信，详细讲讲通过什么类型的隧道，讲讲具体操作
12. 漏洞预警
13. 有没有复现过中间件类型的漏洞（有没有完整的复现过漏洞）
14. 在学校的攻防演练中扮演的角色的主要职责是什么

0x08 小鹏汽车-安全工程师

时长：37分钟

1. 自我介绍
2. 有没有挖过src？
3. 平时web渗透怎么学的，有实战吗？有过成功发现漏洞的经历吗？
4. 做web渗透时接触过哪些工具
5. xxe漏洞是什么？ssrf是什么？
6. 打ctf的时候负责什么方向的题
7. 为什么要搞信息安全，对安全这一块有多大的兴趣，以后会不会转行，还是打算一直从事安全方面工作
8. 自己平时怎么学安全的，如果让你做一个新的方向（app安全），会投入多少时间去学习，还是说有自己想做的方向
9. 聊一聊代码审计的流程
10. 平时是怎么做代码审计的

11. 有没有审计过开源框架、CMS?
12. 怎么判断一个数据库是mysql还是oracle的?
13. sql注入的种类，利用方式?
14. 聊一聊sql注入的原理及防御思路
15. 做开发的时候用的是什么语言
16. 做java开发的时候用过什么框架，能不能做java安全开发
17. 有没有做过安卓开发
18. 有没有用python写过工具?
19. msf利用的是哪个漏洞，有没有成功反弹?
20. 护网的时候主要做了些什么，聊一聊对安全产品的理解
21. 公司现在需要做app安全的人，现在要你做的话，你会去学吗，或者说感兴趣吗，还是说有别的想做的，不想做app安全，能投入多少时间去学
22. 内网渗透了解吗？聊一聊内网渗透的思路

> 接下来从0x09~0x0B都是同一位博主的面经，发在牛客上，看了下感觉很不错就转过来了，再附上这个博主的一些面试题/学习笔记的链接，个人觉得挺好的
>
> CSDN 网络安全-常见面试题
>
> CSDN 网络安全-自学笔记

0x09 阿里巴巴-阿里云安全

作者：宠你＆我的天性

链接：https://www.nowcoder.com/discuss/642461?source_id=profile_create_nctrack&channel=-1

来源：牛客网

一面

1. 自我介绍一下，讲一下课题和课外实践?
2. WAF管理平台后端API有做过压力测试吗?
3. 你现在的论文已经发表了吗?
4. 你的毕业论文是什么?
5. 在字节跳动训练营最大的收获是什么?
6. 在研究生期间或日常生活中有什么可以分享的有意义的事情?
7. 快排的时间复杂度是多少?
    - 最快的情况下是多少？是什么样的情况?
    - 最慢的情况下是多少？是什么样的情况?
8. 哈希冲突有哪些解决办法?
9. 编程题(easy)

二面

1. 自我介绍一下?
2. 我们这里是密码管理服务，密码这块你了解多少呢?
3. 你未来计划更偏向于安全研究还是安全研发?

4. 你对云上PKI的安全，身份认证的能力感兴趣吗？
5. 介绍一下字节跳动训练营做了什么？
    - Sql注入的原理和防御方案有哪些？
    - WAF防护SQL注入的原理是什么？
    - 本次训练营中，怎么分工协作的？你的角色是什么？你的贡献是什么？有没有提升效率的可能？
    - 漏洞挖掘是纯工具还是有一些手工的？
    - WAF管理平台后端API有哪些功能？
    - WAF的增删改查数据量大吗？
    - Redis解决了什么问题？
    - 热点数据怎么保证redis和db中的一致？
    - 用户登录认证是怎么做的？
    - Token的安全怎么保护？
    - Token的内容该如何设计？
    - 怎么保证数据不被篡改呢？
6. SDN漏洞挖掘的思路？
    - 漏洞挖掘有挖掘出RCE漏洞吗？
    - 对栈溢出、堆溢出有研究吗？
7. 说一下https协议的过程？
    - 随机数一般有几个？
    - 如果有一个的话会如何？
8. 对C++或C熟悉吗？
9. 哈希表的原理和冲突解决办法？（和一面重复了）
10. Mysql查询快的原因？
    - 事务的四大特性，mysql隔离级别？
    - 解释一下乐观锁和悲观锁？
11. 多并发编程有涉及过吗？
    - 读写锁和互斥锁/排他锁用过吗？有什么区别？为什么会用？
12. 有一项软件著作权，做的什么软件？
13. 编程题(medium)

三面（交叉面）

1. 字节跳动训练营越权问题解决办法？
    - 防火墙都是自己写的规则去防御吗？
    - 任务都是一样，你们得了第一，你们团队做的好的地方在哪里？
2. SDN漏洞挖掘项目，你能列举一个比较有技术含量的漏洞吗？漏洞原理和挖掘过程？
3. Python2和Python3的区别？
    - Xrange和range返回的是什么？
4. 数据库索引的作用？mysql索引的变化？
5. 数据库弱口令，登进去后如何提权？
6. 你自己写项目的时候，怎么进行的 SQL注入防御？
7. 怎么进行CSRF防御？
    - Token加密什么东西？
    - 校验什么？

    - Token为什么需要加密?
    - 使用明文随机数可以吗?
8. 怎么防重放攻击？
9. Docker有哪些安全上的好处?
10. 个人发展方向?
11. 当前在哪里日常实习?
12. 实习多久了？为什么想来阿里?

0x0A

0x0B 字节跳动-无恒实验室

部门：无恒实验室

岗位：安全工程师

作者：宠你＆我的天性

链接：https://www.nowcoder.com/discuss/749954?source_id=discuss_experience_nctrack&channel=-1

来源：牛客网

---

1. 自我介绍
2. 阿里巴巴实习介绍?
3. 启明星辰实习介绍?
4. 消息队列是自研的，还是开源的？叫什么名字?
5. 任务下发？状态监测
6. 子域名扫描插件怎么写的?
7. 指纹识别插件怎么写的?
8. wappalyzer怎么进行指纹识别的?
9. CSDN的XSS漏洞挖掘过程?
10. SQL注入的原理?
11. 目前防御SQL注入的方式有哪些?
12. 有哪些SQL语句无法使用预编译的方式?
13. SQL注入如何判断注入点?
14. 已知example.com/?id = 1，是mysql，如何获得mysql版本?
15. 无回显情况下怎么弄？ceye dnslog外带
16. 除了外带呢?
17. CSRF的原理?
18. CSRF使用POST请求时，如何攻击？隐藏表单
19. 不是表单呢?
20. AJAX发送POST请求?
21. Ajax发送POST请求会发几个数据包?
22. 让你来写一个CSRF攻击插件，你怎么写？包含哪些模块?

23. SSRF的原理?
24. 让你写一个SSRF插件，你怎么写?
25. 反问环节

0x0C 58同城-安全工程师

岗位：安全工程师

作者：Lamber-maybe

链接：https://www.nowcoder.com/discuss/766311?source_id=discuss_experience_nctrack&channel=-1

来源：牛客网

---

1. 你先做个自我介绍吧
2. 假如说有个SQL注入如下

```
select * from user where userid = {};
```

   1. response里面没有返回内容
   2. 1s就超时了，直接返回404页面

   这种情况下如何注入?
3. 比如说我写一个安全SDK
   1. sql注入的修复, 怎么写(伪代码)

      答：我倾向于使用预编译的方式
   2. 但是预编译的话, 研发可能不会用怎么办呢, 就是说如果他觉得改起来太麻烦了能不能更方便一点. 因为预编译的话, 我每条SQL每条查询都得去改.

      答：那设计一个白名单怎么样呢
   3. 那你大概写一下怎样设计一个白名单. 你可以分场景, 比如说什么场景什么场景的SQL注入, 或者是参数里面应该做什么操作
   4. xss的修复, 怎么写(伪代码)
      答: 用实体化转义
   5. 但是我们有一个场景啊, 你看我们上传简历这里, 有时候会支持上传html的简历, 对吧. 他本身业务就需要用到html, 如果用html实体化转义的话, 他全都会被转义, 那这样的话业务就崩了嘛, 对不对. 那这种情况下我们要怎么样去写一个xss的过滤, 或者是说转义, 去解决这个类似于简历这个场景. 你可以想一想, 写不出来代码也没关系.

      答：白名单限制, 黑名单过滤.
   6. 其实我们自己是这样做的, 对于这种情况, 我们第一是会做一个html标签的白名单, 第二是事件的白名单. 黑名单我们就不搞了.
   7. rce的修复, 怎么写(伪代码)(java或者python的命令执行)
      答: 白名单限制, 只允许需要的函数. 但RCE的话我感觉在业务场景当中, 一般来说也不是很容易出现
      面试官: 欸, 我们就出现了很多. 尤其是运维部门.

我: 我打CTF比较多, 我了解的RCE都是PHP方面的. 比如说system, popen之类的. 一般来说都是直接做过滤

8. 那PHP中这些函数全部被黑名单了, 你还有什么方法

   答: 字符串拼接 `$a=p.h.p.i.n.f.o()`

9. 你有没有用过php里面的反引号啊

   答: 还有用 `chr()` 函数来绕过

10. 面试官: 编码是吧

11. xxe的修复, 怎么写(伪代码)
    答: 对XXE来说, 我只了解他的攻击方式, 对他的防御不是很了解. 攻击方式就是做XML的外部实体化注入. 一个攻击模板, 可以读文件, 可以做命令执行

12. XXE怎么做命令执行呢, 就拿php来说, XXE怎么做命令执行

13. XXE这个命令执行是要他的服务端本身支持某些特殊的协议, 一般来说是不行的

4. 了解过自动化代码审计的工具吗, 类似于fortify这种

   答: 我只用过那个一个比较老的那个, 我想不起来了(指seay)

5. 没关系, 那你有没有了解过他的一些原理, 大概怎么做的

   我: 他原理一般都是通过匹配一些特殊函数, 去定位可能出现漏洞的函数的位置

6. 但这种的话他误报很高欸, 就像我这种RCE的话, 你直接匹配的话他很多都是误报了, 很多他都不是web思路的

   我: 还有一种是, 给他加一些自定义规则

7. 那有没有更好的办法呢, 误报太多了我们没办法接受啊

   我: 我有一个想法就是, 他自己匹配了之后, 能不能从前端从一个黑盒的层面再去验证一遍

8. 那黑盒验证, 我就有需求是, 首先我得知道, 首先我php里面我这个函数到底是哪个入口传进来的, 对吧. 但这个有可能经过了层层调用, 甚至有可能是 `include()` 这种, 那这种的话, 对于我来说 , 我并不知道他影响到了哪一些入口, 这种情况怎么办呢

9. 你们学校有学编译原理吗

10. 其实我觉得安全专业还是要学一下编译原理

11. 有没有搞过linux的这种后渗透相关的

    1. 面试官: 比如这个linux被我攻陷了, 我想去拿到更多的信息, 比如说一些横向的信息, 那种有没有搞过
       我: 这种不是很了解, 但windows的会一点
    2. 面试官: 那你可以简单讲一下, 比如你先攻陷一台windows的机器, 然后我想在这个windows的域内去做一些横向移动, 我想把这个windows的域的权限给拿到, 这种你该怎么做
       我: 通过票据伪造, 白银票据和黄金票据
       面试官: 你这个票据伪造要怎么做呢
       我: 一般用mimikatz就可以了吧
    3. 面试官: 你mimikatz抓取的是内存里面的密码和一些他的票据, 那我如果本身是低权限的呢, 就我本身抓不了密码, 或者我抓到的用户密码并不是域账号的, 是一个低权限账号呢. 因为大部分渗透进来都是个应用, 应用他可能并没有域权限
       我: 从低权限往上提
    4. 面试官: 那你一般会怎么提权
       我: 一般windows的漏洞吧
       面试官: 那现在就用这个windows系统的提权, 我现在就一个webshell, 那我怎么样去提权

5. 面试官: 你可以这样嘛, 你上传一个提权的脚本或者exe嘛, 你webshell去跑这个exe, 他就把这个web应用权限提权了

12. 那你最后有什么想问我的吗

0x0D 腾讯-玄武实验室

作者：立志区块链安全的菜鸡

链接：https://www.nowcoder.com/discuss/711602?source_id=discuss_experience_nctrack&channel=-1

来源：牛客网

部门：玄武实验室

1. 自我介绍
2. 讲解一下CSRF原理吧
3. 什么时候接触web安全的
4. 为什么学WEB安全
5. 参加过哪些比赛
6. 你发挥了那行作用
7. 讲讲反序列化吧
8. 说一说最近你关注的安全圈大事
9. 那你说说你遇到最优印象的吧
10. 我看你简历上有黑盒测试 说一说吧
    - 一个是钱包的测试 一个是交易所的测试，钱包主要是信息泄露，水平越权
11. 怎么发现的
    - 信息泄露是webpack可以直接查看api 等调用信息，水平越权是构造josn包返回了用户数据账户密码之类的
12. 怎么构造的
13. 那继续说说交易所
14. （区块链相关）讲一讲逆向函数涉及到的接收参数的指令集
15. 说说重入漏洞
16. 有对最近那个最大的区块链安全事件有了解吗
17. 好，那你对密码学有什么接触嘛
18. 我看你简历有许多对Defi的审计，那你有什么对漏洞的挖掘的经验吗
19. 嗯好 那现在我问你个问题 你思考下 在DEFI项目中建立了各种各样的经济模型 怎样才能找出可能存在的漏洞
20. 讲讲你对未来可能出现的新型漏洞的猜想吧
21. 有一种 游戏在猜对正确答案后可获得奖励
22. 反问

0x0E 360-安全工程师

作者：Djade

链接：https://www.nowcoder.com/discuss/628090?source_id=discuss_experience_nctrack&channel=-1

来源：牛客网

1. 自我介绍
2. WAF及其绕过方式
3. IPS/IDS/HIDS
4. 云安全
5. 怎么绕过安骑士/安全狗等
6. Gopher扩展攻击面
7. Struct2漏洞
8. UDF提权
9. DOM XSS
10. 数据库提权
11. 怎么打Redis
12. 内网渗透
13. 容器安全
14. k8s docker逃逸
15. linux、windows命令：过滤文件、查看进程环境变量
16. 站库分离怎么拿webshell

0x0F 快手-安全实习生

作者：ArrowQin

链接：https://www.nowcoder.com/discuss/651317?source_id=discuss_experience_nctrack&channel=-1

来源：牛客网

部门：系统运营部

一面

1. 自我介绍
2. 问项目
3. 针对项目问了很多详细的问题，不便透露，通用问题如下：
4. 做项目的时候有没有遇到什么问题，怎么解决
5. 做项目学到了什么东西
6. 项目中有没有什么地方自己做过优化
7. 有没有对网站做过渗透测试
8. Linux操作熟悉吗，怎么看进程PID
9. 用过什么数据库，答：sqlite,mongodb,面试官好像不太了解没咋问
10. 为什么用mongodb
11. 了解ES吗(Elasticsearch)
12. HTTPS建立过程
13. python怎么管理内存
14. 深拷贝和浅拷贝区别
15. python多进程、多线程、协程有用到吗，都在什么地方用到

16. python可以实现真正的多线程吗
17. 代码题：ip排序

（转成元组排序就行了，记得把str转成int，不然192会比50大）

```
输入：iplist = ["1.1.1.1","192.168.1.110","10.192.2.4","10.50.2.3","10.50.2.10","111.120.12.1","172.18.5.112"]
输出：
1.1.1.1
10.50.2.3
10.50.2.10
10.192.2.4
111.120.12.1
172.18.5.112
192.168.1.110
```

18. 写Web API的时候怎么防止SQL注入
19. 怎么防XSS
20. 了解越权漏洞么，有没有挖过越权漏洞
21. 有没有什么比较擅长的我还没问到的

二面

1. 问项目
2. 项目哪一块时间花的比较多
3. 怎么溯源攻击
4. 举一个溯源攻击的例子
5. 怎么检测webshell
6. sql注入在mysql和sqlserver中有什么区别
7. 想找安全开发的岗位还是安全研究的岗位
8. 代码题：手机九宫格键盘，输入数字，输出所有的字母组合

   如输入23，输出['ad','ae','af','bd','be','bf','cd','ce','cf']
9. 讲一下DNS协议的作用、解析过程
10. DNS协议的安全问题
11. 实习时间

0x10 华顺信安-安全服务工程师

来源：知乎

链接：https://zhuanlan.zhihu.com/p/426763642

1. 自我介绍
2. 红蓝队经验
3. 关于shiro漏洞了解多少
4. 说说你APP测试的经验
5. xposed用的什么框架，有没有自己写过app解密

6. Xss、SSRF、SQL 产生的原因，修复方案?
7. 如果你Xss打了后台，发现是内网的怎么办
8. 假设给你一个目标站，你要怎么做?
9. linux和windows提权知多少。
10. 会不会进程注入?
11. 做过几次应急?
12. 讲讲windows和linux应急你咋做的
13. 用过没用过我们家的goby和fofa?
14. 会不会apk反编译?
15. 你python水平咋样?
16. 你php怎么审的

> 备注：从0x11~0x14都是同一位师傅的面经，来源于知乎，里面有这位师傅的回答及一些总结、知识点，我这只是选了几个个人认为比较有代表性的公司和面经的题目出来
>
> 来源：知乎
>
> 链接：https://zhuanlan.zhihu.com/p/164774894

0x11 奇安信面试复盘

1. MVC框架详细说一下
2. 详细介绍一下sql注入
3. xss与csrf的区别
4. csrf的原理以及如何防范
5. 还有什么你擅长的但是没有问到的吗
6. 讲一下xxe的原理
7. xxe会用到哪些函数
8. 文件上传，详细说说
9. 常见的web容器有哪些
10. apache 7.0 文件上传黑名单怎么绕过，详细说说
11. 密码学的对称密码与非对称密码有哪些
12. md5是不是对称加密
13. apache可以执行php文件吗
14. 了解哪些数据库
15. 说说反序列化的原理
16. 反序列化会用到哪些函数
17. xxe有没有实战过
18. java的多线程
19. python有过哪些项目，写过什么东西
20. 之前python学到什么地方

0x12 京东-安全研发

1. 首先根据简历提问
2. 问我的一个项目完成的怎么的样了，//简历中的
3. Java基础怎么样，
4. 有没有自己动手写过一些工具
5. 有没有想过自己以后要写一下扫描器

6. sql注入的简单原理及其如何防御
7. 有没有了解过反序列化 尤其是Java方向的
8. 数据结构还记得多少
9. src主要挖掘一些什么类型的漏洞
10. 了解的MSF框架怎么样
11. 数据库主要了解的哪些，主要学的什么数据库
12. ssrf的原理及其防御 ---> 这有深入

0x13 安恒面试复盘

1. sqlmap爆出当前库名的参数是什么?
2. namp探测系统的参数是什么 --->大写还是小写
3. namp的小写o与a是干嘛的
4. 布尔型盲注的具体语句是什么
5. 宽字节的原理
6. python有没有反序列化
7. get传参与post传参的区别
8. Http有哪些请求方式
9. 如何判定cdn与cdn的作用
10. 如何确认服务器的真实IP
11. 详细说了说信息收集过程
12. 一串编码如何确认是base64
13. 栅栏密码的原理是什么
14. base64与md5如何区别
15. oracle的默认端口是多少
16. mysql的管理员密码一般放到哪
17. 如果substr()函数被禁用，你脑子里有多少替换函数
18. redis如何拿下，哪个端口，具体语句，具体操作
19. 如何通过邮箱知道对方的IP
20. 说一下同源策略
21. 如何收集网站管理员邮箱等等
22. ssrf有哪些危害
23. 如何防御ssrf-->问的较深---->建议在详细了解一下
24. Linux的某两个文件怎么分辨（忘了具体是哪两个文件了）
25. MSF框架稍微问的深入了一些
26. web容器（中间件）有哪些解析漏洞与原理
27. 如何防范sql注入 --->这问的很深

0x14 浙江东岸检测

1. xss的标签
2. 说说大学这几年，你最自豪的事情
3. 简单说说sql注入
4. 说说偏移注入
5. 说说ctf你都做哪些题型
6. 遇到的比较困难的web题型的ctf题目
7. xxe了解吗，有没有自己审计出

8. 说说反序列化
9. bypass说说
10. 假如，让你设计一个waf，你会怎么设计
11. 内网渗透与提权了解吗
12. 平常都挖掘哪些src
13. 有没有自己手写过一些脚本
14. 说说sql注入，手工怎么爆出所有库名字

0x15 360-安全工程师实习

时长：45min

来源：知乎

链接：https://zhuanlan.zhihu.com/p/362868972

1. 自我介绍
2. WAF及其绕过方式
3. IPS/IDS/HIDS
4. 云安全
5. 怎么绕过安骑士/安全狗等
6. Gopher扩展攻击面
7. Struct2漏洞
8. UDF提权
9. DOM XSS
10. 数据库提权
11. 怎么打Redis
12. 内网渗透
13. 容器安全
14. k8s docker逃逸
15. linux、windows命令：过滤文件、查看进程环境变量
16. 站库分离怎么拿webshell

0x16 某一线实验室实习

来源：知乎

链接：https://zhuanlan.zhihu.com/p/426747686

技术面

1. 面试官：你好，听说你对来我们公司的意愿非常强烈，是为什么呢

我：因为我在项目中与贵公司的人员有过合作，感觉无论是技术还是硬件或者是待遇都算圈子里一流的

2. 面试官：那你了解我们实验室吗?

   我：我有了解过，巴拉巴拉说了一下

3. 面试官：那我先给你介绍一下实验室的方向，分为三个方向....

   我：好的明白了

4. 面试官：你在项目中是否使用过我们公司的设备，感觉使用体验如何（意思就是让说设备的优缺点）

   我：那我就实话实说了？

5. 面试官：没问题的，我就想听听你的意见

   我：我使用过.... ,优点就是性能好，能探测到更多的威胁情报之类的（大家脑补吧），感觉不足的就是探测和分析出的威胁，没法给出具体的流量片段，没法通过一个设备有效确定攻击，没有流量特征不好和其他全流量设备进行联动，可能是设备出场的保护机制，保护特征库不被外泄。

6. 面试官：你知道主流的设备原理和开发过程吗

   我：（我就说了一下原理，还不知道对不对）

7. 面试官：你在项目中是做过流量分析对吗？能不能说说你的具体案

   我：我在国家hvv中协助发现过0day，单独发现过frp反弹定时回确认包向外输送流量，shiro反序列化等漏洞（我主要讲了我frp反弹的发现思路和流程）

8. 面试官：除了这些常规的特征发现，你自己还有什么快速确定的方法吗？

   我：（给大家分享一下我自己的流量分析心得）

   1. 确定事件的类型（确定事件是什么样的攻击，比如sql注入和爆破和frp的流量分析步骤就不一样）
   2. 确定事件的时间，首先划定一个时间段
   3. 确定数据流，攻击的数据流我们是要看HTTP，TCP，还是ssh
   4. 分析是内网—>外网还是外网—>内网，内网和外网时两种查询方法，正确的查询能有效的通过分析更少的数据包获取结果
      比如 内网—>外网 我们确定后，第一步肯定先去先查看外网ip的流量，判断行为
      外网—>内网 这样一般都是拿下了一个外网的服务器当做跳板机，我们肯定要先去分析内网的受害者服务器，看看有没有被攻击成功
   5. 首先我们需要确定到攻击行为后，再深入的流量分析和应急响应，很多都是误报
   6. 数据包的大小也是分析的条件，分析SSL数据包需要解密
      - 爆破攻击
        1. SMB,SSH,MSSQL等协议比较多，看包的大小，成功登陆的包很大
        2. 看ACK，SYN包的次数，如果成功至少20起步，放到科莱上为40起步，但是注意不是失效包和重传的包（注意加密流的ack和syn包也很多，为客户端一次，服务端一次）
      - 重传攻击：
        1. 如果一个数据包非常大，几个G或者一个G，我们就考虑数据包是否进行了重传，然后查看数据包的重传数，打个比方就是刷新，如果短时间重传数非常多，就为机器操作，判定为攻击
   7. 我们发现一个攻击（如平台登录后的sql注入）我们可以通过流量回溯装置抓取那个被登录用户的用户名和密码，登录平台后自己利用发现的payload进行尝试，看是否能注入成功

9. 面试官：听说你还做过红队？是哪个项目，你在里面的职责是什么

   我：介绍了一下我的项目经验，然后说我在红队的是突击手负责打点（我们当时孤军奋战没后援，也没擅长内网的选手）

10. 面试官：说说你项目中的成果

    我：....

11. 面试官：说一下你在项目里遇到的问题

我：我们通过exp拿下了一个锐捷路由器的webshell，但是卡在了反弹shell上面，无法进行反弹

12. 面试官：那说一下项目结束后你是否有思考过这个问题，是否咨询过他人，解决方式是什么？（我感觉真的非常重视思考和问题解决，非常重视项目的闭环）

    我：我有问过也拿过锐捷路由器的朋友，然后我认为是数据库和网站分离开了，然后只能拿下来webshell权限

13. 面试官：你如何快速准确的确定资产？

    我：通过fofa，谷歌语法，钟馗之眼，一些的注册信息

14. 面试官：fofa的语法是什么？

15. 面试官：你如何在这些资产中快速的确定漏洞？

    我：最快的就是扫描器先扫描一遍，然后进行信息搜集，针对性的攻击，或者我们通过fofa语法针对性的在资产表中搜集是否存在特殊的cms或者oa系统....

16. 面试官:一般扫描都会封禁你，你会怎么办

    我：我会第一就是使用ip池代理，要么就是使用5g

17. 面试官：你这些信息搜集和攻击都是效率不是很高的，项目结束后你有没有思考解决方法呢

    我：我有想过自己写一个程序，把代码池和一些信息搜集和特定的利用方法融合，但是没写出来（又一次感到代码不好的痛苦）

18. 面试官：那你是否有了解过国家hvv红队的隐藏流量过防火墙的技术呢？

    我：有了解过，但是这个我不太会，没有地方去学（有点尴尬）

19. 面试官：你们在打点的时候有没有什么特殊的方法呢？

    我：我们除了搜索特点的oa系统，还会搜集资产里的邮件系统，进行信息搜集登录邮件系统，搜集各种配置文件数据库文件登录网站后台，我们成功登录到两个网站后台，和一个邮件系统，也拿下了几个oa

20. 面试官：你们这么针对特定oa，是因为有0day吗（笑）

    我：我们队有这几个oa的0ady和半day

21. 面试官：开发这边怎么样？能直接上手开发吗？

    我：python还能自己开发几个小工具，java还是只能看懂（好尴尬我真不行，可能是学安全时间还不够长，本来想今年主攻代码的）

22. 面试官：意思就是只能开发几个简单的扫描脚本对么（大家一定啊要好好学代码）

    我：是（尴尬的笑），最近在学习使用pos3编写poc

23. 面试官：你如果来实习你想进行哪方面的学习呢？

    我：（我选择了一个偏向防御类的方向，因为我知道攻击类的我应该水平不够，我很有自知之明）然后就是一些询问能工作几个月，什么时候能到岗

> 综合下来我认为面试官认为我的不足就是，红队时的攻击和信息搜集效率不高需要改进，可能缺少一点项目的反思和解决思路

hr面

1. 首先介绍一下你自己的经历？
2. 你才大二该大三，你在学校是怎么自学安全的？
3. 你是怎么接触安全的？
4. 你现在的学习内容是什么？
5. 近期的学习规划是什么？

6. 你在大学中平时课程和安全的学习是怎么分配的？是否会冲突？

0x17 腾讯-科恩实验室实习

一面

时长：一个半小时

1. tcp三次握手
2. 介绍一次渗透测试过程
    - 讲了一次代码审计
3. SSRF漏洞
4. 内网渗透大致流程
5. 再介绍一次难度比较高的渗透测试
6. 防守方有哪些入侵检测手段，有哪些痕迹是可以抓到的
7. 介绍进程和线程
8. 进程和线程内存空间的关系
9. 父子进程的介绍
10. 孤儿进程和僵尸进程
    - 这个我讲反掉了
11. kill一个进程的时候，都发生了那些事情，从父子进程角度讲
12. 反弹shell的几种方式
    - 本质是用tcp协议传输bash程序
13. att&ck矩阵的类别，介绍其中的CC
14. 到域名下拿到命令执行的结果
    - 这部分没听清楚，面试的时候直接说了不知道，复盘听录音还是没怎么听清，但好像大概想问的是DNS域名解析获取命令执行回显
15. Linux命令通配符
16. 护网的溯源、威胁分析工作之类的问了十分钟左右
    - 完全不会，以后简历上再也不写护网了
17. xx攻防演练中防守方有哪些手段，问的比较杂，主要就是问入侵痕迹检测和溯源之类的东西
    - 这部分也不太会
18. SVM、KNN介绍
19. 卷积神经网络介绍
20. 莱文斯坦距离
21. 搜索引擎算法
    - 不太了解，大概讲了下字典树
22. 倒排索引
23. 恶意样本给出函数家族的md5，如何进行分类
    - 从统计规律讲了下
24. 反问

二面

时长：半小时

1. 第一个问题就直接问了护网，和一面问的差不多，直接裂开
2. Linux开机自启动方式
3. init.d脚本介绍
4. Linux怎么查看程序调用了哪些文件
5. 如何监控Linux文件操作
    - 问到这里就已经非常慌了，Linux比较进阶的操作都不是很会，而且面试官一直在叹气我日
6. Linux有哪些系统调用
    - 不会
7. GDB调试
    - 不会
8. 查看Linux开放的网络端口、多线程状态
9. 反弹shell的方式
10. Linux下怎么隐藏文件
11. 子域名收集
12. DNS重绑定
13. DNS解析的流程
14. CC流量
    - 听都没听过
15. ssh隧道
    - 面试没听清楚，听到隧道就以为是UDP穿越隧道开讲了
16. https证书机制介绍
17. burpsuite一些使用方法，插件开发方法
18. nmap的基本操作
19. syn开放链接原理
20. redis漏洞利用
21. runc容器逃逸原理
22. 常见WAF种类(不知道为什么还特别问了长亭的WAF)
23. MySQL的UAF
    - 没听过
24. 算法题(比较简单，leetcode easy级别)
25. Linux进程通信
26. 反问

> 备注：从0x18~0x1B均来自于许少牛客网的分享，不多说了，许少yyds

> 作者：4ra1n
>
> 链接：https://www.nowcoder.com/discuss/772753?source_id=profile_create_nctrack&channel=-1
>
> 来源：牛客网

0x18 某四字大厂面试复盘

这个面试有许少的两个问答式文章，建议参考

一面链接：https://zhuanlan.zhihu.com/p/412934756

二面链接：https://zhuanlan.zhihu.com/p/413684879

一面

1. 看你做java多一些，讲讲java内存马原理和利用
2. 那你讲下如何查杀java内存马，工具和原理角度
3. 冰蝎和哥斯拉了解吗，讲讲原理
4. 你之前在其他公司实习做了些什么事情
5. 有绕waf的实战经验吗，从各种漏洞的角度谈下
6. 熟悉webshell免杀吗，讲下原理
7. 做过其他免杀吗，比如结合cs和msfvenom的
8. 谈谈fastjson反序列化原理和常见利用链吧
9. 数据结构熟悉吗，谈谈红黑树原理
10. java的hashmap用到红黑树，讲下hashmap的原理
11. 有没有流量分析的经验
12. 谈谈代码审计经验
13. 看你有些cnvd和cve，讲讲挖洞的过程
14. 有打过知名的ctf吗，讲将经历
15. 熟悉内网渗透，域控这些，说一下实战经历
16. 谈谈java反序列化的cc链原理吧
17. 看你重写过sqlmap，读过sqlmap源码吗
18. 看你熟悉mysql，讲讲索引，存储结构等
19. 讲讲mysql为什么要用b+树
20. 看过mysql源码吗
21. 分析过二进制漏洞吗
22. 有没有用汇编写过东西
23. 谈谈linux内核的漏洞
24. 挖过缓冲区溢出漏洞吗
25. python的沙箱逃逸了解吗
26. python的flask模版注入讲讲
27. 看你做过抽象语法树相关的项目，谈一谈
28. 讲讲rasp的概念和原理
29. 谈谈rasp的对抗
30. 谈谈php和golang语言本身的安全问题
31. 机器学习和算法相关懂嘛
32. 看你尝试写过简单的操作系统，谈谈思路
33. 你有什么要问我的吗

二面

1. 讲讲你挖过印象最深的洞
2. 讲讲你写过的安全工具，从出发点和原理层面谈谈
3. 讲讲文件上传这里怎样绕WAF
4. SSRF的利用和绕WAF手段
5. 谈谈MSSQL如果XPCMDSHELL不能用怎么拿SHELL
6. 遇到没有回显的RCE怎么办
7. 不使用SQLMAP的OS-SHELL，各种数据库怎么写SHELL
8. 给你一个比较大的日志，应该如何分析
9. 谈谈redis未授权会导致哪些问题
10. 讲讲SYN FLOOD原理，防御，检测手段
11. 讲讲UDP反射放大的原理，防御，检测手段
12. 说一说自己的优势吧
13. 你有什么要问我的吗

三面

1. Padding Oracle Attack讲讲
2. Fastjson反序列化原理以及1.2.47绕过的原理
3. 除了readObject以外造成反序列化的函数有哪些
4. CC链中找你最熟悉的几条链讲一讲
5. Shiro550反序列化的原理及利用工具编写思路
6. Spring/Struts2的RCE中印象最深的讲一讲分析过程
7. sql注入绕WAF的方式尽可能多说
8. 分块传输绕WAF的原理
9. 文件上传绕WAF的方式都有哪些
10. 讲讲你挖过这些CVE中印象最深的
11. 你自己最大的优点和缺点是什么
12. 未来你想做安全的哪一个领域
13. 你学校成绩如何有挂科吗
14. 你有什么要问我的吗

0x19 某四字大厂实习面试复盘

一面

1. 自我介绍
2. 数组和链表各自的优势和原因
3. 操作系统层面解释进程和线程区别
4. 线程和进程通信方式以及数据安全问题
5. 多进程和多线程的选用场景以及原因
6. 了解过哪些WAF说说原理
7. 尽可能多地说下SQL注入绕WAF方式
8. FUZZ绕WAF的Payload长度通常是多少
9. 写过哪些正则说说具体的场景
10. 不查资料不能测试直接写ipv4的正则
11. Fastjson的反序列化原理
12. Java反射机制会导致怎样的安全问题
13. XSS和CSRF的相同点以及如何配合利用
14. CSRF_TOKEN的位置以及原理和绕过

15. 尽可能多地说你所知道的HTTP头
16. Nmap常见扫描方式的原理以及NSE脚本原理
17. 看到你有不少CNVD证书讲一讲挖洞过程
18. 讲一讲你考过的证书都学到了些什么
19. 看到你Github有不少项目讲讲
20. 你觉得自己还有什么亮点吗
21. 你有什么要问我的

二面

1. 自我介绍
2. 熟悉哪些Web漏洞讲讲
3. 跨域的解决办法原理以及安全问题
4. Python多进程和多线程如何选择
5. Python的GIL锁本质上做了什么事情
6. Java的JVM为什么要有GCROOT
7. Java的JVM有哪些垃圾收集器
8. 垃圾回收计数引用机制的缺点是什么
9. CSRF怎么拿到Cookie
10. 如何判断一个网站是钓鱼网站
11. 不同域名怎样通过CSRF拿Cookie
12. 说一些常见的HTTP头以及作用
13. HTTP-Only本质上做了什么事情
14. 平衡二叉树和二叉搜索树讲一下
15. SYN Flood攻击原理及解决方案
16. SYN 反向探测的原理是什么
17. TCP SYN Cookie的原理
18. ARP欺骗攻击原理及解决方案
19. UDP端口探测的有效方式是什么
20. Nmap的FIN扫描和空扫描是什么
21. 三次握手的序列号变化说一下
22. Python的值类型和引用类型是哪些
23. Python的list和dict线程安全吗
24. 讲一下你做过收获最大的一个项目
25. 你有什么要问我的

三面

1. 自我介绍
2. 解释下CSRF
3. 结合实际的例子说说SSRF
4. 结合实际的例子讲讲RCE
5. 为什么现在文件上传很少了
6. 基于语义分析的WAF了解吗
7. 讲一下你上一段实习做了什么
8. 讲几个印象深刻的挖洞经历
9. 讲一下你对未来的规划
10. 有没有转正的意愿
11. 你有什么要问我的

四面（HR）

1. 面试的体验怎么样
2. 谈人生理想
3. 最早实习时间

0x1A 某两字大厂面试复盘

一面

1. 自我介绍
2. 前两段实习做了些什么
3. 中等难度的算法题
4. java的class文件结构
5. kafka的原理了解吗
6. fastjson反序列化原理
7. 讲讲你研究最深入的领域

二面

1. 排序处不能用预编译应该怎么防
2. 从白盒黑盒两个角度讲下挖过的漏洞
3. ssrf的绕过和防御
4. 讲讲fortity等代码审计工具原理
5. 存储过程角度讲讲预编译的原理
6. csp是如何防御xss的
7. csrf为什么用token可以防御
8. 给你一个项目讲下审计思路
9. 内网相关的问题
10. 讲下你挖过的逻辑漏洞
11. 讲讲你用golang写过的东西
12. 什么是安全

三面

1. 讲下你自己写ysoserial的思路
2. 确定sql注入漏洞后如何进一步利用
3. 泛微OA的漏洞原理讲讲
4. 新爆出的Confluence RCE讲讲
5. 以前的实习中做了什么事
6. ***原理以及实战中的绕过
7. 红蓝对抗的流程讲讲

四面

1. java反序列化原理和工具
2. 讲讲关于指纹识别的方式
3. shiro反序列化工具的原理
4. 不用sqlmap情况下sql注入点如何找
5. 讲讲你挖到的这几个cve
6. 二进制方面有无了解

0x1B 某安全公司-安全研究员

一面

1. 讲讲你写的几个Burp插件原理
2. 做过什么JavaWeb项目吗
3. CC1-7找熟悉的讲一下原理
4. Fastjson和Jackson反序列化原理讲讲
5. BCEL可以用其他类加载器吗
6. XStream反序列化讲讲
7. 最基本的反序列化原理是什么
8. 了解JEP290的原理吗
9. 讲下RMI原理以及相关的漏洞
10. JdbcRowSetImpl如何触发的JNDI注入
11. CC链四个Transformer区别
12. 讲下你挖过的CVE和CNVD
13. 反序列化除了readObject还有什么触发点
14. 讲下Spring相关的RCE原理
15. 讲讲IIOP和T3反序列化原理
16. PHP等语言的反序列化讲讲

二面

1. 做了几年安全
2. 未来想做什么
3. 讲讲实习期间做的事
4. 工作地点要求

0x1C 腾讯-科恩实验室实习

一面

时长：一个钟

1. 自我介绍
2. 简单介绍做的项目->基于项目的衍生（搜索域、搜索方法等）
3. 逆向C++相比起逆向C有哪些困难点？有用IDA python吗？
4. Linux程序分为哪几个段？
5. .data段存放哪些数据？.bss段存放哪些数据？
6. 函数调用时的流程，参数如何传入，寄存器的变化，栈的变化？
7. 解释程序的编译和链接，编译的过程中会有哪些操作（编译原理），If/Else语法树？
8. 了解Linux /proc目录吗？如果要查看进程打开了哪些文件，有哪些方法？
9. 人脸识别有哪些方法？怎样去进行相似度比对？有没有听过三元组损失
10. 如何比较两篇英文文献的相似度？如何比较两个C函数的相似度？
11. 什么情况下源代码与IDA反编译程序的代码差别很大？讲讲函数展开造成的区别？如何消除这种区别实现代码相似度匹配？
12. 了解TF-IDF文档匹配算法，搜索引擎的算法吗？

13. python中集合，求交集与并集的时间复杂度是多少？有没有o(1)的方法，迅速判定元素是否在集合中?

二面

时长：一面的一半

1. 工控场景的入侵检测与普通场景入侵检测的区别（简历项目）
2. 有了解过真实场景的入侵检测项目吗？（如一个企业办公的出口网部署入侵检测）
3. 面对加密后流量，正常访问与木马的区别可能有哪些？如何用AI或传统方法进行检测？是有监督问题还是无监督问题?
4. 面对静态编译的大型木马（几百M...），如何通过IDA定位其网络传输部分的逻辑?
5. 如何动态地去找导入表->从攻击者的角度，如何不在编码时直接导入相关API的前提下进行攻击?
6. Windows下有哪些常用的反调试技术?
7. 单步执行的原理是什么?
8. 在内存中已Load的程序，如何快速找到其具有执行权限的段?
9. 恶意软件有哪些方案检测自己处于沙箱中?
10. 怎么知道进程和其开的端口的对应关系?
11. SGD和Adam的区别?
12. 神经网络架构搜索领域目前的进展
13. WAF的实现原理，与IDA的区别，WAF针对包会检测哪些字段
14. 简介Linux下的Syscall
15. 工作中符合个人兴趣的研究项目或思路
16. 如何缩减模型的检测时延?
17. 如何降低模型的误报率?
18. 如何找攻击样本?

0x1D 长亭科技 安全服务工程师实习

1. 讲一下最熟悉的三种web漏洞类型，原理，测试方式
2. SQL注入过滤单引号怎么绕过
3. mysql报错注入常用的函数
4. 报错注入绕waf
5. mysql写文件的函数有哪些
6. into outfile使用有哪些限制
7. mysql提权
8. sqlserver除了sql注入外还有什么渗透的方式
9. ssrf漏洞原理
10. ssrf可以使用的伪协议
11. 哪些功能点会有ssrf
12. 对内网ip进行过滤，有什么绕过的方式
13. 有了解过Redis RCE的过程吗
14. Redis未授权如何获得服务器权限
15. Redis主从复制漏洞
16. 任意文件读取，一般读取什么类型的文件
17. 如何通过文件读取获取到web的绝对路径
18. /etc/passwd文件包含哪些内容
19. java反序列化漏洞有了解吗

20. 之前shiro的反序列化漏洞有了解吗
21. 知道哪些组件或中间件包含反序列化漏洞
22. 针对一个站点，你首先会做什么事
23. 说几个你比较熟悉的CMS，它有哪些特征
24. 正向代理和反向代理的区别
25. 说一下常见的端口对应的服务有哪些
26. 有没有接触过护网这块的工作
27. 比较常见的内置用户有哪些
28. 说一下映像最深刻的一次渗透测试经历，说一下大概过程，发现了什么漏洞
29. 有没有挖过业务逻辑的漏洞
30. 挖过哪些SRC
31. 挖到最多的是哪些类型漏洞
32. 弱口令，有验证码怎么绕过
33. 说一下非对称加密算法的加密过程
34. 有哪些了解过的非对称加密算法

> 接下来篇都是来自`xiabee`师傅在牛客和博客上的同步分享
>
> 牛客链接：https://www.nowcoder.com/subject/index/8032f6748b124176bbe67fb37b19ecad
>
> 博客：
>
> 作者(Author)：xiabee
>
> 链接(URL)：https://xiabee.cn/coding/2022-spring-recruitment/
>
> 来源(Source)：xiabee-瞎哔哔

0x1E PingCAP 安全工程师

岗位：安全工程师

一面

时长：四十多分钟

CTF相关：

1. 你给同学的授课内容
    - 如实说
2. SQL注入如何判断数据库类型
    - “sqlmap一把梭……”
    - 手动注的话用version函数等
    - 面试官在听完我的答案之后说了他的答案：一般采用撞函数的方法，xxx数据库的函数名是xxx，xxxx数据库的函数名是xxxxx，特定函数执行正确的话即可判断数据库类型，`version`广义上说说撞函数的一种
3. 布尔盲注、时间盲注
    - 忘记怎么答的了，面试官应该没有补充我的答案
4. 印象中比较有价值的题
    - 聊了一下去年的国赛SQL签到题，“网络原因，时间盲注不行……”
    - 聊了一下职业杯的某题，特定的font导致报错看不到，最后用curl实现了报错注入

    - 聊了一下职业杯的某题，利用注入直接执行了SQL命令修改了密码执行逻辑，而非传统的读写注入
5. 接上一题的`font`，“平时用过Burp Suite吗，BP中会打印全部内容，为什么会看不见`font`呢”
    - “用过，当时太懒了没开BP……curl了一下发现可以注就懒得开BP了”
6. 一些BP的操作
    - 忘了答了啥，应该没啥大问题
7. SSRF相关
    - 简单聊了一下
8. 如何理解逻辑层面的漏洞
    - 聊着聊着跑题了，后面面试官提醒我，又重新编了一段（x）
    - 大概意思就是“不该加的功能别乱加”，顺便提了一下log4shell的漏洞成因，“乱加功能”
9. XSS相关
    - “打比赛用的不多，细节可能忘记了”

护网相关：

10. 聊聊演习
11. 如果让你给甲方企业做渗透测试，你的大概思路
    - 主站扫描、CDN检测、口令探测、注入之类
    - 在授权范围内攻击上游厂商，尝试获取甲方站点源代码，现场审计0day
    - 在授权范围内攻击下游客户、旁站等，先进入内网再突破DMZ
    - 面试官也给出了他的答案进行补充，具体是啥忘了……
12. 介绍了很久的黄金票据和白银票据，准备提问……
    - “金银票据听说过，但是具体使用细节不熟悉……没有实操过”
    - 面试官给我科普了一下

项目相关：

13. 邮件系统
    - 大概聊了一下多线程编程，C与python
14. 作品赛
    - 背了一下摘要，讲了一下个人工作，区块链与libsnark
    - 没有细问，但是也没有打断我，让我自己叨逼叨了半天
15. 区块链与智能合约
    - 聊了一下truffle、solidity，吐槽了一下solidity不好用
16. 爬虫
    - 聊了一下“乐学给爷爬”系统和知乎刷流量系统
    - “初代项目，维护跑路，停止服务”
17. 容器，介绍了很久的k8s，准备提问
    - “暂时还不会，目前只用过docker-compose”，场面一度十分尴尬
    - 虽然但是，面试官还是给我科普了一下k8s
18. 可能还问到了一些二进制的问题，具体忘了
19. 反问：工作时间，是否加班等
    - “我们和国外公司比较像，周六周日、法定节假日一定不上班”
    - “我们以结果为导向，上班时间没有强制要求，你愿意九点来也可以，愿意十点来也可以；愿意五点走也可以，愿意六点走也可以，公司没有强制要求；如果有需要，也可以远程办公”

- “正常情况下不加班，但是如果遇到突发事件可能需要应急响应，像log4shell这种级别的漏洞就得做应急”
- 聊到这里突然有点哽咽，如此遵守中国劳动法的公司，对标的却是外企，国内996的公司真的需要那么多人996吗……

> 总体而言，PingCAP是截至目前，我面试过的面试体验最好的公司，问题的问题很深入，涉及的面很广，但是不管我答的有多烂面试官都会听我讲完；并且能明显看到面试官在记录面试内容，在我讲完之后再针对性提问，而不是在我讲到一半直接打断我…… PingCAP是今天最晚面试的公司，但是最早发出了二面邀请（大概一面过了三个小时就通知了）……可以感受到他们虽然不加班，但是效率还是挺高的。

二面

> 实打实面了一个小时，聊了很多很多方向，从项目经历到个人发展规划，还聊到了公司选择等，感觉收获挺大的。

1. 自我介绍
    - 简单背了一下简历（然后是针对简历的提问）

作品赛相关:

2. 介绍这个系统
3. 数据安全相关
4. 聊了一下区块链的开发经历

区块链相关

5. 智能合约的鉴权、公私密钥相关等
6. 数字钱包的身份认证等
7. 智能合约的开发遇到那些困难

作品赛相关:

8. 这个系统和普通联邦学习系统有什么突出特点吗
    - “挺鸡肋的……保证了安全性，但是牺牲了性能”（瞎说什么大实话）
9. 聊了一下大型开源项目二次开发的经历与感悟

渗透相关:

10. 介绍一下渗透经历
11. 方便聊聊渗透思路吗
12. 渗透过程中的感悟，防守方有哪些不足，作为进攻方主要利用了哪些方式进行渗透
    - “利用防守方安全意识薄弱……正经的WAF打不穿，但是并不是所有的站点都有WAF”

Github相关

13. 面试官看到了我的Github，里面有一些docker-compose的脚本，聊了一下项目
14. 介绍一下上述项目的开发历程、设计初衷等
15. 聊了很多云配置的内容
16. 聊到了LNMP的系统搭建，dockerfile相关

CTF相关

17. 介绍一下CTF相关学习、比赛、获奖等
18. 介绍一下擅长领域

工作意向相关

19. “像你有CTF经历，简历也不错，应该能去很多公司，像长亭、腾讯云、深信服等，包括我们公司，你对未来的公司选择会有怎样的考虑”
    - 直接点名长亭了，有点慌；内心OS：长亭的面试邮件到现在都没发，PingCAP搞快点把我收了……
    - 说了一下自己的选择标准：优先选择“不加班”，然后选择可能可以落户的公司，最后比较薪资；
20. 关于加班问题和面试官产生了一点分歧，“我可能要给你泼点冷水，我们也不是不加班，对于一个刚入职的新人，而且你还这么有目标，为了自己的理想肯定是要付出一定努力的……”
    - 狡辩了一下，“我不是厌倦加班，我厌倦的是那种没有意义的加班……单纯的堆积工作时常其实没有太多意思”
    - 然后提到了其他申请的公司，聊了一下对其他公司以及PingCAP的看法；没有踩一捧一的意思，就单纯的聊了一下对工作模式的看法
21. 英语水平相关: 问了一下口语咋样，但是没有直接上英文，好像下一轮有英文
22. 反问环节：问了一下面试流程，其他忘记了

> 二面居然秒过了（半小时以内吧），我这面试复盘害妹写完就给我发三面邮件了……呜呜呜我宣布PingCAP也是我的Dream Company之一

三面

> 项目主管面，总面试时间约50分钟，聊的内容挺多，体验也很不错。

1. 自我介绍
2. 介绍一下项目
3. SSRF相关
4. 开发过的脚本、项目等
5. python相关：python是真正的多线程吗
6. 挖过的漏洞
7. 英语相关：用英文介绍一下XSS
8. 英语相关：介绍不出来，介绍一下自己吧
9. 平时安全相关的技术是怎样学习的呢
10. 了解安全咨询的渠道等
11. 实战相关
12. 反问：主管介绍了工作内容、工作组等
13. 反问：实习相关
14. 主管点评：整体不错，渗透和开发这块需要加强，个人强项不够突出，可以多看看漏洞测试、漏洞公开等，尝试自己挖掘开源项目的漏洞

四面

> 大主管+HRBP面，一共面了约四十五分钟，大主管面了半小时，HRBP面了十五分钟左右。 大主管主要是业务方向，对攻击手段问的不深，主要是防护与架构相关的问题，给我一种我是架构师的错觉（不是）

1. 介绍一下你了解到的C/C++相关漏洞
    - 聊了一下缓冲区溢出
    - 聊了一下和其他业务嵌套时的漏洞
2. 详细聊聊缓冲区溢出
    - 栈溢出

    - 堆溢出（不会）
    - BSS溢出（不会）
3. 缓冲区溢出如何避免
    - 编译时避免
    - 运行时避免
4. 了解GO语言吗
    - “暂时不了解”
5. “没有关系，那根据你的认识，你认为GO语言有哪些安全漏洞呢”
    - “缓冲区溢出是不可避免的，只是利用难度的区别”
    - 然后提了一下嵌套业务相关的漏洞
6. 刚刚提到的其他漏洞如何避免
    - 提到了SQL注入等
    - “预编译，上WAF”
7. WAF相关，对于某些实体，比如本身就是一段SQL代码，如何防止误报
    - 实体化，权限控制，纯代码直接实体化，使其没有执行权限
    - 不能实体化的代码宁可误报也不放过……（瞎答的）
8. 开放性问题，本公司的攻击面有哪些，应对策略有哪些
    - 具体比较细节了，包括内部攻击外部攻击之类的
    - 回答的比较泛，基于规则/行为/角色等，也对一些具体的服务说了些应对策略
9. 数据安全相关，安全架构相关，如何保障数据安全等
    - 零信任模型
    - 最小权限原则
    - 基于身份/角色的访问控制等
10. “简历里面提到了容器，你对容器安全有了解吗”
    - 瞎扯了点容器逃逸
    - “平时接触容器主要是开发，容器安全接除不多”
11. 剩下内容不记得了，大概问了半小时
12. 反问：安全组的人员配置、团队规模等，以及这个凑够一桌麻将开office具体政策
    - 安全团队其实都是remote work，基本上都不在北京……
    - 开office的政策由HRBP解答的，确实有，也可以在南昌开，凑够人就行。

> HRPB基本上没有涉及技术问题，中途聊了一下作品赛，可能是提到了数据安全，HRPB对这个比较感兴趣（x）

1. 在北京吗
2. 有无实习打算
3. 是否为独生子女
4. 有无考研打算
5. 回应了一下刚刚开office的问题
6. 还有没有其他公司的offer
7. 对公司的选择是怎么样的
8. 为什么觉得PingCAP是dream company
9. 反问环节问了一下怎么不谈薪资……“下一轮会有专门的同学和你交流”

> 从0x1F到0x26都来自于https://github.com/biggerduck/RedTeamNotes/blob/main/2022%E5%A4%A7%E5%8E%82%E9%9D%A2%E7%BB%8F.pdf 觉得写的很好就把一些比较多的整过来了，建议去下个pdf看前言部分，问题部分仅供参考

0x1F shopee

1. 和信息安全相关的返回 response 头（https://www.cnblogs.com/yungyu16/p/13333909.html）
2. linux 常见命令
3. docker 常见命令
4. jwt 是什么
5. weblogic 反序列化原理（有一个 xml 反序列化漏洞 还有后台文件上传 还有二次 urldecode 权限绕过）
6. java 代码审计 exec 命令执行的相关利用 前面拼了一段 然后调用 lang.runtime.exec("fuck" + a) 这里可以利用吗 （不行 因为根据 exec 的方法 这里不能识别执行）
7. 内存马相关原理
8. shiro 反序列化漏洞利用的时候 由于 waf 过长 被 ban 了 怎么解决这个问题（如果是 waf 拦截 可以尝试更换 http 头 如果是 tomcat 头过长 可以在 cookie 写一个 loader 然后 shellcode 写到 body 里）
9. 内存马扫描原理 如何检测内存马
10. java 代码审计反序列化原理(输入的恶意类被识别 解析了)
11. ysoserial 原理 commoncollections 利用链的原理 (cc1 最后 invoke 反射加载输入的方法 cc2 cc3 等等大同小异)
12. linux 全盘查找文件命令(find / -name fucku)
13. docker run 的常用命令(docker run -it centos -p --name -d)
14. java 反序列化 php 反序列化 python 反序列化的区别和相同点(java 反序列化需要利用链 php反序列化也需要利用链 python反序列化不需要利用链 有一个__reduce__可以自己构造 命令执行)
15. linux 全盘搜索含有某个字符的文件/linux 全盘搜索叫某个名字的文件(grep -rl 'abc' /)(find -name / fucku)

0x20 深信服

1. 宽字节注入原理，是只有 gbk 编码的才存在宽字节注入吗?
2. php 反序列化原理
3. 内网一台机器，只有一个 mssql 的服务账户权限，如何进行后续的利用
4. rsa 算法原理/aes 算法原理
5. 一台机器不能出网，如何把一个 exe 文件放到对应的目标机器上去（dmz 区）

0x21 华为

1. log4j 如何绕过 trustcodebase
2. Springboot+shiro 环境如何进行渗透
3. 实战中如何判断 fastjson 的版本
4. Fastjson 文件读写 gadget 是哪条，原理是什么
5. 内存马类型，如何检测
6. 给一个后台登录框有什么利用思路
7. Spring4shell 原理&检测&利用
8. 安卓系统如何进行 rce，有什么思路

9. 给一个移动端的 app，已知服务端是 cloud 环境，有什么思路利用

0x22 360

> 红队&&企业蓝军方向
>
> 以下都是同一场面试提的问题，两个面试官，一个代审一个红队，时长接近两小时

1. shiro 如何绕 waf
2. weblogic 如果在打站的时候，一旦遇到了 waf，第一个 payload 发过去，直接被拦截了， ip 也被 ban 了，如何进行下一步操作
3. jboss 反序列化原理
4. weblogic 反序列化原理，随便说一个漏洞，然后说触发原理
5. fastjson 怎么判断是不是有漏洞，原理是什么
6. fastjson 判断漏洞回显是怎么判断的，是用 dns 做回显还是其他的协议做，为什么
7. fastjson 高版本，无回显的情况，如何进行绕过，为什么可以这样绕过
8. 代码审计，做过哪些，主流的代码审计 java 框架请简述
9. 泛微，致远，用友这三套系统代码框架简述
10. 泛微的前台漏洞触发和后台漏洞触发，如何通用性的挖泛微的洞，泛微能反序列化吗， 怎么挖
11. php 代码审计如果审计到了一个文件下载漏洞，如何深入的去利用?
12. php 里面的 disable_function 如何去进行绕过，为什么可以绕过，原理是什么
13. 假如说，在攻防的时候，控下来一台机器，但是只是一台云主机，没有连接内网，然后 也没有云内网，请问怎么深入的对这台云主机进行利用?
14. redis 怎么去做攻击，主从复制利用条件，为什么主从复制可以做到拿 shell，原理是什 么，主从复制会影响业务吗，主从复制的原理是什么?
15. becl 利用链使用条件，原理，代码跟过底层没有，怎么调用的?
16. 假如我攻击了一台 17010 的机器，然后机器被打重启了，然后重启成功后，机器又打成 功了，但是无法抓到密码，为什么无法抓到，这种情况怎么解决这个问题?
17. 内网我现在在域外有一台工作组机器的权限，但是没有域用户，横向也不能通过漏洞打 到一台域用户的权限，但是我知道一定有域，请问这种情况怎么进入域中找到域控?
18. jboss 反序列化漏洞原理
19. 内网拿到了一台 mssql 机器的权限，但是主机上有 360，一开 xpcmdshell 就被拦截了， 执行命令的权限都没有，这种情况怎么进行绕过。
20. 什么是 mssql 的存储过程，本质是什么？为什么存储过程可以执行命令?
21. 如果想通过 mssql 上传文件，需要开启哪个存储过程的权限?
22. 内网文件 exe 落地怎么去做，用什么命令去执行来落地，如果目标主机不出网怎么办?
23. 内网域渗透中，利用 ntlm relay 配合 adcs 这个漏洞的情况，需要什么利用条件，responder 这台主机开在哪台机器上，为什么，同时为什么 adcs 这个漏洞能获取域管理员权限，原理 是什么
24. 内网域渗透中，最新出的 CVE-2022-26923 ADCS 权限提升漏洞需要什么利用条件，原理 是什么，相比原来的 ESC8 漏洞有什么利用优势?
25. 内网渗透中，如果拿到了一套 vcenter 的权限，如何去进一步深入利用？db 文件如何解 密？原理是什么?
26. vcenter 机器拿到管理员密码了，也登录进去了，但是存在一个问题，就是内部有些机 器锁屏了，需要输入密码，这个时候怎么去利用?
27. 内网权限维持的时候，360 开启了晶核模式，怎么去尝试权限维持？计划任务被拦截了 怎么办?
28. mssql 除了 xpcmdshell，还有什么执行系统命令的方式？需要什么权限才可以执行?
29. 如果 net group "Domain Admins" /domain 这条命令，查询域内管理员，没法查到，那么 可能出现了什么问题？怎么解决
30. 查询域内管理员的这条命令的本质究竟是去哪里查，为什么输入了之后就可以查到?

31. 免杀中，如何去过国内的杀软，杀软究竟在杀什么？那么国外的杀软比如卡巴斯基为什 么同样的方法过不了呢？
32. 免杀中，分离免杀和单体免杀有啥区别，为什么要分离，本质是什么？
33. 打点常用什么漏洞，请简述
34. 内网横向中，是直接进去拿一台机器的权限直接开扫，还是有别的方法？
35. 钓鱼用什么来钓？文案思路？如何判断目标单位的机器是哪种协议出网？是只做一套来 钓鱼还是做几套来钓鱼？如何提高钓鱼成功率？
36. 钓鱼上线的主机，如何进行利用？背景是只发现了一个域用户，但是也抓不到密码，但 是有域

0x23 深信服-深蓝攻防实验室

1. 内网怎么打 思路
2. 国护刷分策略 通用性的寻找通用靶标思路 怎么刷
3. 数据库 主机 云 vcenter 刷满是多少分（看你打的多不多 对分的规则熟悉不）
4. 内网的多级代理用什么东西代理
5. 如果 tcp 和 udp 不出网 用什么策略来进行代理的搭建
6. 多级代理如何做一个 cdn 进行中转 具体怎么实现
7. 内网有 acl 策略 如果是白名单 如何绕过这个白名单进行出网上线 ip 和域名的都有可能

0x24 B站

1. k8s 和 docker 如何去做攻击 有哪些利用方式 是什么原因导致的
2. cs 的域前置和云函数如何去配置
3. 内网攻击的时候 内网有那些设备可以利用 （hadoop kibana 之类的设备）
4. 攻击 redis 不同的 linux 系统有什么不同
5. sql 注入的时候，如果遇到了返回的时候长度不够，怎么解决，如何截取，用什么函数截 取
6. 域前置
7. 免杀

0x25 shopee-红队-Singapore

1. linux 除了基本的内核提权还有什么别的方式可以进行提权
2. 如何删除 linux 机器的入侵痕迹
3. 寻找真实 ip 的快速有效的办法
4. print nightmare 漏洞利用&分析
5. java invoke 反射具体利用
6. 域内常用命令
7. 根据子网掩码探测指定资产
8. 什么是无状态扫描
9. kerberos 原理
10. ntlm relay 原理
11. 内网现在微软至今都没有修复一个漏洞，可以从普通的域用户提权到域管用户，用了 ntlm relay，你讲一下是什么漏洞
12. 100 家单位，现在需要在一天时间内拿到所有单位的 ip，port，banner，怎么做，用什 么东西来做

13. 黄金票据原理，黄金票据在 kerberos 的哪个阶段？如何制作？用哪个用户的 hash 来制 作?
14. cs 域前置的原理？流量是怎么通信的？从我直接执行一个命令，例如 whoami，然后到 机器上，中间的流量是怎么走的?
15. java 反序列化原理

0x26 长亭

1. spring spel 漏洞原理&利用方法 什么情况才能利用
2. java jdbc 反序列化高版本不出网的条件下如何利用
3. tomcat becl 如何利用
4. shiro 反序列化用的是哪种加密方法 如何利用
5. ueditor 哪种语言环境存在漏洞 怎么利用 如何绕 waf
6. 内网 Windows Print Spooler 利用&原理
7. 内网 PotitPetam 利用&原理
8. 域内 pth 和工作组 pth 的差别
9. 域内用户和工作组用户的差别
10. 如何攻击域控
11. spirng4shell&log4j 利用
12. 外网常用打点漏洞有哪些
13. 一个任意文件读取/任意文件下载，如何进一步利用
14. 用友 nc beanshell 执行命令如何过 waf
15. shiro 反序列化漏洞如果 cookie 中的 payload 过长被 waf 拦截如何绕 waf

0x27 奇安信 安全研究员 实习

作者：想搞二进制

链接：https://www.nowcoder.com/discuss/970682

来源：牛客网

一面 5.17

1. 自我介绍，内容包括：第一部分，做过的安全相关的有难度的项目，难点在哪。第二部分，安全技能树，哪些是比较擅长的，能做什么。
2. 讲讲linux平台的漏洞缓解机制
3. 讲讲linux平台的ELF文件结构，或者windows平台的PE文件结
4. NX是怎么绕过的
5. 讲讲ASLR怎么绕过
6. 用过kali的msf吗？都用来干嘛了，哪些工具用的比较多？
7. 函数的调用约定有哪些?区别是什么?32与64位有什么不同
8. 用fuzzing主要是用来干嘛？主流的产品（chrome那些）有挖过漏洞吗？
9. 对windows平台的漏洞和保护机制了解多少？
10. 分析过linux的公开漏洞吗？写过exp吗？
11. 有没有逆向分析过linux平台下的病毒
12. 英文水平怎么样

二面 5.18

聊了一下我现在做的fuzzing，之前做过的APT实习

三面 5.24

聊对奇安信的了解，聊人生

6月1号打电话说过了，6月10号收到offer： 珠海安全研究员

0x28 美团 安全岗实习

备注：作者是二进制的

作者：hx19970923

链接：https://www.nowcoder.com/discuss/889681

来源：牛客网

Q: 介绍下项目和专业技能
A: blah blah

Q: 说说你的反汇编器如何开发的
A: 当时学逆向所以想写一个，上网查 x86 指令格式后就开始写

Q: 反汇编器支持的 opcode 全吗
A: 一字节的比较全，两字节的不够全

Q: 做一个反汇编器，指令集 opcode 的意义去哪查
A: 厂商的手册，比如英特尔开发者手册，如果是代码虚拟机那种就自己逆向

Q: 怎么识别指令跳转条件和内存访问
A: （？没懂这个问题）是说指令 opcode 内部是怎么设计的吗

Q: （重新解释了一遍问题）
A: （？？继续懵逼）不同的跳转条件对应不同的 opcode，也对应不同表项，反汇编器里内置了一个表，比如 0xaa 对应 jne，0xbb 对应 je（难道是想问 ModR/M, SIB 那些?

Q: （好像还是不满意于是跳过了上一个问题）那你觉得这个项目难点在哪
A: 一开始完全不懂 x86 指令格式，然后自己学习查资料实现了它（好了我知道没有难点

Q: 介绍下你开发的 Windows 沙箱
A: blah blah

Q: 这个重定向你做全了吗
A: 文件重定向比较全，注册表的写了一点没继续写

Q: 做一个沙箱，有什么需要重定向的
A: 文件，注册表，还有一些 IPC 对象比如管道

Q: 你做到什么程度
A: 文件比较全，注册表不全，进程隔离完全依赖于系统安全机制，IPC 对象没做（逐渐小声

Q: 说说你的研究生课题
A: blah blah

Q: 怎么增强模型健壮性的
A: blah blah

Q: 怎么看健壮性增强了
A: 增强前后各自攻击一下记录成功率，降低了就是增强了

Q: 训练学过的样本又拿去攻击，不会有问题吗
A: 训练集和测试集是分开的，对抗训练学的是训练集上的对抗样本

Q: 比赛是团体赛吗
A: 是

Q: 你负责什么
A: 逆向和少量 pwn

Q: 这个比赛的脱壳是什么壳，怎么脱的
A: nSPack，ESP 定律脱

Q: 有没有手动修复，还是工具直接脱
A: 没有，OEP 直接 dump（感觉事情不妙）

Q: 那我可以理解你这个脱壳就是工具点一下呗
A: ……是（呜呜

Q: ESP 定律原理知道吗
A: 一大堆废话，最后才转到堆栈平衡（反思一下应该先点出堆栈平衡再说废话emmm）

Q: 这场比赛你贡献了啥
A: 做了这道逆向队伍进了决赛，虽然是因为队里 Web 手没做出题而已

Q: 看了你的博客，做这些逆向 CTF 题，可能投入了足够时间大家都能会，下一步你要怎么做
A: （以为是问未来学习规划）一个是实战经验很缺乏，要加强，一个是明确方向，现在有点没方向

Q: （解释了一下他说的是人工分析有局限，要向自动化分析发展）知道自动化分析吗
A: 知道但没深入了解

Q: 你知道哪些自动化分析的例子
A: fuzzing，AEG，Unicorn

Q: 自己调试过真实漏洞吗
A: 无

Q: 研究生方向为什么不是安全
A: 导师选的

Q: 毕业想做安全还是研究生的方向
A: 安全

反问阶段
Q: 部门是基础研发吗
A: 我们主要做安全的一些基础研究，包括刚刚跟你说的自动化分析，还不是研发

Q: 能提些学习建议吗
A: 多实战，往自动化方向靠，深入了解操作系统的细节，重视正向开发

总结：找实习以来收到的第一次面试，没想到自己这么拉垮。本来就知道自己菜，一问三不知感觉更菜了，看得出面试官尽力找问题问我了，是我不争气凉得明明白白

0x29 美团 安全工程师实习

作者：h4m5t

链接：https://www.nowcoder.com/discuss/624742

来源：牛客网

面试官是一位会弹吉他的安全工程师，比较和蔼，没有问刁钻的问题。 面试时间总共15分钟，我也不知道为啥这么短，可能那边有业务要做吧。

1.自我介绍

2.平时怎么学安全的

3.每天有多长时间学安全

4.SQL注入有哪些

5.给你一个URL，怎么判断注入

6.SQL注入防范

7.平时有看安全方面的文章吗，讲一篇

讲了一下昨晚看的DNSlog注入

8.讲一下CTF

9.讲一下你做过的渗透

最后 你有什么要问的吗?

1.怎么学习安全

2.甲方和乙方的安全有什么不同

面试建议

其实提前看了几篇美团技术部的文章和面试官写的web蜜罐，但我没讲。

可以提前查一下面试官的研究方向，如果正好是你擅长的，那就好了。如果是你不擅长的，就尽量把话题引导其他方向，让面试官跟着你的项目走。

0x2A 京东 安全研究

作者：方糕姐姐

来源：牛客网

1. 深挖项目。

   每个项目的主要难点，以及你做了什么，提到的有中间人攻击、数字证书之类的。

2. Java八股

   final关键字的用途?

   static关键字的用途？两者的区别?

   非对称密码算法和对称密码算法的区别和联系?

   RSA的数学证明?

为什么web端的数字证书能够被抓包 解析之类的?

序列化和反序列化中有什么漏洞?

还有记不清了 哈哈哈

3. 手撕代码以及优化

   斐波那契 递归

   双指针

   快速查询

0x2B 百度

作者：zhengtu

来源：牛客网

一面

时长：48分钟

1. mysql注入，已知information.schema相关表在代码层中被过滤，不考虑绕过情况，还可以怎么查询表名或字段
   考虑sys数据库，一些被访问过的表会被存储信息，索引中存在的表等
2. mysql注入中基于报错注入的多种方式
   记得floor,updatexml，extractvalue三种，第一种主键重复，后面两种基于xpath语法解析错误
3. 前端xss如果特殊字符输出被htmlscecial过滤了怎么办
   该函数默认只编码双引号，对单引号无效
   在js中可以利用\u003c等绕过符号过滤
   采用反引号执行命令，(可以采用jquery加载第三方js，或者添加script子节点引入js，或者直接获取cookie利用js访问第三方脚本)
   编码转换，富文本，数据库输出输入场景都有可能失效，比如前端调用了html函数作为输出的情况
4. 同源策略是啥，rerfer检测，前端空rerfer防御，怎么构造
   同源的标准是协议，端口，域名三者的统一，实质是浏览器对不允许的服务端返回的数据进行了拦截
   实现跨域有两种方式，jsonp和cors
   服务端验证rerferer头(为空则不用rerferer头判断)，校验csrf token，在http头中自定义属性并验证
5. jsonp是什么，怎么绕过
   劫持问题，防御取决于服务端如何配置，绕过取决于服务端的配置，关键词绕过
6. sqlmap源码是否分析过。
7. tp漏洞复现
8. java反序列化rmi原理(简历上有写)，其他类型的反序列化是什么
9. 如果让你编写一个DOM型xss扫描器，你该怎么写？假如事件需要点击，比如onclick去点击，该怎么检测这种类型的xss
   返回结果，人工判断，或者利用windows事件触发
10. 内网渗透流程和方式，比如域渗透
11. windows10上面的pth怎么利用
12. linux主机留后门的各种方式?
    计划任务，webshell，自启动后门，写注册表
13. DNS隧道搭建方式

二面

时长：53分钟

1. 如何入门的经历
2. 数据结构，算法，计网基础(非计科类专业自闭)
3. 针对已有的项目深入提问(实现，拓展，创新)扫描器实现对比拓展(不晓得)
4. 知识面深入，内网探测高危服务除了端口扫描还有啥?
5. 漏洞挖掘的挑战性的事件的优秀亮点
6. 其他公司面试情况
7. 渗透方向能力目标，学习的新方向。
8. 反问，有点考核提问智慧的意思，让我各种方面问他问题

三面

1. 问了项目的思路和思考方式
2. 挑战性的问题如何解决
3. 聊了未来城市选择和发展路线
4. 还有一些其他遇到某问题表现和思路是什么样的

和技术相关的问题占比很少

0x2C 腾讯

一面

作者：zhengtu

来源：牛客网

1. 编写工具的具体思路，sql注入，xss
2. csrf的防御， referer验证，referer为空则防御(referer是浏览器特性，为空排除特性之外的问题则做防御验证)，
3. xxe无回显探测 dns验证，内部实体探测
4. xss硬编码如何利用 前端dom型被js代码转义出来，比如\u003c,前提是返回在了js中，在html中除非具备某种标签，其特性可导致特殊编码执行，则能转义出来
5. java反序列化基础
6. 白盒审计能力问题--这一点应该说可以自行拓展，对owasp10做过调试，对tp审计做过深入调试，对rmi反序列化做过调试，学习过一本书的样子
7. 密码重置处的逻辑问题--第一二三步验证不统一，验证统一但后台返回的更改密码的token可被预测，枚举可猜解，返回敏感数据，后端与前端验证不一致，存在数据查询则可注入，xss编码问题

二面

问了各种问题，包括项目中如何解决问题，应急响应做过哪些处理，针对大量请求高并发的解决
有很多具体的场景，询问你的思路
聊了国家安全，各种安全视界的思考，见识

0x2D 奇安信 A-TEAM

作者：zhengtu

来源：牛客网

我投的这个岗位是奇安信A-TEAM的渗透测试，这个团队方向是以红队为主。面试流程是我体验最快的一家，可能是由于已经快11月份了，所以采取了滚动批次面试的方式，一个下午就完成了面试流程。面试官问的东西技术难度比较广和深，而且都是基于实际的应用场景来问的。所以基本杜绝了做题和背题的方式，需要一定的实战经验和见识。

一面

1、sql注入基于利用方式而言有哪些类型?

2、sql注入写马有哪些方式?

3、oracle注入除了注入数据之外有哪些直接利用的方式？(这个真没见过，答不出来)，sqlserver获取shell的方法?

4、xss的利用方式?

5、同源策略的绕过方式?

6、完整的渗透测试流程思路？(从拿下webshell到后渗透的实战经历)

7、如何绕过基于语义检测的waf，比如雷池，阿里云waf等(不是太理解语义这东西，说了一些我知道的绕过场景)

8、问了预编译场景下是否存在sql注入。(这一点老实说并不存在，但面试官提到第一次预编译的过程假如存在可控数据，这确实是可能的，我说了自己的看法)

9、编程问了个多线程和协程的区别。

二面

1、问了项目的实现思路和方法。

2、黄金票据和白银票据的区别?

3、pth中LM hash和NTLM hash的区别(这个之前做过研究，不过只记得一点了)

4、CDN的绕过方式?

5、waf的绕过方式?

6、其他忘了

三面

1、问了学校经历

2、问我自己觉得是个内向还是外向的人？？？(事实上我觉得让自己来评判这个问题没有意义，我可以把自己塑造得很内向，也可以说得很外向，但性格是矛盾和多样化的，用这样非黑即白的问题去询问，反而不如直接问平时相关的经历和事项)

我:我觉得性格这个东西是不应该一概而论的，我觉得我既不内向，也不外向。不如让我说说我的其他经历和思考。您这边来看看我是什么样的。是否适合这个岗位。剩下就balabala

3、询问其他offer状况

0x2E 快手 安全工程师

作者：牛客271656551号

来源：牛客网

1. 自我介绍
2. 介绍项目
3. Linux提权方式，脏牛提权原理
4. 公司中了勒索病毒怎么办、分哪几步，勒索病毒原理，勒索病毒是怎么传播的
5. 如何绕过waf
6. SQL注入的种类，怎么防御SQL注入，业务层面防止SQL注入的方法
7. 哪些情况SQL预编译无效
8. 怎么判断服务器是Windows还是Linux，能不能用ping命令判断
9. 了解的安全论坛有哪些
10. 平时有什么兴趣爱好
11. 学习过程中遇到的最大的挑战或困难
12. 反问

0x2F 快手 安全实习生

作者：ArrowQin

来源：牛客网

面试岗位：【暑期实习】安全实习生-系统运营部

一面

1. 自我介绍
2. 问项目
3. 针对项目问了很多详细的问题，不便透露，通用问题如下：
4. 做项目的时候有没有遇到什么问题，怎么解决
5. 做项目学到了什么东西
6. 项目中有没有什么地方自己做过优化
7. 有没有对网站做过渗透测试
8. Linux操作熟悉吗，怎么看进程PID
9. 用过什么数据库，答：sqlite,mongodb,面试官好像不太了解没咋问
10. 为什么用mongodb
11. 了解ES吗(Elasticsearch)
12. HTTPS建立过程
13. python怎么管理内存
14. 深拷贝和浅拷贝区别
15. python多进程、多线程、协程有用到吗，都在什么地方用到
16. python可以实现真正的多线程吗

17. 代码题：ip排序（转成元组排序就行了，记得把str转成int，不然192会比50大）
18. 写Web API的时候怎么防止SQL注入
19. 怎么防XSS
20. 了解越权漏洞么，有没有挖过越权漏洞
21. 有没有什么比较擅长的我还没问到的

二面

1. 问项目
2. 项目哪一块时间花的比较多
3. 怎么溯源攻击
4. 举一个溯源攻击的例子
5. 怎么检测webshell
6. sql注入在mysql和sqlserver中有什么区别
7. 想找安全开发的岗位还是安全研究的岗位
8. 代码题：手机九宫格键盘，输入数字，输出所有的字母组合
9. 如输入23，输出['ad','ae','af','bd','be','bf','cd','ce','cf']
10. (我就模拟做)
11. 讲一下DNS协议的作用、解析过程
12. DNS协议的安全问题
13. 实习时间

0x30 快手 安全工程师

作者：Qber

来源：牛客网

技术类：

1，自我介绍

2，根据简历逐步问技术，问工具的具体使用

3，SQL注入漏洞，类型，可以造成什么危害

MSSQL与Oracle

SQL注入写入Shell的具体命令

4，XSS，存储型怎么利用，有哪些危害，除了钓鱼

带外COKIES的时候，遇到WAF怎们

5，AWVS登录扫描怎么操作，SQLMAP怎么用，有那几个级别，分别有什么区别，参数

SQLMAP如何扫数据包，本地读文件，指定参数，这些的具体命令

6，如何绕过WAF

7，如何入侵快手

视频上传点、社工，钓鱼邮件

供应链攻击

8，钓鱼邮件你会用那些恶意木马、shellcode

9、NMAP如何静PING扫描，如何看端口开放，如何看系统版本信息，具体的命令是什么

编程题：比较version号不同，写了大概思路，但是细节没处理好，直接给面试官说放弃了，面试官问了思想，然后又问特殊情况，想了一下，实在想不错

经历类：

1，你挖到的比较有意思的漏洞

2，你最近学习的东西，比较有意思的

反问：

1，甲方安全与乙方安全有啥不同，

2，感觉自己答得磕磕绊绊的，希望面试官能给一些后续的学习建议

总结：

面试体验非常好，中间说了好多不会，面试官也没有非常生气，还是完整的走完流程，最后给了很好的学习建议。

对于工具的使用问题问的很细致，但是最近都在手工渗透，复测，自然没有经常用工具，哎，反正感觉每场面试问的都很不一样。

0x31 快手 安全工程师

作者：HsiAo.

来源：牛客网

老早之前投的快手，26号通知面试，27号11点面试，面了40分钟。

面试官很好，是我自己菜，还有我代码能力真的不行，尤其是用python（不自量力，python还没怎么刷题呢）

1、自我介绍

2、介绍下项目

3、介绍实习

4、信息收集

5、给你一个网站，你会怎么去挖掘漏洞

6、sql注入修复意见

7、XSS修复意见

8、弱口令修复意见

9、数据库操作

10、手撕代码，我代码真不行，题目：给你几个版本号如：1.3.2，2.1.4，1.0，让你判断版本号大小

11、操作系统查看最近登陆的用户

12、查看文件的最后300行

13、文件的权限777之类的

14、osi7层

15、tcp3次握手

16、反问

0x32 蚂蚁 安全工程师 实习

作者：求求了让我来个offer

来源：牛客网

面试时间线

3.7初面也就是简历面，3.9一面，3.18二面，3.22hr面

简历面

3.7初面 25min

1. 自我介绍一下
2. hw的项目做了什么负责什么角色
3. 重保的项目做了什么负责什么角色
4. 应急响应做过吗
5. 内网渗透有了解吗然后问了关于内网渗透的东西
6. ctf有打过吗
7. 逆向二进制有做过吗
8. 反序列化php和java
9. 你有什么想问我的吗

因为初面是简历评估的问题也不是很难就问了些项目延展了一点点就过去了

一面

3.9 一面 32min

1. 自我介绍
2. hw项目
3. 重保项目
4. src项目
5. src中你印象最深刻的一个漏洞
6. src中你碰到的困难以及如何克服的
7. log4j2
8. jndi注入
9. 逆向二进制有了解吗
10. 大学中学的最好的课
11. 我们地点是在xx地有问题吗
12. 有没有考研的想法
13. 你有什么想问我的吗

一面属于在初面的基础上对项目更加深层次的挖了一下

二面

二面 3.18 25min

1. 自我介绍一下
2. 自我介绍完面试官说前面两次面试已经基本差不多技术方面的东西都问完了，我来问你点别的
3. 然后问我对我这些src中挖到的漏洞的思考以及克服的困难和印象最深刻的漏洞
4. 如果是我蚂蚁的业务支付宝你会怎么样去测试
5. 有考研的打算吗
6. base地没问题吗
7. 什么时候能来
8. 你有什么想问我的吗

这二面的感觉就是更加注重你的发散思维以及对他业务的逻辑思考，因为我属于是src出身，所以这次面试正好对在我的口上了，所以对他业务的东西思考我就说了很多

hr面

3.22

hr面

hr面就是根据简历问你一些性格方面的东西

你项目中克服的困难

什么时候能来实习

意愿的地点是哪

为什么北方人不选择北京

0x33 蚂蚁 安全工程师 实习

作者：verf1sh

来源：牛客网

一面

时间：2022/03/07

1. 对什么方向比较兴趣，漏洞挖掘还是利用
2. 有没有写过实际的利用exp（写过路由器的）
3. 路由器那个exp能达到什么效果，能rce吗
4. 这些知识是你课程上学习的还是自己打ctf学的
5. 有没有用fuzz挖到过漏洞
6. 读过英文的技术文献吗，有没有看一些英文的论文
7. 有没有写过论文
8. 愿意做偏研究的工作吗
9. 数据库fuzz你有哪些改进思路
10. 数据库的漏洞利用除了dos还能达到什么程度
11. 你用的fuzz是python写的还是c写的
12. c开发能力怎么样
13. 用的win本还是mac本
14. 做过安卓的利用吗
15. 有什么想问我的

二面

时间：2022/03/07

1. 做一下自我介绍，把实习和项目都介绍一下
2. 介绍一下rhg可以做到什么程度，能进行哪些漏洞利用，能绕过哪些保护措施
3. rhg参加的是什么比赛，是bctf吗
4. bctf参加过吗，有哪些有意思的题
5. 对比一下qemu模式fuzz和源码模式fuzz
6. 说说qemu模式的动态插桩怎么实现的，有什么优缺点
7. 把你的实习展开说一下
8. fuzz普通程序和数据库有哪些不同点
9. 论文里是怎么去解决数据库fuzz中的一些难点
10. 你觉得作者的思路哪些是好的，哪些存在问题
11. 你做的一些改动提升了什么，有比较好的效果吗，有没有挖出漏洞
12. 看你的博客有用过afl++去挖漏洞，说说afl++和afl有哪些不同
13. 你觉得afl++有哪些策略对你来说很有用
14. 说说afl有哪些模块，每个模块的流程
15. afl-fuzz为什么速度很快
16. C++程序怎么去逆向找虚表

三面

时间：2022/04/08

1. 自我介绍
2. 介绍在深信服的工作
3. 数据库fuzz和普通程序fuzz有什么不同
4. 怎么给AFL做适配去fuzz数据库
5. 介绍一下fuzz的流程，从选取目标开始
6. 讲一下AFL的插桩原理
7. 怎么选择fuzz测试点，感觉类似于fuzz单个API函数吧
8. Linux内核你了解哪部分，内存、网络、设备？
9. 如果让你做内核的安全研究，你想从哪一块入手，为什么
10. 有计划过怎么去夯实自己的基础吗
11. 有没有工作上的规划，毕业后做哪方面研究
12. 期望base哪里
13. 什么时候可以来实习，实验室老师会限制实习时间吗
14. 研三的时候可以实习吗

HR面

时间：2022/04/20

1. 介绍一下本科和研究生的学习情况，为什么研究生选择换方向
2. 印象深刻的比赛，负责哪方面工作，遇到过什么难点，你认为在队友会用哪些形容词形容你
3. 了解部门工作内容吗，是你最想做的方向吗，希望base哪里

4.28 意向

> 从0x34至0x40均来自于 **Theoyu** 师傅的分享

0x34 商汤科技 安全开发工程师

一面

20分钟+做题

1. 问实习，问项目
2. 基础问题：
   如何查看自己服务器某个端口情况： netstat lsof
   如何查看远程服务器情况：telnet、nc、三次握手查看
3. 两道题
   一个字符串全排列
   一个第一个不重复子串

说了一下安全开发是基本上全开发，推去了安全攻防

二面

安全攻防
时长：55分钟

1. 自我介绍
2. 面试官介绍部门下面三个工作分组：
    1. 入侵检测
    2. 安全体系建设（SDL）
    3. 红蓝对抗
3. 反弹shell 如何检测?
4. 如果攻击者使用了AWK、如何检测?
5. 除了进程树的命令匹配，还有可以检测反弹shell的方法吗?
6. 你了解哪一些提权手段?
7. 细说一下什么是SUID提权
8. 分别说说这几类提权的检测方法
9. 如果让你设计一款入侵检测系统，你会往哪几方面考虑（发散思维）（文件、网络连接、进程）
10. 进程隐藏技术是什么，如何检测?
11. log4j的原理
12. 如果一个环境下存在有漏洞版本的log4j，如何在不升级的情况下做预防?
13. 聊聊IAST
14. 如果多进程下，A进程的Source 触发到了 B进程的sink点，如何溯源?
15. 职业规划
16. 反问

0x35 海康威视 网络安全工程师

一面

时长：45分钟

1. 自我介绍
2. 你认为海康威视哪些地方存在安全风险
3. iot漏洞挖掘有了解吗
4. 云上攻防了解多少
5. 数据上云有哪些风险
6. ssrf和csrf
7. openrasp看过源码吗
8. jndi如何做hook
9. 高版本jndi如何绕过

```
算法：给一棵树，输出树每一层第一个和最后一个不为空节点中间的个数（中间可以为空）
     10
    /   \
   8     18
  / \      \
 5   9      20      -----第三层节点数为4

     10
    /   \
   8     18
  / \    /
 5   9  16          -----第三层节点数为3

很离谱，只有题目，没有输入输入样例也没有模版，只给10分钟，我说如果树是以数组的形式输入，可以得到树每层第一个和最后一个的边界，双指针遍历再坐标相减即可，面试官好像没认真听，草草结束了。
```

0x36 度小满 信息安全工程师

一面

时长：40分钟

1. sql注入原理，waf如何检测
2. ssrf csrf区别
3. 邮件协议了解多少
4. smtp如何伪造？ （搭建匿名邮件服务器、如果目标域名没有设置SPF Sender Policy Framework, 就可以伪造）
5. 入侵检测全流程
6. 提权怎么检测
7. 提权 什么情况会出现误报?
8. 容器内提权，怎么检测?
9. 内网被搭了隧道，怎么检测?
10. 流量加密了 怎么检测?

二面

时长：30分钟

1. 框架类漏洞挖掘思路、业务逻辑漏洞挖掘思路
2. 反序列化漏洞如何检测
3. AES分类，默认密钥长度
4. AES加密流程
5. shiro爆破key，构建的初始序列化数据是什么？

0x37 长亭 安全开发工程师

一面

时长：40分钟

会问一些计算机基础的八股，但都是结合具体案例说的，体验不错

1. nmap支持哪几种扫描方式，分别对应tcp三次握手的哪个流程
2. 进程 线程 协程，分别用具体的场景说明一下
3. 浏览器开启多个窗口，属于多进程还是多线程？一个窗口内的多标签呢？为什么这样设计？
4. 知道go的协程内部是如何实现的吗？
5. shiro反序列化说一下
6. 如何探测是否存在某个类（jar包）(反序列化炸弹)
7. 如果让你开发，如何设计前后端的权限校验
8. 聊项目，聊了很久的XRAY
9. 看过cs源码吗？对武器研发有没有什么想法？
10. 会rust吗？
11. 聊规划
12. 反问，问了一个项目上的问题，面试官从技术上帮我讲解了（第一次反问技术问题..）

0x38 小米 安全工程师

一面

时长：45分钟

1. sql注入怎么预防、预编译为什么能防？
2. php和java侧预编译有什么区别
3. SSRF php 和 java 分别有什么利用方式
4. 说一下php和java侧反序列化的异同、利用
5. SCA是什么，具体该怎么实现，灰盒怎么做、白盒怎么做（灰盒可以依赖agent分析，白盒结合maven插件会比单纯分析xml好一些）
6. log4j有哪些防御方法
7. 从agent到字节码hook的整个流程（伪代码）
8. 谈一下codeql，能不能用来做CI/CD
9. codeql哪些地方会断，该怎么处理
10. 白盒理论了解多少，相比于灰盒
11. 说一下SAST、DAST、IAST的优缺点
12. 了解 devsecops 吗
13. 未来想从事什么方向

二面

时长：45分钟

1. 说项目
2. 说实习 x2
3. 终端命令的进程信息具体该如何采集
4. runtime.exec 后面的部分注入能不能执行
5. 漏洞挖掘和SDL 对哪部分感兴趣

0x39 携程旅游 基础安全工程师

一面

时长：80分钟

1. 自我介绍
2. 反序列化流程
3. 如何挖掘的0day
4. sql注入本质
5. sql注入怎么写马
6. outfile和dumpfile的区别（前者支持多行以及自定义编码）
7. 宽字符截断的原理，说一个具体例子
8. SSRF利用和防御
9. SSRF无回显怎么利用
10. 如果有一个接口可能有SSRF说你说你的流程
11. shiro说一下
12. shiro利用如果失败，可能是哪一环出了问题？（控制变量，逐一摸索）
13. 文件上传如何防御
14. 说项目，漏扫怎么做?
15. 了解sqlmap是怎么实现的吗？或者常规xss如何扫描?
16. 聊实习，反弹shell如何检测?
17. 反弹shell的本质是什么?
18. 作为一个agent，需要采集哪一些信息，如何构建进程树?
19. 提权如何检测?
20. 说一下其他主机侧的安全重点。
21. 云原生，容器安全了解多少
22. docker逃逸说一下
23. 云服务了解吗，打云上攻防吗?
24. 内网渗透了解多少、AD域了解多少
25. 隧道的本质是什么
26. 反问

二面&三面

（二面面完根据我想做的方向帮我转了一下岗，两面差别不大，放在一起）
时长：50分钟

1. 实习2做了什么

2. 如果在甲方做代码审计，你认为和在红队漏洞挖掘有什么不一样?
3. 如何权衡各种漏洞扫描或者入侵检测到漏报和误报
4. 实习具体做了什么，有什么收获
5. IAST 主动和被动的区别
6. IAST应该放在CI/CD的哪一环，了解过代理式吗?
7. 实习过程中有什么困难
8. 希望做自己擅长的领域，还是乐意探索新的方向?

0x3A 欧科云链 安全开发

一面

时长：一个多小时

面试官思路非常清晰，做完自我介绍后就和我说面试会涉及攻防以及开发三个角度，每个环节循序渐进。

攻：攻从前中后三个阶段展开

前：

1. sql注入如何判断数据库类型（根据利用的难易程度展开）
2. xss除了打cookie还有什么其他的思路
3. 代码审计的流程
4. filter的作用域
5. 哪些业务场景可能会出现反序列化漏洞
6. 除了readobject，还有哪些反序列化触发点
7. 如果一个反序列化打失败了，可能存在哪些原因?
8. 如何挖掘一条新的反序列化链
9. AST是什么
10. 代码如何生成AST?
11. 有没有不经过IR阶段（比如借助LLVM），直接生成AST的方法，和前者相比又有什么缺陷?

聊的有些偏了，回到攻击。

中：

1. 抛开exp，如何提权 （说了suid和mysql提权）
2. suid提权的生命周期（结合euid）
3. windows 烂土豆了解吗
4. 免杀知道多少，webshell免杀，静态、动态免杀

后：

1. 隧道相关
2. CS源码看过吗
3. 内网相关，我直接说不太了解

防：

1. HIDS的流程是什么
2. IAST和RASP的区别
3. 两者在埋点深浅上有什么处理（同样一类漏洞，会怎么做埋点处理）
4. 埋点埋的深和埋的浅对检出率有什么影响？（一下子没转过弯来，说让我想一想）

5. log4j做埋点，直接在log4j的Class里做hook，和直接hook jndi的initial和lookup 有什么区别（算是对上面那个问题的提示）
6. 了解百度的iast是怎么做的，主动式和被动式的的区别
7. 这两者会产生脏数据吗？

开发：

1. 聊项目
2. 符号执行了解吗
3. 符号执行是如何做约束求解的
4. 哪些漏洞可以用fuzz检测到
5. 纯白盒了解多少？说几个市面上开源或者闭源的白合工具，知道是基于什么实现的吗
6. 反问

二面

时长：30分钟

1. 英语水平（ ok很看重英语，包括听说读写）
2. 聊项目
3. 介绍了很长一段的培养方案（很吸引人）
4. 聊理想、职业规划

0x3B 大疆 安全技术开发工程师

测评

形式：机考，80道单选

时长：80分钟

内容：

1. 性格测试
2. 行测（推理、逻辑、计算等）

笔试

形式：机考

时长：90分钟

内容：

1. 选择题14道，共66分，多选单选都有，主要是四大基础课内容
2. 编程题2道，共34分，每道17分，第一道应该是简单难度，第二道估计也就中等

总结：

好像和安全一点都不沾边这个笔试。。。总体难度应该是比开发低的（舍友投的开发岗，5单选5多选2问答1编程，编程是动态规划）

一面

时长：25分钟

1. 自我介绍
2. 介绍一次印象深刻的渗透测试
3. 再讲一个
4. 讲一个不利用poc、工具等的渗透测试
5. 讲一下完整的渗透测试的流程
6. 攻击时怎么防止被溯源
7. 防守时怎么溯源
8. 我看你也做过开发是吧，java、python什么的
9. 代码审计是怎么审的
10. 漏洞挖掘的方法方式
11. ct实习的时候有和甲方合作过吗，做了什么
12. ctf出题怎么出的
13. 反问：面试官部门的业务：护网、内部渗透测试、无人机漏洞挖掘

二面

时长：20分钟

1. 自我介绍
2. 实习3（互联网公司攻击队）工作内容
3. 渗透测试思路
4. 怎么判断蜜罐、蜜网
5. 代码审计思路
6. 代码审计一般会关注哪些地方
7. 反问

0x3C 经纬恒润

一面

时长：25分钟

1. 自我介绍
2. 研究生是考的还是保的
3. 考研多少分
4. 六级过了吗，多少分
5. 硕士期间参与了什么项目，自己是一个什么角色，承担了什么任务
6. 做项目用过什么工具
7. 实习经历这么多是网上找的还是真的（雾，这是什么问题....是指我的简历造假吗..直接拉低印象分）
8. 实习3（互联网大厂）工作内容
9. 说个印象深刻的漏洞复现
10. 说个印象深刻的工具调研
11. 实习2（乙方安全公司）工作内容
12. 说个印象深刻的代码审计
13. 实习1（互联网大厂）工作内容
14. 这几段实习、包括学校的项目，你觉得遇到印象最深刻困难是什么
15. java开发熟悉吗

16. 除了java还会什么语言，会c吗
17. 对工作地点有什么看法
18. 职业规划
19. 对出差和加班有什么看法
20. 说说自己的优点和缺点
21. 了解车载安全吗，聊一聊
22. 反问

> 做车载信息安全的，需要出差，出差时间从几天到月不等，平时不加班，基本965，项目上线前可能需要加班

0x3D 微众

笔试

时长：120分钟

选择*20 + 编程*3

选择很多java（八股、看代码写答案），还有操作系统信号量

编程：

1. 拼接数字
2. 移位数字（乘除2）
3. 升序子序列

一面

时长：20分钟

1. 自我介绍
2. 聊了hw
3. 聊了实习3
4. 聊hw任务分配
5. 聊成果
6. hw期间学到了什么
7. 问了工作意向方向
8. 介绍一下业务
9. 反问

二面

时长：25分钟

1. 自我介绍
2. 聊实习1、2、3
3. 聊实习3具体工作内容
4. 写poc的范围
5. 聊扫描器
6. 漏洞挖掘相关

7. https比http安全在哪，https原理
8. 怎么判断服务器身份
9. 数字证书里面包含了什么
10. 数字签名怎么产生的

HR面

时长：20分钟

忘记记录了。。

0x3E 百度

笔试

时长：120分钟

单选*4 + 多选*5 + 问答*5 + 系统设计*1 + 编程设计*1

问答：ssrf的常见绕过、减少企业安全漏洞、TEE安全启动、安卓检测模拟器

编程设计：动态规划/贪心算法 完全背包问题，代码不用运行，我只写了思路和伪代码

0x3F 米哈游

笔试

时长：90分钟

题型：15*单选（45分）+ 5*多选（25分）+ 1*问答（40分）+ 1* 编程（40分）

选择基本都是计算机基础（数据结构、计网、操作系统等）还有一些信息安全的概念（csrf的修复等）

问答：有人在公司的某网站上了个webshell并截图证明，你要怎么做，并进行安全加固

编程：不算难，排个序就差不多了，主代码就10行

一面

忘记记录了

问了一些通用漏洞、简历，问有没有挖过app的洞，聊了下微信小程序挖洞的思路，问到客户端（windows、安卓），我说不会，然后就没有然后了

0x40 传音控股

一面

时长：30分钟

1. 自我介绍
2. 渗透测试思路
3. owasp top10有什么
4. sql注入原理、分类、修复

5. xss原理、修复
6. dom xss修复
7. ssrf原理、修复
8. xxe原理、修复
9. xxe和ssrf区别
10. 反序列化原理、修复
11. 一般用什么语言
12. 做过开发吗
13. 都做过哪些开发，是二次开发还是完全自己开发
14. 反问

二面

时长：20分钟

1. 自我介绍（包括硕士的方向
2. 硕士的课程
3. 哪门课最感兴趣、为什么
4. 讲一个漏洞挖掘的经历
5. 家是哪里的
6. 工作地点的选择
7. 想做什么方向
8. 对自己的职业规划
9. 有没有其他offer
10. 反问

HR面

时长：50分钟

以hr介绍业务及发展路径为主，聊了职业规划、其他offer，谈了薪资、base等工作后相关的待遇福利等

0x41快手 安全工程师

一面

时长：50分钟

1. 自我介绍
2. 聊简历项目
3. 渗透测试的流程
4. 信息收集，有一个域名，怎么做信息收集
5. 收集完了怎么寻找突破口
6. 拿到webshell怎么扩大战果
7. 端口复用了解吗
8. 内网扫描除了扫服务和端口还会收集什么信息
9. sql注入的分类
10. mysql报错注入的函数
11. mysql读写文件的函数
12. sql server命令执行的方法
13. 除了xp_cmdshell还有什么
14. sql注入引号绕过

15. sql注入读文件和写文件可以用引号绕过吗（读文件可以，写不行，因为写文件不是一个函数）
16. sql注入的修复
17. 预编译无法防御的order by怎么修复
18. xss的修复
19. ssrf的修复
20. 一个域名怎么判断是不是内网域名
21. redis的攻击姿势
22. linux命令：最近登录的用户
23. linux命令：查看一个文件的后500行
24. linux命令：查看一个文件的行数
25. linux命令：查找文件的位置
26. linux文件权限777代表什么，分别代表什么
27. windows命令：知道一个端口，怎么找进程
28. windows命令：杀进程的命令
29. windows命令：怎么启动和终止进程
30. windows命令：忘了。。还有好几个
31. 手撕两道算法，第一道是路径标准化，用递归写（不会）第二道是版本号比大小（也没写完）
32. 反问

> 面试分三部分：基础问题（攻防）+操作系统问题（linux&windows）+手撕代码

二面

时长：45分钟

1. 自我介绍
2. 三段实习分别说说工作内容
3. 想做什么方向（攻防/安全运营）
4. 做过安全运营吗，做防守队的时候都做了什么
5. 使用过什么安全产品
6. 处置过什么攻击事件
7. 误报的来源都有什么
8. 代码审计审出过什么漏洞吗
9. 聊hw经历
10. 再聊hw经历
11. 继续聊hw经历
12. 有0day吗，聊聊挖掘思路
13. 文件上传漏洞的危害
14. 文件解析漏洞有哪些
15. %00截断的原理
16. 开发能力怎样
17. 写一条sql盲注的语句
18. 写一个xss获取cookie的payload
19. 有其他offer吗
20. 反问

三面

时长：65分钟

1. 自我介绍

2. 聊个印象深刻的攻防演练经历
3. 聊实习3的工作内容
4. log4j漏洞原理
5. 怎么防护
6. 如果公司有几万台机器需要防护，有什么思路
7. 。。。（忘了一部分了，都是业务相关的好像）
8. 开发能力怎样，擅长什么语言
9. 代码审计的思路
10. ctf打什么方向的题
11. 代码题：ssrf绕过方式
12. 代码题：写几个sql注入语句
13. 代码题：力扣1171

HR面

时长：35分钟

1. 硕士研究方向
2. （说了区块链和密码学，然后就聊了很久这东西。。）
3. offer的选择会关注什么
4. 对安全研究和业务安全有什么看法（拓展聊了不少国内互联网的情况）
5. 自己想做什么
6. 三方什么时候下来
7. 实习3的工作内容和架构
8. 反问

0x42 腾讯

一面

时长：80分钟

> 两个面试官，ieg基础安全团队，游戏技术运营

1. 自我介绍
2. 聊hw经历
3. 攻击腾讯的思路
4. 在没有web突破口的情况下还有什么方式进行攻击
5. 企业有hids的情况下怎么攻击
6. 企业要怎么做敏感数据泄露的防护
7. 聊hw中的绕过或技巧性强的经历
8. 怎么判断蜜罐
9. 攻击过程中遇到的困难
10. 聊简历项目
11. sqlmap源码看过吗，觉得有哪些技术性的特点
12. linux下后门的优缺点和排查方法（排查方法问的很细，包括排查的方法有什么问题、会遗漏什么都问了）
13. sql注入原理
14. 布尔盲注、报错注入原理
15. 写几个sql注入绕waf的语句
16. 数据库名、当前登录用户暴破
17. xss和csrf异同

18. 从研发转到安全的想法
19. tcp拥塞控制和慢启动
20. http三次握手
21. https的握手流程
22. 涉及到哪几方、用了哪些密码算法
23. https中有哪些攻击面
24. 在腾讯的收获是什么
25. 会关注前沿的安全资讯吗（云原生、开源框架、软件成分分析之类的）
26. 未来工作规划
27. 反问

0x43 海尔

一面

时长：15分钟

1. 自我介绍
2. 今年hw的职责、成果
3. poc怎么写的
4. 自己以后的发展方向
5. 接受去北方工作吗
6. 有女朋友吗
7. 反问

0x44 4399

一面

时长：15分钟

1. 自我介绍
2. 给一个web站点的渗透测试思路
3. dns劫持了解吗
4. arp劫持了解吗
5. ddos是tcp还是udp
6. 反问

0x45 滴滴

一面

时长：40分钟

1. 自我介绍
2. 渗透测试的思路
3. 攻防演练是代表哪参加的
4. 实习3（互联网公司攻击队）工作内容
5. 安全工具调研是做什么的
6. hw的分工，有什么成果
7. 最近做的漏洞复现

8. 实习2（乙方安全公司）工作内容
9. 聊了几个攻防项目
10. windows下的权限维持（利用windows特性）
11. java反序列化原理
12. 内网渗透怎么做的
13. 假如拿到了一台办公设备、笔记本之类的，有什么内网的渗透测试方法（除了内网扫描）
14. windows域渗透了解吗
15. 工具是自研的吗
16. 自己有参与工具开发吗
17. 自己写过什么小工具
18. 实习1（互联网公司防守队）工作内容
19. 有真实的入侵应急响应吗
20. 一台机器如果被入侵了需要怎么排查
21. 反弹shell有什么好的检测方法吗
22. 如果让你写入侵检测的规则，你会从什么方向入手
23. 聊了会自己的博客
24. 反问

二面

时长：35分钟

1. 自我介绍
2. 渗透测试的思路
3. 怎么通过域名找ip（绕cdn）
4. 怎么通过ip反查域名
5. 信息收集中子域名的收集手段
6. 谷歌语法：怎么收集子域名
7. 谷歌语法：识别指纹的时候，如何搜索路径
8. 谷歌语法：如何搜索前端源码的指纹
9. 平时poc怎么写的
10. 身份验证漏洞的poc怎么写的
11. fastjson和log4j了解吗
12. log4j有遇到过能rce的吗
13. ssrf怎么寻找漏洞点
14. 提权了解吗
15. redis攻击手法
16. 代码审计审的是什么语言
17. 聊0day
18. 聊了几个攻防经历
19. 大hw拿了多少分
20. 开发了解吗
21. 开发过什么工具
22. 有自己的linux服务器吗，用来干什么的
23. 反问

0x46 海康威视

一面

时长：15分钟

1. 自我介绍
2. 渗透测试的流程
3. 大hw的成果介绍
4. 觉得实习3（互联网公司攻击队）和其他攻击队比起来你们的优势在哪里
5. poc用什么写的，会经常关注新漏洞吗
6. 有了解最近的漏洞吗（spring、log4j）
7. 会研究一些产品的安全吗
8. 会java吗，代码能力怎样
9. 以后的方向规划
10. 反问（内部渗透测试、企业安全、产品安全（二进制、java）、省级攻击队）

二面

时长：20分钟

1. 自我介绍
2. 硕士期间的研究方向
3. 现在做的方向（web安全）和研究方向（密码学、区块链）不一样吗
4. 为什么选择这个方向
5. 当初是怎么学习的
6. 实习3（互联网公司实验室）的工作内容
7. 在这段实习中觉得自己哪里得到的提升或者进步最多
8. 实习期间遇到最困难的事情是什么
9. 哪里人
10. 对工作地点有什么要求吗
11. 对于offer的选择更看重什么
12. 了解杭州的情况吗
13. 期望薪资
14. 有女朋友吗
15. 其他正在面试公司的进度
16. 有几个offer了
17. 聊聊家庭情况
18. 反问

0x47 字节跳动 安全工程师

一面

时长：35分钟

1. 面试官自我介绍及部门业务和工作内容
2. 自我介绍
3. 硕士期间的研究方向是什么
4. 在学校有参加安全相关的项目吗（攻防演练、ctf）
5. 打ctf吗？有参加学校的战队吗？有打哪些比赛出过什么成绩吗？主要负责哪方向的题？
6. xx的工作内容？（xx指我的大厂实习，下同）
7. 你们写poc的范围和来源是什么
8. 会不会去官网下载补丁找diff
9. 可以说一下你的0day吗，这是可以聊的吗
10. 攻防演练的角色是什么，大概的一个攻击思路和流程？

11. 内网横向怎么做的，扫描器用的是什么
12. 内网中会关注些什么
13. 怎么打fastjson
14. fastjson历史漏洞、fastjson需要升级到什么版本
15. 讲一下jndi、rmi
16. 打点时擅长打什么类型的漏洞
17. sql注入的修复，预编译无法防御order by时，怎么利用和修复
18. sql注入空格绕过、引号绕过
19. CSRF的修复
20. XSS中svg的利用和修复
21. DNS重定向绑定
22. 同源策略了解吗
23. 学校的攻防演练中有没有让你们给出修复方案
24. 在xx实习的时候，身边有没有什么很厉害的人介绍一下
25. 擅长什么语言，python和go会吗
26. 反问

0x48 美团 安全工程师

笔试

时长：120分钟

5道编程

一面

时长：30分钟

1. 自我介绍
2. 说一下技能栈都有哪些
3. 印象比较深的渗透测试，比较能体现技术能力的渗透测试
4. 再讲一个有打点过程的
5. 再讲一个
6. 数据库提权方式（任意数据库）
7. 通过数据库getshell都有哪一些
8. redis主从复制的利用手法
9. sql server除了xp_cmd还有别的rce方式吗
10. java反序列化在构造链的时候可以用到哪些类、组件、接口
11. 实习安排的工作中花费最长的是研究什么事情，花了多久，成果是什么（不是别人安排的，是自己研究的）
12. 0day聊一聊
13. java表达式注入研究了什么，成果是什么
14. 攻防演练中除了打点还做了别的事情吗
15. sql有两个数据集a和b，怎样取在a中但不在b中的数据
16. 进到内网后一般会做什么
17. 反问：面试官的业务：入侵检测（流量上、终端上）

0x49 vivo

笔试

时长：90分钟

题型：单选*6 18分 + 多选*4 12分 + 编程*3 70分

一面

时长：30分钟

1. 自我介绍
2. 介绍一个攻防经历
3. 内网扫描的时候没碰过hids吗，不会被拦截吗
4. 攻击的时候机器不出网怎么办
5. 有堡垒机怎么办
6. 数据库中的数据没加密吗，加密了怎么办
7. 被ban ip了怎么办
8. 如果攻击的是个人PC可以怎么找数据
9. 域渗透
10. 介绍另一个攻防经历
11. 登录做了双因素认证怎么办
12. vpn服务器没绑定机器编码（证书）吗
13. 反问

HR面

时长：30分钟

1. 自我介绍
2. 了解vivo吗
3. 几段实习经历中觉得哪段收获最大
4. 在学校做的什么事情是最有成就感的
5. 身边的同学和老师是怎么评价你的
6. 遇到过什么印象深刻的困难
7. 怎么解决的、怎么缓解压力的
8. 对于今年互联网不太乐观的形势，有什么想法
9. 对于工作的选择会看重什么要素（待遇、平台、地点、工作内容）
10. 期望薪资
11. 反问

0x4A 小米

笔试

时长：90分钟

单选+多选+不定项+判断

一面

时长：45分钟

1. 自我介绍
2. 聊一个hw经历
3. 聊云aksk相关的利用和防御
4. 聊在只有任意文件读取一个点的情况下有什么利用方式
    1. 怎么找开了什么服务（`/proc/pid/cmdline`）
    2. 怎么找绝对路径
    3. 怎么找配置文件
    4. linux开机自启动文件`/etc/rc.d/rc.local`、`/ etc/init.d`
5. 聊另一次hw经历
6. 聊sso相关的攻击方式
    1. 怎么绕过动态token
    2. 怎么绕过双因子认证
7. 反问

二面

时长：45分钟

1. 自我介绍
2. 介绍一次hw经历
3. hw分工
4. 内网扫描有流量检测怎么办
5. 木马怎么写
6. 域环境怎么打
7. 不出网攻击方式
8. 协议绕过，比如tcp有限制
9. sql注入getshell
10. udf提权
11. 文件上传绕过
12. iis文件解析漏洞
13. redis攻击方式
14. redis主从复制条件
15. redis版本限制
16. jwt攻击方式
17. 聊我的博客
18. 栈溢出原理
19. 栈溢出保护机制
20. 做过什么开发
21. 反问

0x4B TCL 鸿鹄实验室 软件开发工程师（安全方向）

笔试

52题，限时2小时

俩主观，一道密码学设计，一道算法（算法题不用运行，直接写代码）

判断+单选：大部分是c语言的知识，还有一部分安全的知识（包括密码学和一些安全的概念）

一面

时长：35min

1. 自我介绍
2. 计网OSI七层模型+协议
3. https比http安全在哪
4. sql注入的原理
5. sql注入的拼接和闭合是什么意思
6. 延时注入
7. xss的修复（后端怎么修，前端怎么修）
8. 水平越权和垂直越权
9. 擅长什么语言
10. 实习1干的活（互联网公司防守队）
11. 有没有用过运维产品
12. 处置过什么告警、研判、溯源
13. 实习2干的活（乙方安服）
14. java代码审计审的是什么
15. 了解了一下简历上的几个攻防演练
16. 信息收集的过程
17. 信息收集的目的
18. 实习3干的活（互联网公司攻击队）
19. 写poc用什么写的
20. 实习中独立完成或者印象深刻的例子
21. 打过云服务吗，怎么打的
22. 假如现在你的攻击目标，只有各种接口，不是传统的web服务，你有什么攻击思路
23. 反问

二面

时长：45分钟

1. 自我介绍
2. 在学校都学了哪些课程
3. 硕士研究方向是什么（答了密码学、区块链）
4. 密码学都学了什么
5. 区块链介绍一下原理
6. 区块链的共识算法介绍一下
7. 工作量证明是怎么做的
8. 为什么哈希的值需要穷举
9. 比特币的计算难度是怎么控制的
10. 国家hw的成果
11. 小组分工情况
12. 小组人员的配置
13. 得分大概是什么水平
14. 自己找了哪些突破口
15. 工作中觉得老员工和新员工的差距在哪里
16. 经验上的差距一般体现在什么地方

17. 平时有什么兴趣爱好
18. 打篮球吗
19. 打游戏吗
20. 王者荣耀什么段位
21. 游戏安全了解吗，外挂的原理?
22. 反外挂反作弊了解吗
23. 觉得国企和互联网企业的安全水平哪个更高
24. 对国内安全行业和互联网的看法
25. 了解TCL的业务吗
26. 对于广州和深圳这两个城市，有什么评价、对比（我说了我在广州，然后岗位base在深圳）
27. 反问

0x4C 京东 安全工程师

笔试

20单选+3编程

单选有漏洞的修复方式、数据结构、看代码等

编程

1. 字符串大小写
2. n^2的矩阵，相邻数之和为奇数
3. 长城数

一面

时长：45分钟

1. 自我介绍
2. 渗透测试的流程
3. fastjson和log4j了解怎么打吗
4. ssrf了解吗，常见漏洞点有哪些，危害是什么
5. 文件上传漏洞的绕过
6. 文件解析漏洞（IIS、Apache、Nginx）
7. sql注入原理，二次注入原理
8. xxe原理
9. 有没有用xxe直接rce过
10. 对浏览器的会话状态了解吗（cookie、session）
11. 擅长什么语言
12. 聊一下0day
13. 做java项目代码审计的步骤
14. 了解移动端的渗透测试吗（说了微信小程序）
15. 微信小程序有和安卓一样的activity组件吗
16. 微信小程序反编译的混淆和加密怎么处理的
17. 木马病毒这块了解吗，怎么做免杀
18. 二进制了解吗
19. 有没有防守方的经历
20. 用的什么类型的安全产品
21. 用的时候感觉有什么优缺点

22. 上机排查的步骤
23. 做过溯源吗
24. 蜜罐溯源了解吗（jsonp）
25. 有用过远控工具吗（C2这些）
26. 有接触过开源管理工具吗（ossim之类的）
27. 写poc用什么写的（答python）用了python什么库
28. 扫描工具用的是什么
29. 反问：面试官部门的业务（集团内部安全、产品上线的渗透测试等）

二面

时长：40分钟

> 这一面基本没什么技术问题了，都是些对具体问题的看法和解决思路什么的

1. 自我介绍
2. 硕士期间的研究方向
3. 毕设题目
4. 办公网的安全防护要怎么做
5. 从攻击者的角度看，防守方应该怎么防守（这个问了挺久，外网到内网都聊，大概就是从攻击的每一个步骤相应的去分析）
6. 其他一些攻击，例如近源渗透（还有啥忘了）这些攻击要怎么防护
7. 实习了这么久怎么不打算转正（没hc+自己太菜。。）
8. 聊了当时实习的选择
9. 实习期间除了技术上的长进，其他的关于人际关系方面有没有什么收获
10. 实习期间有没有遇到什么困难，怎么克服的
11. 聊了实习和学业的平衡
12. 团队的工作，在需要远程的情况下有什么困难点
13. 聊了学业成绩
14. 聊了学校的经历
15. 有参加过学校的组织或者活动吗
16. 反问（这个岗位工作量可能比较大，工作安排可能会比较紧凑）

hr面

时长：25分钟

1. 自我介绍
2. 硕士期间研究方向
3. 本科学什么的
4. 本科参加的社团
5. 选择本科专业和硕士专业的时候是怎么选择的
6. 实习（互联网大厂）这么久，聊一下工作内容和收获
7. 实习期间最有成就感的事
8. 导师对你的评价
9. 实习为什么不转正
10. 对工作地点的看法
11. 国企、互联网、外企想去哪个
12. 对国内互联网形势的看法（卷的程度、加班等）

13. 为什么想进互联网
14. 为什么选择京东
15. 有和一面二面面试官了解我们部门的业务吗
16. 对我们部门有什么看法吗
17. 反问

0x4D 阿里-菜鸟

一面

时长：30分钟

1. 自我介绍
2. hw的职责
3. hw的成果
4. 分享一下有意思的案例
5. 每年的hw的分数和规则有什么不一样的地方
6. 除了hw以外自己会去挖漏洞吗
7. 代码审计的思路，审计的流程
8. 代码审计是java还是php的
9. java用的多吗
10. java反序列化（fastjson、log4j、本身的反序列化的区别）
11. java fastjson怎么修复
12. java原生反序列化（readObject、writeObject）的修复
13. 黑盒渗透测试的思路
14. 找回密码的逻辑漏洞
15. 有没有做过开发相关的，写小工具之类的
16. 了解阿里、菜鸟职级的消息吗
17. 反问

二面

时长：35分钟

1. 自我介绍
2. 今年hw的经历，展开说说
3. 这次hw和往年有什么区别，和往年不同的地方，规则、攻击方式等
4. 对供应链的数据分的看法
5. 甲方视角下关于代码审计的想法
6. 对越权类漏洞的看法，从研发的角度来看的话
7. 最近发生的安全事件以及看法（聊了spring4shell和log4shell)
8. 可以说一下对这两个的看法吗（其实面试官问的是安全事件以及看法，但是我莫名就回答成了漏洞的原理。。）
9. 西北工业大学攻击事件，对这样的事情怎么看
10. 上海数据泄露事件的看法
11. 以甲方视角聊聊对安全行业的看法，安全措施、安全策略和思路之类的
12. 在自己的职业规划里有什么自己的要求，如果选择以菜鸟为offer的话是什么想法
13. 为什么没留在实习3（互联网大厂）
14. 反问

三面

时长：25分钟

1. 自我介绍
2. 介绍实习经历和项目经历
3. 写poc的要点、会写哪些产品的poc
4. 指纹识别的要点
5. 做测绘引擎时的关键因素有什么
6. 实习3的hw成绩
7. 你们能取得这个成绩的关键因素是什么
8. 聊了下实习3
9. 反问

HR面

时长：40分钟

1. 自我介绍
2. 聊了下对攻防演练的看法
3. 聊了下攻防演练中从防守队视角最容易或最常见的攻击类型
4. 聊了下工作地点的意向程度
5. 反问

0x4E 完美世界 安全分析工程师

一面

时间：30分钟

1. 自我介绍
2. 聊了一下简历上的攻防经历
3. 聊了漏洞挖掘的方式
4. 聊了一下护网的事
5. windows和linux怎么查看登录日志
6. windows自启动的方式
7. 假如现在一台机器中了木马，知道他的C2回连地址，怎么找出这个进程
8. 一台有web服务的机器，中了挖矿木马，怎么应急处置
9. 聊了一下实习1防守队的经历
10. 内网流量了解吗
11. 怎么写ssh暴破的规则（不是主机上的规则，是路由器上流量的规则）
12. 聊了一下他们的安全业务和需求（应急响应、规则分析之类的）

二面

时长：30分钟

1. 聊实习3（互联网公司红队）的经历
2. 国家hw的成果
3. 自己找到了哪些突破口

4. 聊学校攻防演练
5. 聊成果，怎么打的，数据怎么获取的，shell怎么拿的
6. 聊其他hw经历
7. 上传了文件然后执行不了是什么原因
8. 聊实习1（互联网公司蓝队）的经历
9. 应急响应怎么做的（要关注什么地方）
10. 怎么处置告警的，误报会不会很多
11. 发现被扫描了会怎么处理
12. windows下的应急响应（发现回连了c2服务器怎么排查）
13. c2地址是域名不是ip的情况下怎么排查
14. linux下怎么做应急响应
15. 做过pc端的逆向吗（二进制那种逆向）
16. 反问

0x4F 深信服 漏洞研究员

笔试

15不定项45分+10填空20分+2编程25分

选择大多是计网（http协议）+代码分析+windows PE文件分析+部分二进制

填空有sqlmap的参数、tcp三次握手

编程ak，一道送分，另一道思路不难，实现略麻烦

一面

时长：40分钟

1. 自我介绍
2. sql布尔盲注原理
3. sql联合注入的union有什么限制
4. 字段数要匹配，这个需要怎么做
5. 同源策略
6. xss为什么无法用同源策略防护
7. xss的修复
8. ssrf是什么，怎么利用
9. ssrf打redis
10. 文件上传的绕过方式
11. 浏览器访问hxxps://www[.]sina[.]com.cn的流程
12. 实习3工作内容
13. 实习2工作内容
14. hw成果
15. 聊聊漏洞挖掘的思路
16. 逻辑题：A和B赛跑两次，第一次A到终点时B差1米，第二次A后退1米开始跑，求问谁先到终点
17. 代码题：二分搜索
18. 反问

二面

时长：25分钟

1. 自我介绍
2. 聊攻防演练经历
3. 攻防演练规则变化
4. 聊一个攻防演练项目
5. 再聊一个
6. 聊漏洞挖掘思路和0day
7. 对现在这种业务逻辑漏洞有什么想法
8. 反问

三面

时长：40分钟

1. 自我介绍
2. 聊hw经历
3. 聊一次攻击
4. 聊漏洞挖掘
5. hw中自己挖的洞有没有真正能够利用的
6. 实习公司hw成绩好的原因
7. 有没有做过开发
8. 硕士研究方向
9. 进度怎样
10. 现在在干嘛，一天的时间分配
11. 过去一年遇到过什么比较大的困难
12. 同学和老师是怎么评价你的
13. 如果你在团队中出了最多的力却不被认可怎么办
14. 如果团队中出现意见不合的情况怎么解决
15. 自己的职业规划
16. 怎么没留在实习公司
17. 家是哪里的
18. 其他offer
19. 反问

HR面

时长：60分钟

1. 对前面的面试流程有什么建议或者意见吗
2. 经历过最困难的事情
3. 在实习3学到了什么
4. 聊hw
5. 想做什么方向的工作
6. 自己现在想学什么
7. 对安全不同方向工作内容的看法
8. 在一个团队中出现意见不合的情况怎么解决
9. 怎么平衡学习和实习
10. 平时一天都在干什么
11. 用三个词形容自己
12. 胜负欲体现在哪些方面
13. 身边的同学对你的评价最多的是什么

14. 为什么没留在实习3
15. 投了哪些公司
16. 选择offer会考虑什么因素
17. 现在有哪些offer
18. 反问

0x50 联想

笔试

20选择（有两三道多选）+2编程

选择包括数据结构、操作系统、linux操作、密码学、部分安全知识

编程第一道：字符串修改，三行代码搞定

编程第二道：制造回文串

一面

时长：20分钟

1. 自我介绍
2. 平时用哪个语言，用来干什么
3. java和python在写工具或者漏洞武器化时怎么写的，用了哪些类库
4. 漏洞挖掘（代码审计）的思路
5. 对产品的漏洞挖掘，比如移动端和iot方面，有兴趣吗，可以接受后续的学习吗
6. 渗透测试思路
7. 聊了某次攻防演练的成果
8. 聊了另某次攻防演练的成果
9. 聊了另另某次攻防演练的成果
10. 扫描器是用什么写的
11. 现在人在哪
12. 能接受去北京吗
13. 本科哪里读的
14. 什么时候毕业
15. 实习1和实习2 base在哪

0x51 商汤

一面

时长：35分钟

1. 自我介绍
2. 给一个网段，聊聊攻击思路
3. xss的修复
4. xss所有地方都可以用html编码修复吗
5. 在设置了httponly的情况下怎么利用xss
6. sql注入绕waf
7. 文件上传绕waf
8. 有没有了解过windows&linux的提权
9. mysql提权的条件

10. log4j漏洞原理
11. jndi原理
12. log4j除了升级版本外还有什么修复方式
13. jsp免杀
14. 从甲方视角，如何检测web服务器是否被上传了webshell
15. 内网渗透，windows域渗透
16. msf用的多吗
17. docker和k8s的漏洞了解吗
18. docker逃逸
19. docker api未授权
20. 拿到一个webshell怎么判断他是在docker里还是实机里
21. 反问

二面

时长：35分钟

1. 自我介绍
2. 聊个印象深刻的经历（细聊细节，聊了很久）
3. 再聊一个印象深刻的经历（也是细聊）
4. python一般是用来干什么的
5. 漏洞挖掘的思路
6. 水平越权怎么进行代码审计
7. java中的注入怎么防御（sql、xss）
8. spring的鉴权
9. burp使用（场景：token不能重放的情况下怎么设置）
10. 反问

0x52 竞技世界

笔试

时长：很快

10单选20分+10不定项30分+7问答50分

都是很纯粹的安全问题，不算难，但问答题属实有些不容易写，感觉把一面提到问答来考察的感觉

一面

时长：50分钟

1. 自我介绍
2. 实习3（互联网大厂）的经历
3. sql注入延时注入的函数（mysql、sql server、oracle）
4. 报错注入的函数
5. 接4，这两个函数在数据库执行的原理是什么
6. 布尔盲注中使用substr可能会动静太大，有什么别的方法吗
7. 数据库读写文件的条件
8. sql注入的各种绕waf方法
9. select被过滤了怎么绕过（除了注释符）

10. mysql提权方法
11. udf提权可以在linux下使用吗
12. ssrf常见的漏洞点
13. ssrf有哪些可以利用的协议
14. ssrf怎么打redis
15. jsonp了解吗
16. 怎么避免踩jsonp蜜罐
17. csrf的修复
18. 会代码审计吗
19. php命令执行的危险函数有哪些
20. 怎么寻找路由映射
21. 审过php框架吗
22. java反序列化怎么回显（除了dnslog带外）
23. java内存马原理
24. 机器重启后内存马还在吗
25. tomcat内存马分类
26. 内存马怎么排查
27. 审过什么产品（各种oa什么的）
28. 用友nc常见漏洞点在哪
29. coremail前段时间的0day有了解吗
30. 场景题：现在有一个文件上传点，上传的服务器是一个存储桶，但是他和目标的主域名是相同的，能够怎么利用
31. 场景题：fastjson不出网不回显怎么打
32. 场景题：当你代码审计时发现了一个后台的命令执行，怎么想办法在前台利用
33. 场景题：云上的一个机器，他有一个虚拟局域网，拿到webshell后攻击思路是什么
34. 场景题：打了个webshell，机器不出网怎么搞
35. 自己有破解过验证码吗
36. 大hw的角色分配
37. 扫描工具是开源的还是自研的
38. 免杀了解吗
39. 内网渗透怎么做的
40. 怎么找域控
41. 会钓鱼吗
42. 某次攻防演练成果（源码泄露、云aksk相关）
43. 打的是哪个云，怎么利用的
44. 另某次攻防演练成果（nday rce和杀软对抗）
45. 平时都是从哪获取安全资讯的（安全事件、漏洞预警、漏洞细节等）
46. 平时有看哪些知识星球
47. 现在有拿其他offer吗
48. 反问

二面

时长：30分钟

1. 自我介绍
2. 介绍一下攻防的经历
3. 做过入侵检测、应急响应之类的事吗
4. 有什么比较有成就感的事
5. 为什么没留在实习3
6. 对工作地点是怎么看的

7. 对公司规模是怎么看的
8. 面试官介绍了很久的安全业务和公司情况
9. 反问

三面

时长：50分钟

1. 自我介绍
2. 自己的优点和不足之处是什么
3. 最有成就感的事
4. 为什么有成就感，是什么给你带来了成就感
5. 之前实习离职的原因
6. 经历过最困难的事
7. 如果不考虑其他因素的话，自己最想做什么方向
8. 对自己职业道路的规划
9. 觉得自己带领团队的话有什么优势
10. offer的选择会参考什么因素
11. 一个规模大但工作内容单一的offer和一个规模不大但会接触很多方面知识的offer二选一，为什么
12. 工作地点的选择
13. 对同事有什么期待
14. 家庭情况（父母工作、是否独生、家在哪）
15. 有女朋友吗
16. 还拿了什么offer或者意向
17. 为什么不留在实习3
18. 反问

HR面

时长：40分钟

1. 自我介绍
2. 对一二三面面试官和面试流程的评价
3. 高考多少分
4. 考研还是保研
5. 介绍下实习3（甲方红队）
6. 哪里人
7. 工作地点的选择
8. 自己工作学习方面的特点
9. 自己秋招的优势和劣势
10. 了解竞技世界吗
11. 面试官介绍公司情况和业务
12. 问了前几段实习的base
13. 对北京互联网和北京文化的看法
14. 考虑offer的因素
15. 手里其他offer或者投递其他公司的进展
16. 反问

0x53 度小满

一面

时长：25分钟

1. 自我介绍
2. 聊一下0day
3. 有提交到什么平台吗
4. 聊一下本科专业
5. java开发有做过网站吗，用的什么框架
6. 代码审计一般审什么语言
7. 代码审计会用什么工具先审一遍吗
8. php的危险函数
9. 审计时用了什么工具
10. 加密的源码怎么处理
11. 实习3（互联网公司攻击队）的实习经历
12. 实习3的绩效考核
13. 为什么离职
14. 实习2（乙方安全公司）的实习经历
15. 实习2什么项目给你留下了比较深刻的印象，或对你提升比较大的
16. 实习1（互联网公司防守队）的应急响应经历
17. 溯源经历
18. python用的多吗
19. 写poc会审计1day吗
20. 反问

二面

时长：40分钟

1. 自我介绍
2. web安全一般熟悉哪块
3. 聊一下LFI（本地文件包含）
4. 聊一下sql注入（分类）
5. 布尔盲注聊一下
6. 延时盲注聊一下
7. mysql除了sleep还有什么函数可以用
8. 数据库的rce
9. mysql读写文件怎么做的
10. 了解mysql读文件的溯源吗（mysql蜜罐）
11. sql server的命令执行，除了xp_cmdshell还有别的方式吗
12. h2数据库的rce
13. mysql 8有关注吗，什么特性可以利用的
14. 有没有挖掘过框架、中间件的sql注入
15. 预编译和参数绑定的区别（预编译在数据库操作层面，参数绑定在代码层面）
16. 实习2（乙方安全公司）的经历
17. java表达式引擎研究了什么
18. 实习3（互联网公司攻击队）的实习经历
19. 大hw的成果
20. 0day聊一下
21. java代码审计怎么审的
22. 越权漏洞怎么找的
23. java反序列化原理

24. cc链各种利用姿势
25. 在一个java项目中怎么找可以利用的链
26. java反射的具体流程
27. java动态代理
28. log4j的反射怎么利用的
29. 拿到shiro的key后怎么找利用链
30. 有什么我刚刚没问到的东西吗
31. 对自己以后的安全道路有什么规划吗
32. 反问

三面

时长：40分钟

> 非技术面，基本就是性格、心理等的面试，主要考察和部门、企业文化的契合度之类的

1. 自我介绍
2. 用三个词语来描述一下自己
3. 是什么支撑着你获得今天的一些成就
4. 在选择这条道路的时候是怎么想的
5. 对自己未来工作的规划
6. 对自己技术上的规划
7. 觉得自己的好奇心强吗
8. 这二十多年最懊悔的事和最有成就感的事
9. 怎么看待事在人为，谋事在人成事在天这两个词语
10. 怎么看待按部就班，循序渐进，你觉得这是事情最好的解决方案吗
11. 有没有做过一些违规的事
12. 有没有对别人做出承诺然后没有做到的情况
13. 如果自己的团队处于竞争劣势的话你会怎么办
14. 如果团队里面有人是你反感的类型你会怎么办
15. 有哪些事情或任务是你不想去做的，你会怎么办
16. 当你接受一个全新的任务的时候，你会怎么评估任务的难度
17. 之前实习的公司有没有发offer的
18. 反问

HR面

时长：15分钟

其实也不算面试，应该算“保温”电话

问了意向，其他offer和意向的情况，问了我有没有什么想了解的

0x54 绿盟 梅花K

一面

时长：50分钟

1. 自我介绍
2. 做过开发吗
3. 接触安全的时间

4. 介绍实习3的工作内容
5. 攻击思路
6. 大hw成果
7. 粤盾成果
8. 内网攻击方式
9. 有自己开发工具吗
10. 聊漏洞挖掘思路
11. java搞的多还是php搞的多
12. 聊0day
13. 聊泛微和致远
14. 场景题：fastjson不出网不回显利用（拓展：BCEL不可用）
15. 场景题：php站，文件上传403，怎么打
16. 场景题：shiro绕waf（长度检测、关键字检测）
17. 场景题：代码审计，php无`serialize`和`unserialize`怎么反序列化
18. 场景题：RDP的时候被人挤下去了怎么办
19. 场景题：拿了一台内网机器，发现有个zabbix agent，怎么打zabbix server
20. 打过云环境吗
21. 打过域环境吗
22. 工作地点选择
23. 反问

二面

时长：25分钟

1. 自我介绍
2. 实习2（乙方安全公司）离职原因
3. 实习3（互联网大厂）离职原因
4. 实习3工作内容
5. 开发能力怎样，有参与大型工具或基建编写吗
6. 有没有统计过自己审计了多少套大型项目
7. java还是php
8. 代审的思路
9. 内存马的分类
10. 内存马怎么排查
11. shiro的原理
12. 反序列化为什么需要gadget
13. IAST和RASP的相同之处和差异
14. 反问

0x55 中兴-未来领军-软件开发工程师-网络安全

作者：B1@nk
链接：https://www.nowcoder.com/discuss/531859044491890688
来源：牛客网

一面

1. 自我介绍；
2. OSI网络七层/五层模型；
3. Ping属于哪一层？底层依赖什么协议？
4. TCP和UDP的主要区别？
5. 如何结合TCP和UDP，保证大量数据传输效率的同时尽可能增加数据可靠性？
6. HTTP3.0基于的底层协议是什么？具有哪些特性？
7. 使用过/常见的对称密码算法？哪些具有安全问题？具有什么样的安全问题？
8. 使用过/常见的非对称密码算法？
9. 对称和非对称密码算法的适用场景？
10. 使用过/常见的散列算法？MD5安全性？
11. 对区块链有了解吗？区块链现阶段应用场景？
12. 熟悉常见密钥协商/交换等安全协议吗，如IBE，SSL？
13. 了解指令集加速或拥有该方面开发经验吗？
14. Intel SGX的原理？项目中使用可信内存实现什么功能？

二面

1. 自我介绍；
2. 选一个收获最大的项目介绍，你在其中扮演什么角色？主要负责哪些工作？
3. 除密码算法流程解耦外，分布式落地过程中还存在哪些问题？
4. 系统内部不同实体之间安全性如何保证？
5. SSL应用过程中应注意哪些问题？
6. 对嵌入式开发，汇编，AVX指令熟悉吗？
7. 树莓派项目中遇到什么难点？
8. 交叉编译过程中除更换编译链之外还有哪些难点？
9. 主语言是什么？
10. 老家，择业观，升学期望，薪资期望；

0x56 美团

作者：幾
链接：https://www.nowcoder.com/feed/main/detail/5c27e13dafeb4ae783237eea67729bd8?sourceSSR=search
来源：牛客网

一面

1. 自我介绍
2. 实习
3. 聊天局，不会挖洞，后面就不问挖洞了
4. smail相关。数组表示的方法；修改smail，如何重打包
5. arm指令。跳转指令有哪些,如何切换寄存器状态
6. 如何分析so层的文件
7. 检测frida及绕过方式
8. 检测方法写在so层，如何处理
9. fps外挂功能，使用场景，外挂原理，如何分析
10. 小程序保护杂谈
11. js域名锁定
12. js防格式化
13. selenium隐藏特征
14. 反问

> 备注：从0x57~0x5B均来自于Drunkbaby师傅的博客
>
> 链接：https://drun1baby.top/2023/08/23/2023-%E6%98%A5%E6%8B%9B%E5%AE%89%E5%85%A8%E7%A0%94%E7%A9%B6%E5%B2%97%E4%BD%8D%E9%9D%A2%E7%BB%8F%E5%88%86%E4%BA%AB/

0x57 安恒-卫兵实验室

1、你的简历与你之前发过来的简历有什么变化吗?

2、说一说你研究过的东西，然后有什么产出

这里我说研究了 Weblogic、shiro，但是没产出，那边似乎比较失望。

3、最近出了 Weblogic 的一个新的洞，你有研究过吗？自己在研究的时候有没有思考过别人是怎么挖出来的洞。

人麻了，没复现漏洞过，然后也没思考过这个。。

4、你觉得挖什么样子的洞比较好呢？你一般是怎么开展研究的

我说看漏洞类型，但是无论如何你需要先去简单了解一下它的流程，如果一个组件的流程你不清楚，盲目的开始挖洞比较愚蠢，像盲人摸象。然后在了解过基础流程之后，如果是反序列化的洞，就用 codeql、tabby 这些东西去找漏洞。

不知道那边是什么想法，不过有一说一面我的时候感觉大部分时候都是吸气和叹气qaq

5、你学习安全是什么时候开始的呢，一路上的经历是怎么样的

就简单聊了聊

6、有没有什么让你感觉很自豪的项目

当时说了 golang 写 sqlmap

7、你是什么状况下去学习 golang 的呢？是出于什么考虑呢

似乎很多面试官都会问这个问题，还是和之前一样回答了一下。

8、为什么在连连只实习了一个月呢？都做了什么业务

xxx

9、能简单说说在连连做了什么渗透测试吗?

10、能说一说常见的 SQL 注入种类吗？自己有绕过过一些 SQL 注入的 waf 吗?

这里说了绕过安全狗，麻了，当时就想到很可能会问 HIDS 的相关内容，果不其然后面就问了

11、一般是怎么绕 waf 呢？具体说说

我说了先 fuzz，然后具体的 bypass 就根据可用字符来打，那边似乎很不满意

12、有遇到过语意型的 waf 吗？自己是怎么 bypass 的呢?

我这里真的有点麻，满脑子都是 HIDS 和阿里的产品，包括先知 ban waf

13、如果给到你一个1day，你要怎么样进行漏洞分析呢?

14、又问了我如果就是一个 SQL 注入的 1day，让你漏洞分析，你会怎么分析呢，比如是有些特定条件下的 SQL 注入，比如什么什么配置文件下，你会怎么分析呢?

15、那你这样分析流程不会很耗时间吗？如果ddl之前你还没有分析完漏洞呢？你会怎么办？

16、那如果还是分析不出来，你是不是要思考一下你的方法是不是有问题了

我: 嗯……应该是吧

17、那如果你的 1day 积累的很多都完不成呢

我说我可能会考虑问一下其他有过经验的师傅，多多取经。

我大致了解你的情况了，能说说 SSRF 怎么样才能最好的利用呢?

我说，SSRF 用的好的话是可以 rce 的，但是前提是你需要先探活。当然这里 rce 的方式有很多，比如配合文件上传 gopher 打。

18、那如果目前我们探活出来有个 redis 服务，你要怎么打呢

SSRF 打 redis 的本质就是仿 redis 命令，将其写入一些 shell。我答了最多的一般都是 crontab，还有写入 shell，就类似于文件包含的原理。其实还有写入 ssh 私钥。还有主从复制什么的。

19、能说一说 ssrf 的防御嘛

我说了加白，最常用的方法，后续又补充了说限制一些不必要的协议，像 gopher 这种完全没必要啊，还有就是不给回显，这样的话对方探活也探不出什么东西，可能就以为这里并不存在 ssrf，但还得是白名单牛逼

20、那如果在变量里面呢？你要怎么过滤

我感觉这里就是加个 filter，实现单一职责原则

21、那如果我这里限制了 127.0.0.1，限制了 127.0.0.2 ，那你要怎么 bypass 呢

我直接说了 dns rebinding，我说这种攻击非常可观。面试官问我还有没有其他的呢？我补充了 @ 符绕过，进制转换，句号替换.符号。

22、能展开讲讲 @ 符是这么绕过的吗

这里其实是和 url 协议是有关系的，因为我们本质的 url 协议是这样请求资源的
http : //url@ip，然后后面跟上请求的资源，比如 http://www.baidu.com@1.1.1.1，那么我们这里把后面 @ 的内容修改成恶意的 127.0.0.1即可。

23、面试官又问，如果把这些各种符号都禁了呢，因为很多时候我们会过滤这些输入。

我说那就 dns rebinding 呗，面试官说 dns rebinding 的事儿到时候再说。然后答了进制转换，他说算一种，又答了 xip.io 与 xip.name
泛域名解析，无需配置，将自定义的任何域名解析到指定的 IP 地址。假设你的 IP 地址是 10.0.0.1，你只需使用 前缀域名+IP地址+xip.io 即可完成相应自定义域名解析。

24、关于内存马有了解嘛？可以简单讲讲有哪些内存马吗?

我说了我只搞了 Tomcat 型内存马，我知道还有 Agent 型内存马和 websocket 型，还有 upgrade 型内存马。

25、内存马的查杀了解过原理吗?

我麻了，我说看调用的所有的filters，看哪些 filters 是恶意的，是程序没有的

26、后面问了问实习薪资期望

0x58 白帽汇-安全研究

一面

1、自我介绍

2、讲一讲最近在做什么吧

3、说一说 Shiro 这个洞都了解多少

4、自己有没有独立挖出过 0day

5、weblogic 了解多少

说了一下复现了的漏洞，然后面试官让我说一说具体的一个漏洞

6、weblogic 的 T3 和 XMLDecoder 漏洞展开讲讲吧

7、fastjson 复现过多少漏洞，你研究的版本是多少

8、能简单说一说 Java 反序列化的流程吗?

9、讲讲 RMI 的通信原理以及为什么会存在漏洞

10、看到你还有在看 PHP 的东西，一般是研究哪种为主呢，PHP 还是 Java

11、说一说你做过的一些项目吧

12、写这个 Java 路线，你是出于什么考虑呢?

13、看到你审计过一些 CMS，自己从中有什么收获吗?

二面

二面主要是聊了聊一些挖洞的思想/个人经历，很有聊天的感觉，个人忘记记录完全了。

HR 面

1、看到你的简历上写了有说网络安全协会，都做了协会哪些工作呢

2、预期薪资是多少呢，我说在北京差不多 330/天吧

后面又说给实习生薪资一个月是 5500

3、有没有一段很难的时光

4、你是独生子女吗

5、最让你自豪的一件事是什么

6、在 CTF 上让你有很自豪的事情吗

7、有收到其他家的 offer 吗

8、目前多久能过来呢

0x59 极氪-安全研究

1、简单说一说你作为红队，在 hvv 期间会有怎样的视角

我说，这是不是就是 hvv 视角下的红队攻击。面试官说是的

然后就说了社工钓鱼、信息收集、外网打点、内网横移、还有就是通过信息泄露拿源码，再进行源码审计，再就是 0day、1day 的应用、恶意流量分析

2、听到你说了源码审计，简单说一下思路吧

就还是那一套 filter ——> pom.xml ——> 细的功能点 ——> 调试

3、说一说如果 hvv 期间出了一个 fastjson 的 day，你需要怎么防护

给我特么问住了，面试官其实在这个过程中一直在向我往工具利用那方面引导。我说了加黑，然后加白这样的策略。

他又和我说，怎么样判断资产里面是否存在这个漏洞呢。我说用工具测，说如果你们有比较成熟的白盒扫描工具是可以的，但是我没用过。反正这个问题纠结了很久。。。。

4、说一说内网横移的思路吧

我说分 Windows 和 Linux，Linux 比较难横移；Windows 就还是那一套

5、说一说除了 web 服务之外还有服务值得注意

这个问题问的挺。。。隐晦

其实就是问有哪些端口，我就说了那些

6、说一说你用 python 做过的一些项目吧

简单聊了聊

7、有做过白盒代码审计的一些项目吗

没有

8、如果你挖掘 Java 反序列化的 0day，你会怎么挖掘呢

就还是那样

下面是反问环节

主要问了问他们的业务、转正、一般上班强度如何、部门地位如何、食堂

就这些

0x5A 奇安信-观星实验室

一面

1、先做个自我介绍吧

2、我看你有复现过一些 Java 反序列化的漏洞，简单讲一讲漏洞原理吧。

easy

3、在这些反序列化的链子里面，有什么比较共通的地方吗

我说了链首、链尾、sink 要求

4、你有审计 Java 代码的经验，可以简单说一说吗?

说了一些思路

5、我看你 CTF 打的很多，其中应该有很多 PHP 吧，然后你挖的 PHP 洞也挖了几个，简单讲讲让你印象深刻的洞吧。

说了一个 SQL 注入，一个 phar

6、我看你复现过 fastjson 系列的洞，说一说最新的那个 fastjson 1.2.80 的洞吧，就浅蓝挖的那个

日了。。。我没很好的复现过

7、那你说一说 fastjson 的一些漏洞原理和绕过思路吧

我说了一些，但是有一条通杀的 jdbc 没有很好的分析过，后悔。

8、PHP 反序列化的漏洞挖掘思路可以说一下吗?

这个不会

9、jpress 我看你有审计的校验，有自己搞出来一些前台 RCE 吗

无

10、简单聊一聊 Java 内存马吧，原理以及如何写入

后面就是反问环节，问了一下他们的业务，然后大概组织架构，转正情况

二面

说实话二面没有准备好，因为一些特殊原因

1、做个自我介绍吧，主要讲一讲自己研究哪个方向。

2、PHP 审计过哪些大型的 CMS 呢

我说了 TP，还有一些其他的自己审计的

3、TP 里面不是有个命令执行吗？可以说一说里面大概后利用是怎么利用的，比如现在目标站开启了 disabled_function

我这里有点麻，本身 PHP 就不是很好，我说如果利用角度来说，蚁剑的插件就行，如果没有这个条件的话就手动写入 .so 文件

那你详细说一说怎么写进去..... 寄、我忘了具体利用手法

4、PHP 里面的 extract 变量覆盖这个问题，有在实际漏洞挖掘的时候遇到过吗

没有

5、面试官似乎还是很想问 PHP 的，问了 PHP 的另外一个问题，还是没怎么答出来。

又问了问 最近打的 CTF，主要是 ant 和 阿里云，让我讲讲印象深刻的题目，我都忘得差不多了。。

6、说一说 Java JDBC MySQL 反序列化这个漏洞吧

我说这只是给了一个入口，需要伪造 MySQL fake server

7、那你说一说怎么判断 MySQL jdbc 的版本吧

我说 wireshark 抓个包，内容应该会在里面

8、看你 Java CMS 审计过 jpress，当时是复现还是

我说了复现，然后让我聊一聊印象最深刻的一个洞

9、如果现在有个文件上传，但是只有 Web-INF 下的 .jsp 文件才会被渲染，你有什么思路

我说了 SSTI、crontab、sh、weblogic 的部署都可以

10、你有在大型攻防演练当中跟进过一些 VMware 类型的漏洞吗？展开聊聊

我说我只做过蓝队，然后 VMware 的话，最新的洞正在看。然后简单讲一讲，感觉面试官没有复现这个漏洞

11、听你说分析了 RocketMQ 的洞，简单聊聊吧

就简单聊了聊

12、那如果不出网呢?

。。。。我说这个单纯从这个漏洞的角度来说，其实是可以写入 crontab 的，但是实际打内存马，我还没有试过。

下面就是反问环节

0x5B 沥泉科技-红队安全研究

1、做个自我介绍吧

2、看你漏洞这块，Java，PHP，Python 都有了解是吗？简单说一说怎么审计 PHP 漏洞的吧。

说了用 Seay 扫一扫，然后对扫出来的重点去审计，黑白盒结合一起打

3、Seay 是很老的东西了，你有没有修改一下它的规则什么的

答：没有。。。寄

4、如果你没有修改过的话，那你怎么样才能挖出别人挖不出来的洞呢?

不会啊。。麻了

5、说一说了解的 Java 漏洞吧，像 fastjson、shiro 这些，就先说说 fastjson 吧，你对它了解多少。

这里我说了说 fastjson 最好用的两条链子，一条是 templatesImpl 的，另外一条是不出网的 BCEL。

6、简单说一说 fastjson 的 checkAutoType 吧

如果开启了就是先白名单过滤，再黑名单。

如果没开启就是会先黑名单，再白名单。

7、那关于 fastjson 的 parse 和 parseObject 呢?

parseObject：返回 fastjson.JSONObject 类

parse ： 返回我们的类 User

一般来说 parseObject 的利用面更广

8、有学过哪些框架和组件呢？为什么要学他们

就简单说了说，不过我的回答好像让那边挺满意的

9、关于 Shiro 的漏洞，有了解吗？展开说说

说了 550，721 和权限绕过

10、说一说 721 的 Oracle Padding Attack 的原理

寄，没背过

11、你用 Python 写过什么工具吗

说了说自己写了爬虫，然后写了个网段扫描的工具。

12、说到 nmap，一般 nmap 扫描很慢的时候会怎么办呢?

这里应该是用 msscan 比较好

13、有了解过内网么？说一说 Kerberos 协议的流程吧，后面又问了 NTLM 协议的流程

寄

14、除了 NTLM Hash，还知道哪些 Hash 呢

寄

15、src 自己有在挖嘛，简单说一说信息收集的一些方法吧。

寄，后门 l3m0n 师傅说有十多种方法。。。

16、话说 fastjson 需要碰到高版本的 jdk8 的时候要怎么绕过呢

这个其实就是 jndi 打高版本 jdk 的思路

17、Java 设计模式了解多少呢

18、打 CTF 是跟着战队拿奖还是自己校队拿奖

19、内网渗透的流程都了解吗

20、我大致了解你的情况了，可以说一说你的规划预期吗

接下来就是反问环节，主要是问了问他们到底是做什么业务的。

面我的是 l3m0n 师傅，很强

0x5C 二进制安全面经汇总

作者：爱看剧的四郎拥抱太阳

链接：https://www.nowcoder.com/discuss/473968551494156288

来源：牛客网

> 先介绍一下本人情况 985本，安全科班，上大学才开始接触的二进制安全，三月初开始准备春招，主投安全岗，辅投开发岗
>
> 主力语言C/C++/Python，接触过C#和java，涉猎比较广，各个领域都有过接触。安全能力上二进制接触比较多，web有过了解，主要经历在安全系统研发方面。
>
> 不得不说的是安全岗就业面确实比较窄，我原本以为自己很热爱安全，现在有一点点怀疑了
>
> 话不多说，上干货!
>
> （我个人总结面经比较喜欢按主题模块分类，不是很喜欢以公司来分类的，所以将各个公司面经都整合成一个了，遇到新问题就往里面加）

C/C++逆向开发

1. C/C++结构体大小如何计算?
2. C++的结构体和C的区别?
3. new和malloc的区别（delete和free的区别）
4. 如何找到main函数？（这里要继续细分，win32桌面程序，控制台程序，linux下的命令行程序）
5. 构造函数与析构函数调用时机
6. C/C++编程有没有遇到的安全问题（我讲的一个浅构造导致的double free）

7. 重载如何实现（静态函数名重载，动态虚函数重写）
8. **虚函数如何实现？**（重点，几乎必问，虚表指针位置）
9. 虚继承/多重继承的内存结构（VC和G++中虚继承中虚表结构不太一样，这里我研究过，扯了一大堆）
10. switch的实现与优化（难点）
11. try-catch的实现与优化（难点，会顺着问到windows异常处理机制）
12. 三种循环哪种效率最高？
13. 32位下调用约定有哪些？（stdcall c标准调用 fastcall thiscall）
14. 64位下调用约定？（VC：rdx rcx r8 r9，GCC: 多rdi rsi）

二进制逆向（反调试/脱壳/免杀/挂钩/注入）

这部分为安全岗面试重点

1. 32位程序如何在64位机器上运行？
2. **PE格式（重点，几乎必问）**
3. **PE装载进内存执行的过程（重点，内存对齐，IAT表建立，重定位）**
4. 知道哪些反调试手段？（SEH，反断点，查调试环境）
5. gdb/od基本命令
6. 调试器原理（三大断点实现）
7. 如何脱壳（压缩壳/加密壳/虚拟化壳）
8. 为什么脱完壳要修复导入表？
9. 花指令有没有脱过？
10. **有没有写过IDA脚本（逆向岗位几乎必问）**
11. 如果一个程序没有字符串/字符串被混淆了如何找核心代码？
12. 内存泄漏如何排除
13. 有没有做过免杀，怎么做的？（静态二分法定位，思考对面规则怎么写的，动态绕钩子检查，卸钩子，提权走底层）
14. 沙箱有接触过吗？（并没有...）
15. 有没有用过虚拟机？（QEMU, VMware Bochs）虚拟化有哪几种方式实现？虚拟机查杀有什么思路过吗？
16. **Hook有哪些方法？（几乎必问，inline hook，函数表hook）**
17. 如果inline hook前几个字节不能正好5字节Patch如何处理？
18. 分析过哪些病毒样本？病毒分析有什么方法？（问到了深信服的实习）
19. 特征码怎么提取的？
20. .NET的实现（因为项目研究过.NET）
21. flags寄存器有哪些位，有什么作用（OF, ZF, TF, 虚拟位）
22. 控制寄存器有哪些，有什么作用（可以重点说说CR0和CR3）
23. 共享内存怎么实现
24. **windows下有哪些注入方式？怎么实现？（重点）**
25. windows下3环向0环的切换过程？
26. ARM汇编了解过吗（没有...）
27. 如何防止内存被扫描？
28. 如何隐藏进程？（说了一个CPU控制区找EPROCESS断链）隐藏之后对进程运行有影响吗？

漏洞利用

楼主pwn菜鸡，web不是很熟悉，说得都是比较基础，不过其实对漏洞利用很熟悉的面试官也不是特别多。

1. windows/linux基本保护机制（栈执行保护，基址随机化，代码段随机化，栈溢出保护）
2. 怎么绕过？

3. pwn的一些印象深刻的题目，或是技巧（这部分如果面试官不是相关领域的建议不要说太深入，太细节的技术很复杂，很难讲懂）
4. 堆漏洞利用？（double free, UAF）
5. 栈上漏洞利用有哪些
6. linux堆管理，glibc/slab/伙伴算法
7. 脏牛
8. web漏洞有了解吗？
9. SQL注入、XSS攻击原理？
10. ARP欺骗怎么实现的？
11. 如何判断远端服务器的操作系统？

项目相关

1. Powershell防御项目讲一下？
2. 怎么防止无文件攻击？
3. 分析过哪些脚本病毒？
4. 加密混淆怎么处理？
5. 知道哪些加密算法，非对称加密与对称加密的区别？
6. .NET钩子怎么下的？
7. 做过流量检测？说说怎么提的特征？
8. 顺便问到TCP连接建立与释放（典中典）
9. 问到毕业设计，简述一下你的静态分析算法怎么设计的
10. 开发过Linux键盘监控？怎么实现的？
11. windows调试器怎么实现的？（3环API...）
12. 写过端口扫描工具，怎么实现的？（netfilter框架编程）
13. ARP Poison怎么写的？（原始套接字，linux上好写一些）
14. 写过区块链的项目，说一下？（写的Spring + Solidity，但是接触不深，不是很回答上来）

> 备注：从0x5D~0x69均来自于**春告鳥**师傅
>
> 链接：https://www.cnblogs.com/Cl0ud/p/16235033.html

0x5D 忆享科技面试 北京渗透岗

一面

1. 自我介绍
2. CNVD是挖掘的通杀漏洞还是事件型漏洞
3. CNVD通杀漏洞一般是怎么挖掘的，挖掘的哪些类型的漏洞
4. EDUSRC比较有意思的漏洞挖掘过程
5. 暑假实习期间主要做的事情
6. 大二HW蓝队期间的设备是哪家的
7. 如何区分告警信息为误报还是真实攻击
8. CSRF和SSRF的简介和区别
9. SSRF绕过
10. XSS绕过
11. SQL注入绕过
12. 文件上传绕过
13. 00截断的原理

14. 内网渗透
15. 自己安全开发一般用什么语言
16. python爬虫问题：为什么有的时候浏览器能够正常访问的页面，在爬虫中访问不了
17. python多线程输出应该怎么操作
18. SQL注入写shell需要什么条件
19. java反序列化
20. weblogic tomcat漏洞
21. 反问环节

0x5E 悬镜安全 成都安全开发

一面

1. 自我介绍
2. 因为看到你有做扫描器的经验，简单介绍一下吧（这一部分扯了很长时间）
3. 说一下信息搜集这部分是怎么做的（因为很多地方都是爬虫爬取信息，以前爬虫用过正则，xpath和beautifulsoup，简单说了一下xpath，信息搜集先简单说了一下信息搜集的内容，然后主要讲的就是子域名搜集的思路）
4. 扫描器是怎么检测注入的
5. 扫描器是怎么检测XSS漏洞的
6. 有看你做红蓝队的经历，说一下有意思的挖漏洞的经历
7. 看到有教育行业HW的经历，讲一下当时做红队的经历
8. 看到有在HW蓝队的经历，讲一下经历（讲了一下实习的经历+蓝队的经历，以及挖掘到的一些漏洞）
9. 面试官可能觉得问的差不多了，就说那我再问几个简单的问题吧~~（我说：感觉要变难了hhh）
10. SSRF漏洞简介 利用 和防御
11. 问了一下内网相关的问题
12. 一句话木马免杀绕过相关问题，简单讲了一下绕D盾和安全狗，这两个比较死，很容易过
13. 然后换了个面试官，应该是部门主管？（因为我前面面试的过程中提到了我来之前查了一下悬镜安全是做IAST 灰盒扫描这一块的，然后觉得这对我自己来说也会是一个挑战）这里部门主管跟我介绍了一下我来之后成都分部这边要做的事情，也介绍了一下灰盒扫描和准备做后渗透方面的内容
14. END

下午2:30面的，晚上通知一面过了，下周一线下二面

二面

（写的时候距离时间有点久，有些问题记不清了

1. 简单交流了一下
2. 自我介绍
3. 扫描器的漏洞检测部分
4. AWD攻防平台的介绍
5. SQL注入的检测
6. 一些通用漏洞的检测的经历
7. fofa被禁用了之后用什么（上一个问题通用检测里面聊到基本的检测脚本写好之后可以用fofa进行批量的导出，又说到前两天fofa因为合规问题被拉入工信部黑名单的事情 。回答钟馗之眼，撒旦，谷歌语法。）
8. 红蓝队的经历

9. 为什么说python的多线程是伪多线程（这里我简单说了一下因为即便存在多个CPU，在python程序中也只会有一个线程同时被执行，其原因是存在GIL 全局解释性锁）
10. 为什么不将这个伪多线程问题修改掉（其实这里我感觉有点答偏了，从python底层的垃圾回收机制说的，因为python主要使用引用计数来进行垃圾回收，即创建对象里面的ref，当引用销毁的时候ref-1，ref=0时内存释放，如果是真正的多线程的话，很可能会出现ref为负数的情况，造成程序的崩溃和出错）
11. 对悬镜安全的了解（这里我属于有备而来了，面试之前谷歌了一下公司的相关信息）
12. 什么时候能来公司实习（其实之前跟HR沟通的时候，HR说的是校招，毕业之后去，这时候部门leader说可以年后可以先来实习，也就是大四下）
13. 问了一下我的毕业设计相关问题
14. 有面其他公司或者其他offer吗?
15. 反问:
    - 公司规模（因为感觉成都分部这边人比较少）
    - 大家平时在哪里吃饭（中午很早就被我妈赶出门去面试了，所以在面试地点下面溜达了很久，感觉周围没啥吃的）
    - 公司的扫描器是自研的还是基于pocsuite的或其他扫描器的
    - ...

回去的路上HR通知二面过了，第二天晚上8点三面

三面 公司CEO

1. 自我介绍
2. 了解悬镜安全吗
3. 讲一讲灰盒扫描吧
4. 说一下动态污点追踪
5. 了解RASP吗（这个我确实不了解 悬镜自研:云鲨RASP-自适应威胁免疫平台）
6. 多久能入职？可以先来实习
7. 反问:
    - 公司对新人会有培训吗
    - 为什么终面会是CEO而不是HR
    - ...

0x5F 中安网星面试 红队攻防开发

一面 上午11:00

1. 自我介绍
2. 看到有写扫描器的经历，说一下扫描器的搭载POC的部分
3. 说一下SQL注入的检测
4. 说一下时间盲注的时候如何判断的
5. 说一下布尔注入的检测
6. 说一下页面相似度算法
7. 为什么不把sqlmap这种工具内置到扫描器里面

8. 自己的职业规划是什么？想做哪方面的
9. SSRF漏洞简介
10. 给一个场景，一般怎么用SSRF打内网
11. SSRF的绕过的一些问题
12. 审计过一些CMS吗
13. 说一下是怎么审计的
14. PHP的反序列化了解过吗
15. 说一下PHP的魔术方法
16. 反问环节
    - 公司主要做的是内网渗透这方面吗
    - 如果有机会来公司的话我会做哪方面的内容
    - 公司的规模

效率很快，马上就约了下午面试

二面 下午2:30

公司CTO

1. 说一下你平时遇到的SQL注入的防御手段
2. 如果你做一个防御的话会怎么做
3. 如果在用户输入的SQL语句在沙盒里面运行，应该怎么放置在系统里面
4. 有过SQL注入攻击的经历吗
5. like后的注入应该怎么注入
6. 说一下SQL注入写shell
7. phpmyadmin怎么getshell
8. XXE了解过吗？回答在现实中没有遇到，一般在CTF里面看到
9. SSRF了解过吗？简单说一下SSRF
10. 你觉得写扫描器以及POC对自己有什么意义或者价值
11. 拿到一个shell之后你会怎么提权
12. XSS漏洞了解过吗？有哪些利用方式
13. 还有几个我忘记了
14. 反问环节
    - 公司今年大概会招多少人
    - ...

HR

HR打电话过来聊了一下薪资，简单说了一下公司的各方面福利，约了第二天中午三面

三面

1. 自我介绍
2. 内网渗透中的Kerberos协议

3. MySQL,redis，oracle端口
4. 知道某个网站的CMS时有什么用
5. SSRF的防御
6. java的反序列化
7. 反问环节
    - 为什么会出来创业
    - 如果有机会来公司的话我会做哪方面的内容

0x60 重庆绿盟面试 红队攻防开发

一面

1. 你想做的方向
2. 说一下你平时是怎么进行代码审计的
3. 看到你有审计过thinkphp，说一下tp3缓存漏洞里面的木马名称是怎么来的
4. php的危险函数
5. phpinfo你会关注的信息
6. 本地文件包含漏洞如何拿到shell +
7. 本地文件包含时你会比较关注哪些敏感信息
8. 说一下最近比较火的漏洞
9. 说一下php里面的常用的伪协议 +
10. 说一下XXE +
11. 扫描器你是做的哪一部分
12. 简单介绍一下扫描器（说到这个我就不困了
13. 现在是没有维护还是在重构
14. 扫描器是主动扫描还是被动扫描
15. 说一下通用漏洞的检测，SQL注入
16. 说一下布尔注入的检测
17. 说一下simhash算法 +
18. 说一下时间盲注的检测
19. 看过sqlmap这方面的源码吗
20. 扫描器的检测引擎是怎么写的
21. 说一下页面URL的爬取
22. 反问
    - 重庆绿盟的规模和人数
    - 安全开发部门使用的语言

有的问题忘记了，将就看

二面

在约定的时间前一晚提前面试了

1. 职业规划
2. base城市
3. 面试官介绍了一下部门和安全开发相关的内容
4. 薪资方面的内容
5. 反问

三面

1. 在前面的面试里面了解过这个岗位是做啥的吗
2. 是怎么了解到绿盟以及怎么投的简历
3. 内推你的朋友做的是什么岗位
4. 平时都挖些什么漏洞
5. 介绍一下你的扫描器
6. 可以检测log4j2漏洞吗
7. 说一下指纹识别以及指纹库
8. 看你写过爬虫，说一下这方面的
9. 反问

0x61 北京微步在线 安全开发

一面

1. 面试官先对自己和部门进行了介绍
2. 自我介绍
3. 你觉得一个好的扫描器应该具备哪些功能
4. 出于什么样的原因去写扫描器
5. 说一下360的POC收集计划
6. 说一下你平时是怎么批量利用漏洞的
7. 一个好的POC应该具备哪些特征
8. 扫描器是自己封装的核心吗，还是封装的pocsuite3
9. 对于基于pocsuite3和yaml文件的poc的看法，你觉得哪种更好
10. 用过Docker吗，是在什么场景下进行
11. 用过vulhub吗
12. 说一下对于无回显漏洞怎么检测
13. 说一下对于不出网漏洞怎么检测
14. 多久能来实习
15. 是想来单纯实习还是想转正的那种，转正那种需要转正答辩
16. 还有什么问题吗
    - 公司安全部门的规模
    - 安全研发这方面用的语言
    - 我来主要做的工作

- ...

二面 第二天晚七点

应该是部门主管，面试之前说翻了一遍我的博客

1. 说一下你觉得自己的三个比较擅长的点（回答：安全开发，渗透测试，代码审计）
2. 说一下你觉得印象比较深刻的挖掘漏洞的过程
3. 说一下你看到的或者自己挖到的某一个漏洞
4. 分析一下这个漏洞是怎么被挖到的，或者说需要什么样的技术才能挖到
5. 算法相关
6. 说一下你的职业规划
7. 你对你要做的岗位的了解
8. 简单介绍了一下微步

三面 HR面 紧接着 二面之后

1. 你在大学里面觉得某件很困难但是最后克服了的事情
2. 你在其中扮演的是什么角色
3. 你觉得还有哪些事情是可以去完善的
4. 你是从哪几个维度去思考和复盘的
5. 说一下你在大学里面印象比较深刻，或者自己比较自豪的事情
6. 自己在这个事情中主要充当的是什么角色
7. 你是怎么去提升你们的沟通效率的
8. 大学里面除了学校的课程以外还有什么兴趣爱好吗
9. 吉他练的怎么样
10. 有什么事情是你一直坚持到现在的（写博客）
11. 你觉得写博客给你带来了什么意义
12. 之前有过实习经历吗
13. 考研考的是哪个学校
14. 哪一科没有考好
15. 你觉得为什么没考好
16. 你会选择调剂吗？为什么不想调剂
17. 没有考上会有遗憾吗
18. 会选择二战吗
19. 是怎么了解到微步在线的
20. 平时花在网络安全上面的时间是多少
21. 你的期望薪资是多少？（回答：我说了也不算啊，得看公司给我多少）（回：确实哈哈哈）
22. 现在手里有offer了吗，哪几家公司的，薪资大概是多少，签了三方了吗
23. 想要在哪里工作
24. 对于第一份工作你的期望是什么
25. 多久能来实习
26. 还有什么其他的问题吗

0x61 成都卫士通 物联网安全研究

一面 晚上电话面试

1. 说一下你参加过的比赛
2. 这些比赛都是团队比赛吗
3. 你在其中做的是什么角色
4. 说一下HW蓝队的时候做的事情
5. 应急响应相关的问题
6. 实习的时候做过什么事情
7. 实习的时候挖过哪些漏洞
8. 说一下在EDUSRC上挖漏洞的事情
9. 平时挖漏洞哪种比较多
10. 是手动挖掘还是自动扫描
11. 说一下代码审计，你平时是怎么代码审计的
12. 说一下中间件漏洞
13. 了解过逆向吗?
14. 逆向的工具用过哪些
15. 工控安全了解过吗，简单说一下
16. 物联网安全的漏洞类型有哪些
17. 记录过自己打过哪些CTF比赛吗
18. 说一下你们学校的安全实验室
19. 你来公司的话是想做CTF还是做渗透
20. 多久能来公司
21. 家在成都哪里

面试官说他家比我家还远，平时都是开车上班orz

- 反问:
    - 卫士通和中国网安的关系
    - 关于木星安全实验室
    - 关于事业编制
    - 后续还有其他面试吗
    - 卫士通的架构和安全部门的规模
    - 来之后我会做的事情
    - ...

0x61 成都数默科技(科来) APT研究

一面

1. 自我介绍
2. 面试之前了解过数默科技吗
3. 大学里面学过哪些课程，你比较喜欢哪个课程，为什么
4. CTF比赛的时候一般都做哪方面
5. 有没有印象比较深刻的漏洞挖掘的经历
6. SQL注入如何GETSHELL
7. 说一下AWD攻防竞赛平台的架构，用到的技术
8. 说一下扫描器的流程
9. 说一下asp文件上传绕过

10. 说一下解析漏洞
11. 说一下反序列化漏洞
12. 平时用过哪些安全工具
13. 流量分析做过吗
14. 毕业设计题目是什么
15. python代码里面会有哪些漏洞
16. 介绍部门和做的事情
17. 你来了之后会做的事情
18. 你的期望薪资是多少
19. 了解过APT吗
20. 反问
    - 部门的规模
    - 后续的面试流程
    - ...

二面 HR面

- 谈薪资
- 介绍部门

0x62 传音控股上海 安全开发

一面

微信视频面试，HR拉了个群，HR+两个面试官同时，整体时长40分钟

1. 自我介绍
2. 说一下扫描器的流程
3. 说一下渗透测试的流程
4. 刚才提到了SQL注入，说一下为什么会产生SQL注入，以及如何防御
5. SQL注入如何GETSHELL
6. 你有过代码审计的经验吗，平时是怎么审计代码的
7. 说一下OWASP TOP 10
8. 说一下XXE和SSRF的区别
9. SSRF和XXE怎么防御
10. 说一下nmap原理
11. 说一下TCP三次握手
12. DOS和DDOS是什么
13. 说一下你做过红蓝队的经历
14. 看到你有写POC的经历，简单说一下（这里简单说了一下log4j2的检测POC流程）
15. 平时做过APP的渗透吗
16. 你所期望的工作是什么样子的

17. 你工作期望base哪里
18. 是因为考研失利还是因为拿了几个offer，才考虑来传音的
19. 你觉得自己相对于同龄人的优势在哪里
20. 你觉得自己的缺点在哪里
21. 老家哪里的
22. 反问
    - 传音控股安全部门的规模
    - 安全部门开发主要使用的语言
    - 如果我来了主要会做哪方面的工作

还有几个技术问题忘记了，总体来说不是很难，最后的时候我和两个技术面试官都笑了orz

HR电话联系

薪资没谈拢，寄了

0x63 绿盟成都-安全服务国际部 安全服务

一面

一到月底学校的网卡的要命，视频面试差不多五分钟断一次orz

1. 自我介绍
2. 说一下你做过的项目
3. 介绍一下扫描器的流程
4. 通用漏洞实现了哪些的检测
5. 简单介绍一下WEB渗透的流程
6. 扫描的过程如果遇到了防火墙是怎么处理的，是有绕过吗
7. 说一下红队的经历，挖过哪些漏洞
8. 看到你之前有实习的经历，说一下这部分
9. 说一下蓝队的经历，做的哪些事情
10. 如果是你的话，怎么检测是否有攻击者进入网络进行危险操作
11. linux用的怎么样，说一下权限相关的
12. chmod +s 是什么
13. 了解过正向代理和反向代理吗
14. 说一下Nginx
15. 说一下其他你了解的OWASP TOP 10
16. 说一下CSRF
17. redis未授权有哪些利用方式
18. 为什么大三的时候没去实习？考研考的哪个专业？哪个学校？哪个科目没考好
19. 对于安全服务的理解
20. 如果有机会来的话主要想做哪些方面
21. 英语怎么样
22. 如果要到国外去短期出差你父母会怎么看？（答：他们会觉得公费旅游）
23. 最后介绍了一下部门的职能，服务的对象等等

0x64 成都360 安全研究

一面

1. 自我介绍
2. 看到你有打CTF的经历，说一下你印象比较深刻的比赛
3. SQL注入的绕过会吗，过滤了逗号怎么绕过
4. 说一下你的扫描器
5. 项目的并发是怎么处理的
6. 看到你有写flask，说一下flask可能存在的漏洞吧
7. 那就再说一下flask是怎么防御这些漏洞吧
8. 说一下POC检测相关的
9. 代码审计做过吗，你平时是怎么进行代码审计的
10. 看到你有用过codeql，说一下它是怎么进行漏洞检测的
11. 用codeql进行过实战漏洞挖掘吗，怎么挖的
12. 说一下java代码审计里面你印象比较深刻的漏洞
13. 看到你有审计过TP，说一下它的安全处理
14. 说一下TP3的I方法
15. 说一下XXE漏洞
16. 多久能来实习
17. 反问:
    - 团队规模
    - 平时做的事情
    - ...

二面

1. 自我介绍
2. 说一下AWD攻防竞赛平台里面你印象比较深刻的点
3. 参赛选手页面的刷新是用的AJAX还是后端定时推送
4. Docker有没有限制目录权限
5. DockerFile的编写有没有什么心得
6. Docker逃逸的问题
7. 刚才说到了没有使用目录挂载，那flag的刷新是怎么实现的
8. 多个Docker的调度问题
    - 我说了一下`docker-compose`,以及其中的一些细节，比如`depend_on`
9. 看到你有写POC，说一下写POC的心得
10. dnslog的原理了解过吗
    - 我简单说了一下
    - 面试官补充加解释
11. 有想过写调用dnslog的单独方法吗
12. 你的职业规划是什么
    - 反问:安全研究一般后来都去做了什么

13. nmap的原理知道吗
    - 我说了一下nmap的默认扫描，nmap的扫描周期以及扫描器里面合并nmap的方案
14. nmap扫描速度的优化方案
15. 成都360车联网那边是做什么的
16. 多久能来实习
17. 毕业设计做的咋样了
18. 最近在做啥
19. 想去车联网安全那边还是我们这边
20. 以后是想在成都发展吗
21. 反问
    - 部门要招多少人
    - 为什么360没有HR来管理招聘流程
    - 面试之后多久会有结果
    - ...

0x65 成都360 车联网安全

一面

1. 自我介绍
2. 你知道过来是做哪方面吗
3. 说一下项目经历
4. 说一下插件系统的实现
5. 问一下学校的课程，说一下你理解的进程吧
6. 多线程和多进程用过吗
7. C,Java这些用过吗，学习的程度咋样
8. 你的职业规划是啥
9. 了解过二进制漏洞吗
10. 说一下缓冲区溢出漏洞
11. 对于车联网安全的了解
12. 介绍了一下部门
13. 多久能来实习
14. 反问
    - 研发部门用的语言
    - 后续如果还有面试的话，面试流程是什么样的
    - ...

二面

接到电话的时候在`无届`吃饭，整个环境很嘈杂，orz

- 了解车联网安全吗
- 了解IOT漏洞吗，有哪些

- 看到你是计算机专业，有做过单片机小车吗
- 路由器破解做过吗
- 认识 腹黑 吗 (orz)
- Linux了解吗，说一下Linux的启动流程
- grub命令了解过吗
- 说一下linux如何分析二进制文件
- docker了解吗，说一下USB应该怎么链接上docker
- 加密算法了解吗，说一下MD5 RSA AES的区别
- http和https的区别
- CA证书的作用
- 你理解的固件是什么
- 介绍了一下部门
- 反问
    - 部门规模
    - 有无车联网安全体系学习资料

HR面

- 自我介绍
- 多久能来实习
- 拿了哪些offer
- 想做安全开发还是安全研究
- 以后在成都发展吗
- 谈了一下360的薪资
- 反问
    - 我能过不
    - 啥时候发offer
    - 部门一共招多少个人
    - ...

三面

- 想做安全开发还是安全研究
- 啥时候能来实习
- 面试官说了一下自己对于车联网安全,安全开发,安全研究的看法
- 聊个人规划

0x66 杭州极氪科技 安全研发

一面

1. AWD攻防竞赛平台中做的事情
2. 漏洞靶机是怎么实现的
3. flag刷新是怎么实现的
4. 如何检测一个服务是否宕机
5. Docker的逃逸考虑过吗
6. 为什么会想到去做扫描器
7. python里面会存在哪些安全问题
8. 插件是动态加载的吗？怎么加载的
9. 考虑过有人上传恶意插件的问题吗
10. 端口扫描是怎么做的
11. nmap扫描的时间比较长，你对它进行了优化吗
12. 打过CTF吗，在里面主要做哪方面的工作
13. 了解车联网安全吗
14. 了解过极氪科技吗
15. 介绍部门
16. 反问
    - 实习的一些问题
    - 现在有哪些公司在做车联网安全
    - 车联网安全的前景
    - 我来了之后主要会做哪方面
    - ...

HR

五分钟之后就通过了，效率很高，HR打电话过来谈薪资

- 谈薪资
- 问福利
- 问实习
- 问其他问题

0x67 成都四叶草安全 安全研发

一面 电话面试

- 现在在学校吗
- 为什么大三的时候没有去实习
- 你对于工作环境，工作氛围这些的要求是什么
- 多久能来公司
- 简单介绍了一下公司部门
- 简单介绍一下扫描器
- 扫描器里面存在误报的情况，你会怎么优化
- 期望薪资
- 你还有什么问我的

二面

- 自我介绍
- 现在在学校做啥
- 漏洞挖掘的问题
- 白盒一般挖掘哪些漏洞
- 黑盒渗透的问题
- 拿到一个shell执行不了命令可能是什么情况
- 权限比较低如何提权
- 拿到shell后如何链接远程桌面
- 写代码的时候会遇到并发比较大的情况，一般你是怎么处理的
- 你对自己的职业规划是什么
    - 反问 你的岗位是什么
- 自己平时有空的时候会做什么
    - 反问 你打游戏吗
- 期望薪资
- 还有什么问我的吗

三面

- 说一下你对漏洞扫描的理解
- 说一下端口扫描的理解
- 说一下数据库索引的底层实现,数据结构
- 了解GO语言吗，说一下相关的
- 说一下TCP四次挥手

HR面

- 对于公司的了解
- 之前的面试问了哪些问题
- 以后会在成都发展吗
- 为什么会选择四叶草安全
- 期望薪资
- 现在拿到了哪些offer,以及对应的薪资
- 为什么没有还没有做最终的决定
- 多久能来实习
- 毕业设计的内容是什么
    - 反问:现在HR也要问技术了吗
- 为什么大学在重庆读的最后想来成都发展
- 你对于公司、团队有什么期望
- 有什么问我的吗
    - 成都安全团队的规模
    - 后续的面试流程

- ...

0x68 成都民生银行

一面

群面 这里我就只记录自己相关的问题了

1. 自我介绍
2. 自己做的项目里面印象比较深刻的点
3. 说一下SQL注入以及检测
4. 你比较熟悉WEB的哪些漏洞，以及他们相应的防御手段
5. 用过多线程吗，有哪些库
6. 了解过前段时间比较火的log4j2漏洞吗，它属于哪种类型的漏洞，讲一下它的原理
7. 你有复现过log4j2吗，说一下过程
8. 如何在一个长度为100的数组里面找到第二大的数
9. LRU算法
10. 还有一些问题忘记了....都没啥难度

0x69 亚信安全 安全分析

一面

1. 自我介绍
2. sqlmap的检测实现
3. SQL注入怎么手工检测
4. 什么是时间注入，你是怎么检测的
5. XSS和CSRF的相同点和不同点
6. 文件上传漏洞应该如何防护
7. 说一下文件包含漏洞以及相关的敏感函数
8. 你经常挖到的漏洞是哪些类型的
9. 自己觉得比较精彩的挖掘漏洞的经历
10. sqlmap里面对于防火墙过滤有哪些操作
11. 如果是你自己实现怎么应对防火墙
12. 说一下一句话木马的发展以及流量加密
13. http和https的区别，https为什么更安全
14. 内网渗透会吗，CS的相关操作
15. 如果你自己要防护服务器，在不用防火墙和态势感知系统等情况下你会怎么做
16. 写漏洞检测POC时你会去看漏洞原理吗
17. 扫描器里面分了哪些模块
18. 信息收集是自动化的还是有指纹库
19. 扫描器实现里面比较自豪的部分
20. 挖矿木马有研究过吗
21. 有无应急响应的相关经验

22. 期望薪资是多少
23. 多久能来公司
24. 反问
    - 成都亚信安全的规模
    - 这个岗位主要做的跟我想的是一样的吗
    - ...

> 备注：从0x6A~0x6D均来自于4o4notfound师傅
>
> 链接：https://4o4notfound.org/index.php/archives/183/

0x6A 头条

一面

和hr约的是下午两点半，结果我听成两点了，然后到了两点钟面试官还没上线可把我急坏了，联系了hr发现是自己蠢了（尴尬）。还好面试官人很随和，我原本紧张的心淡定下来了。首先开始自我介绍，blabla，然后面试官说看我简历上有多个项目，就让我自己来介绍一下项目，我先大致介绍了一下第一个实验室的项目，描述了项目的出发点和着眼点blabla，着重讲了一下我承担的task，然后面试官开始追问，我分别从场景、数据、特征工程、算法、评估分析反馈等角度说了一通，在xx场景下，选了xx数据，我为什么选这些数据？怎么获取这些数据？blabla先声夺人。数据部分是最重要的，需要多说一点，然后到了特征工程部分，我讲了一些常用的技术，手工提取啊，NLP啊，深度学习啊之类的，然后在此场景下我选了哪种，为什么选出了这种（当然是比较了已有技术手段），算法部分我主要说了树类型的算法，为什么我喜欢树类型算法，可能是因为安全领域本来就小众，其下的安全算法、安全数据分析更小众了，而面试官都是安全出身，对算法细节并不care，一些面机器学习岗必问的算法知识都没有问，都是根据安全业务来问。最后的评估分析反馈性能优化方面，我说了一些常见的技术，和传统waf对比啊，无痕人工审核啊，数据再分析，再做特征工程不断迭代，重训练之类的方法。基本上所有安全数据分析的项目都可以按这套流程来解释。穿插着问了我接触安全多久啦，啥时候开始学习智能安全，我说我最早是做web安全的，读研以后走了安全数据分析的路子，没有继续往安全研究上发展，主动认怂说我web安全方面有点生疏了，但是基础安全技术还是掌握的，能跟上师傅们的节奏（没想到给二面挖了坑）。之后问了第二个项目，第二个是我个人github关于智能安全的项目，我从头条的人工智能用于内容分发出发，从四个方面说了我对智能安全的理解，着重讲了人工智能用于解决安全问题部分。面试官拓展问了四部分之一的AI用于攻击的部分，我说了深度强化学习和msf结合进行自动化渗透测试的例子，面试官追问了深度强化学习，我解释了一通貌似没有讲清楚。我觉得之前给面试官留下的印象是我web安全技术生疏了，所以当面试官问我有什么要问他的时候，我抛出了我的问题：如何权衡传统安全技术深度研究和智能安全（安全数据分析）？您觉得智能安全未来会怎样？然后面试官说了很多话，让我茅塞顿开，在智能安全这方面我和面试官的看法很相似，聊到了一起。

二面

二面的面试官好像是做安全技术的，首先介绍项目blabla，介绍完了.....然后说一面面试官的评价说你web安全技术有点生疏了，那我们来问问web安全技术吧，

1. 乌云/src上提交过的都是啥类型的漏洞?
2. PHP审计你都咋审计的?
3. 有没有自己总结的一些经验?
4. 变量覆盖产生原因有哪些?

5. 最近有没有跟过漏洞?
6. SQL注入咋产生的?
7. 如何绕过过滤了空格的注入?
8. 如果过滤了逗号怎么绕过?
9. 宽字节注入咋产生的?
10. MySQL中如何设置字符集编码?
11. XSS怎么防护?
12. 讲讲你挖过的0day。

大部分都答了上来，小部分记忆模糊了，就根据记忆尽量答了。然后聊智能安全，讲讲SVM，二面面试官说他也做机器学习几年了，但不太看好利用机器学习等技术来解决安全问题。面试官觉得应用场景很有限，无非做做waf，性能也有限，不适用于生产环境。我承认了这些问题是目前遇到比较棘手的问题，也给出了一些缓解的措施，比如针对尚未用机器学习解决过的场景，要勇于解决问题，不能怕，不能觉得没人解决过就是解决不了的，举了业务安全中的设备识别的例子，再抽象安全场景，定制化用机器学习解决安全问题。最后说了我还是相信智能安全未来会占有一席之地，如果现在我们不提前占坑，那么以后就被甩在后面了。

三面

三面面试官人很nice，一直笑嘻嘻让我没一点压力，按照套路自我介绍，然后问项目问项目，基本上都是我一个人在blabla，面试官偶尔会根据我的回答打断一下追问问题，卧槽我咋想不起来面试官问了哪些问题了，好像面试官并没有问具体的问题，大多都是我们在讨论，印象深刻的问题是面试官抛出了一个具体的业务场景让我给解决方案，我借鉴了一些以往的经验然后分析抽象了问题，然后blabla，先做个baseline，再不断优化等等。然后开始聊弱智能安全，三面的面试官和一面面试官一样都看好智能安全，对一些新颖的技术比较感兴趣，比如前面提到过得智能攻击技术。还问了有没有了解过其他公司的智能安全研究现状和技术，我举了百度和阿里的例子，讲了下他们的产品和技术，对标了一下，重点讲了我做的和他们类似的demo，说我个人做的还比较菜，和企业级比不了。再然后面试官说来写个代码吧，问我熟悉啥语言，C++？Java？我说都不怎么会，我写python多一些，面试官说没关系写伪代码也行，然后出了个编程题reverse，说在聊天框写代码就行。我想了一下写了代码，面试官评价了一下，然后问我咋测试你写的代码健壮性，我说测试样例要多样化极端化blabla。最后问面试官问题的时候我问了如果入职所在部门的工作内容以及我的一些职业发展规划和他的看法。

hr面

和hr约了晚上七点的电面，六点半到了操场等hr的电话，有点小紧张。起手自我介绍（紧张，不知道是操场冷还是真紧张），hr问为啥考研？考研成绩？家在哪儿对工作地点有没有要求？导师让不让实习？实习时间？职业规划怎么打算的？每个实习生都有mentor，你希望从你的mentor学到哪些东西？怎么评价之前面你的三个面试官？有没有投其他公司？考虑了哪几家公司？为什么考虑这几家公司？拿到了哪些offer？我blabla举例子，对标说了阿里，然后hr问我我给我的面试打多少分？我说85+吧，然后说了为啥85，哪些地方不足还可以改进。全程语速比较快略显紧张，最后问hr问题的时候，我问了您觉得我今天表现的怎么样？以及我有哪些可以改进的地方？hr说觉得我今天有点紧张，我说是的，第一次网申面试，以后会好很多的。hr问我电话号码是不是微信，我说是，然后加了我的微信，说2-3个工作日有消息会通知我。第三个工作日后，收到了hr小姐姐的口头offer，谈了一下入职时间，之后收到了邮件offer。

0x6B 腾讯-云鼎实验室

云鼎一面

哇啊啊一面面试官是rr，一面主要考察安全技术，

1. 乌云的洞都是啥？
2. 有没有跟过最近的洞？
3. ThinkPHP的最近的RCE跟过吗？
4. 审计做的都是啥？
5. 基本的漏洞类型？
6. 常用的语言？
7. SSRF漏洞中绕过IP限制的方法（需要补习）？
8. 主机入侵检测中怎么用机器学习解决问题？
9. python web开发？
10. django的secret key的洞跟过吗？
11. 了解二进制安全吗？

总的来说，rr的安全研究深度很深（rrtql）。

云鼎二面

二面面试官主要是做数据分析的吧。自我介绍，然后开始问大数据框架，

1. ELK都是啥？
2. Spark？
3. 你是咋做DGA域名检测的？
4. 特征咋提取的？
5. GBDT和XGBoost的区别？
6. Kaggle上你的恶意软件那个项目？
7. 阿里云恶意软件多分类项目？
8. Java会吗？
9. R语言懂吗？
10. python web开发咋样？
11. kafka知道吗？
12. 怎么实现关联进程和网络传输

    （这个没回答上来，得好好捋一捋，wget http://www.xxx.com?这种吗？是不是主机入侵检测混合网络入侵检测）？
13. 多个数据源怎么关联？
14. 如果给你文件信息、进程信息、端口信息等等你能用机器学习解决哪些安全问题？
15. 介绍下你简历中的项目一。

最后我问面试官所在部门的主要工作内容以及如果我入职的话我的主要工作内容。云鼎实验室的工作内容之一是用机器学习技术和大数据技术做安全监控，比较符合我的预期。最后问了面试官接下来的流程，面试官说和同事商量一下可能还有1-2轮面试。

云鼎三面

就在刚刚又面完了，感觉面试官是个中年和蔼大叔（上来先介绍了面试官自己，按照套路不是应该我做自我介绍嘛）。总的来说面试官都是根据我简历来问，问了前乌云的漏洞是什么情况？通用型漏洞是什么情况？项目一的情况？我blabla介绍，从问题的着眼点、数据、特征、结果解释了一通，面试官追问了两个问题。然后问了阿里云恶意软件算法挑战赛和Kaggle上的恶意软件预测相关的一系列问题，主要关注点在：数据、特征、算法。又问了SVM和线性回归的区别，讨论了一波SVM的线性不可分情况，核啊，升维啊这些。问的都是做过的项目，感觉回答的还可以。后续：系统里面凉了之后问了rr，说是这次招人目标比较明确就是看代码选手，只有一个hc给了代码审计选手。。。哭。。。

体验

我在想一个问题，如果你看好的团队有比较明确的招聘需求，比如招安全开发开发扫描器，而招聘需求和你目前的研究和规划有出入咋办？是花时间转方向填坑呢还是继续做自己擅长的事？以后工作中也可能出现这样的问题，如果领导让你去填坑，是去做呢还是拒绝呢

0x6C 腾讯云安全

数据分析一面

1. spark等大数据框架的熟悉程度
2. spark和storm的区别，以及什么场景选用spark
3. 常用的语言，java会吗
4. GBDT和XGBoost的区别
5. 无监督学习算法，Kmeans的原理
6. 单分类下HMM和One class SVM效果比较
7. 深度学习和机器学习的区别
8. 如何区分机器流量和正常用户流量，给出解决方案（重头戏）

我当时想了两种方案，有些细节没表达清楚，可能面试官误解了我的意思，后来我查资料发现我说的还是有那么点道理的。给出的第一种解决方案是传统安全手段/无监督学习+有监督学习，针对数据未打标问题，采用传统安全手段比如威胁情报，或是通过恶意机器流量的分析发现有些恶意机器流量来源于一些云服务商来对数据进行一些打标；也可以通过聚类来打标得到标记数据，之后再有监督学习。另一种方案是规避未打标数据的问题，直接无监督学习，使用Kmeans或是HMM等算法区分流量，从问题本身的角度来理解正常用户流量和机器流量的区别在于人的操作是有主观意识、有序的，而机器的操作是无主观意识、无序的，所以暂时倾向于使用HMM算法。两种初步的解决方案的后续都依赖特征工程，这就要分析观察机器流量和正常流量的异同。简单的机器流量可能是从脚本直接产生的，所以直接观察browser可能就可以区分，高级点的机器流量可以伪装成正常的浏览器，这就需要从是否模仿人类交互功能的角度来观察区分了，比如鼠标点击的（网页的）有序性和无序性，鼠标的轨迹等。

数据分析二面

1. 自我介绍
2. 做过渗透测试漏洞挖掘吗
3. 提交漏洞的平台、类型和危险程度
4. 打过CTF吗
5. 会Java吗（看来java不学不行了啊）

6. 机器学习做waf的方法
7. 追问了模型预测阶段如何处理使模型能够自动学习，比如如何达成预测阶段的误报和漏报，然后数据回流再训练模型（开始我以为是训练阶段的漏报和误报，直接说了混淆矩阵，然后花了几分钟才get到面试官意思是预测阶段的误报和漏报，也就是模型自适应性）
8. 如何选择模型，如何调参，有没有什么方法

hr面

吐槽一下腾讯座机，声音超小，hr又用自己手机打给我才继续面下去。

1. 评价一下腾讯安全
2. 用两个词概括你的性格特点
3. 从本科到现在你遇到的最困难的事情
4. 家是哪的
5. 是不是独生子女
6. 对工作地点有没有什么要求
7. 介绍简历上个人维护的项目
8. 有没有和同学发生过矛盾
9. 有没有拿到其他公司的offer，以及包括腾讯在内这些公司在你心目中的排名
10. 相对于其他安全人员，你的核心优势是什么
11. 你打算怎么融入团队
12. 如果实习的话，你有什么担忧
13. 实习时间大概什么时间

0x6D 蚂蚁金服

网商银行一面

时长：49分钟

1. 介绍一下你最成功的一个项目（面试官开始以一个项目为切入点从深度和广度综合考察知识工具逻辑业务体系）
2. 追问数据的构成以及预分析，特征工程如何做，特征编码的比较，算法的对比和选择，效果怎么样（考察深度）
3. 你的核心优势是什么（面试官之后给了一个中肯的建议，非常受用）
4. web安全中你实践过哪些漏洞类型（考察广度）
5. 记不清了...
6. 请面试官就我今天的面试表现给我一些建议

感觉一面是个质量面，从深度和广度不断试探深挖。

网商银行二面

时长：1小时

二面等了比较长的时间，腾讯hr面都面完了二面还没来，可能网商银行安全团队刚组建师傅们都很忙（哭），无奈催了一下，然后二面终于来啦哈哈哈。晚上七点半左右电话来了，我正好出差到广州还在吃晚饭，手机也没多少电，然后和面试官师傅约了十五分钟后再面，赶紧回酒店充电准备面试。

1. 你刚说在广州出差，具体是做啥的
2. 问了本科的学院和专业，研究生的学院和专业，面试官在疑惑我为啥是网络与信息安全学院计算机技术专业
3. 你用机器学习解决过哪些安全问题（我举了url异常检测的入门例子）

4. 面试官开始追问咋做的，具体问了数据和特征这块，算法稍微提了一下
5. 你是怎么选择模型和算法的
6. 除了url异常检测这个例子还做过哪些（说了DGA检测、DNS隧道检测、主机和网络入侵检测等）
7. 常用的语言和工具熟练度怎么样
8. 了解数据安全吗（靠平时这块比较少的积累和面试官讨论了一下）
9. 了解加密算法吗（不了解）
10. 面试官说为啥面了几个同学，对加密算法都不了解，我尝试从学硕和专硕的角度分析了一下
11. 在学校你最喜欢的课程
12. 能不能给我推荐一项技术或是一个领域以及一些学习资料（推荐了智能安全技术，很不要脸的给面试官推荐了我的github项目，介绍了项目的大致情况，会不会多个star，哈哈哈哈）
13. 你对web安全的理解（感觉面试官问的有点大，稍微确认了一下问题，一是基本的漏洞理解，二是我之前做过的一些工作）
14. 问了面试官主要的工作内容以及如果我入职我的主要工作内容
15. 问了面试官多久能给答复
16. 请面试官就我今天的表现给我一些建议（面试官非常nice，提了两点建议，都是我目前的缺点。一是我的回答表述有点啰嗦容易陷入一些技术细节，应该先从整体脉络讲清楚，二是工程能力需要加强，以及不能仅局限于自己的研究方向和擅长方向（感觉是针对数据安全和加密算法问题，知识和技术是通用的））

交叉面

时长：28分钟

内推人说有交叉面说明前面表现不错（至少是A？）。约的昨天交叉面，结果因为赶飞机正巧没接到电话，然后今天晚上七点半电话过来了，面到八点感觉面试官还有很多事要去处理。

1. 自我介绍
2. 机器学习技术解决安全问题对比与传统安全手段有什么优势
3. 问机器学习做DGA检测的例子，追问检出率和召回率多少，海量数据如何处理，传统的DGA都是随机性生成的，如果是单词字典组合的DGA该怎么判别，我回继续人工提取特征，然后面试官提示我，能不能从其他维度数据考虑DGA，然后我想到了时间序列、HTTP层数据。
4. 问机器学习做URL检测的例子，如果是扫描器扫描触发的大量异常该怎么处理，我说用聚类手段聚类忽略，继续追问，如果有攻击成功的异常，不能忽略的话，怎么判别是不是成功的攻击，我回通过响应内容来判断，这就涉及到用机器学习来做页面相似度检测了
5. 问机器学习做XSS检测的例子
6. 请面试官评价一下我的面试表现给我一些建议，面试官给了两个建议。1）在实际场景中不能为了机器智能而机器智能，得综合各种技术解决问题。2）我的表述技术细节说的多了。和二面面试官给的建议一样，我解释了一下，不说细节感觉空落落的。

交叉面的作用感觉是保级的，如果交叉面表现不错大概率还是A，表现不好的话就是B+成替补了，交叉面面下来感觉表现还行，估计技术评级还是A?

hr面

时长：29分钟

hr就问了三个问题，感觉自己的数学思维需要强化，半只脚都迈进蚂蚁了，太惨了，hr面表现不好，感觉要凉。

1. 介绍下让你收获最多的一个项目
2. 说说你的优缺点
3. 数学题1：100层楼两颗玻璃珠的题；数学题2:100颗白豆100颗黑豆的概率题

> 备注：从0x6E~0x均来自于https://blog.51cto.com/sfsec/4862487

0x6E 360企业安全

1.平时用什么软件测试（BP）

2.你觉得BP哪里特别好用

3.你有没有看过测试工具的源码（没有）

4.给你一个网站，你怎么找漏洞，举个例子

5.你说验证码绕过，说说看怎么检测验证码绕过漏洞

6.你知道csrf吗，解释一下

7.csrf怎么防御知道吗

8.看你写过poc，你能举一个例子吗

9.你比较了解哪些漏洞

10.说一说怎么发现sql注入

11.听过盲注吗，解释一下

12.我看你会用python，会的多吗

13.代码注入能讲一下吗

14owasp top 10 哪些你比较了解的说一下吧

0x6F 58集团

1.了解安全审计吗

2.会php吗

3.会什么编程语言

4.未来的方向是什么

5.会写脚本吗？写过哪些脚本

6.用过python框架吗

0x70 海康威视

海康威视似乎没有笔试，突然就来了电话。一开始就直入主题，没有自我介绍。所有面试中问的问题最多（30几个）的面试，中途还换了个面试官接着问（接力嘛）面试全称围绕简历进行，同样针对项目的细节和实习的工作问了很多问题。

面试问题大致如下（省略了项目和实习相关的问题）：

1.我看你简历上说会bp和sqlmap，能说一下你觉得bp有什么优点吗，你觉得哪里好用

2.你觉得哪个功能最好用

3.sqlmap用的多吗

4.了解sqlmap的高级使用吗，比如使用插件和一些条件过滤

5.sql注入有哪些类型说一下

6.盲注知道吗

7.有写过sql注入的插件吗

8.看你写了解主流web漏洞，你说一下主流的有哪些

9.能讲一下xss的原理吗

10.怎么防御xss呢

11.听过富文本吗?

12.黑名单要怎么设置过滤?

13.你写了些什么脚本，是自己定义了策略吗

14.说一下你渗透一个网站是怎么样的思路

15.你见过最有意思的一个漏洞是什么。

16.目前有offer了吗

17.那你了解密码学吧，讲讲AES的流程（因为在学校做了几个密码学的项目，故有此问）

18.你籍贯是哪里?

19.有什么问题问我?

0x71 顺丰科技

面试问题大致如下（省略了项目和实习相关的问题）：

一面：技术面

1.自我介绍

2.实习的时候怎么做渗透测试的

3.xss和csrf的区别

4.说一下你写的poc

5.修复的沟通是联系安全部门还是联系开发?

6.你对安全的看法，为什么想做安全?

7.（看成绩单）java课设做了什么，分挺高的

8.有什么问题想问?

二面：hr面自我介绍

1.为什么做安全

2.用三个词形容你自己，并分别举例佐证

3.籍贯哪里，愿意去深圳吗

4.深圳房价很高，你打算买房吗

5.有什么事情你觉得成长特别多的

6.你人际交往怎么样

7.遇到难以解决的困难你怎么办

8.了解顺丰吗（快递？）还有吗？（物流很厉害？）

9.还有投什么公司

10.有特别想去的吗

0x72 平安科技

一面

一面：面试官人特别好，一见面就笑眯眯地，面试中途还开玩笑。面试全程都像在聊天，完全没有紧张感。同学面的测试和开发都说问了很多技术问题，比较难。但是我基本在聊简历，从实习经历聊到项目经历，然后是关于他们公司的一些实际问题，就结束了。以至于结束的时候，面试官直接说我们今天就聊到这了，你可以离开了，我还愣愣的。回去的时候和同学商量了一下觉得可能是没有hc了，面试官才这么佛系，但是当晚通知一面过了。玄学。

除了项目问题，只记得几个：

1.你觉得公司需要怎样保障业务信息安全?

2.如果程序员写的业务代码很多漏洞，业务明天就要上线了，怎么办?

二面：hr面

参加二面的时候，安全部门大佬没来，于是直接先面hr，通过了后续再单独二面通知，不参与第二天的座谈会

1.为什么想做安全

2.实习做了什么

3.实习期间最有成就感的事是什么

4.实习公司的业务主要是哪些

5.为什么不考研

6.专业其他女生都做了什么

7.希望找什么样的公司

8.有其他offer吗

9.offer薪资多少

10.你的期望薪资是多少

11.有什么想问的

> 备注：从0x73~0x79均来自于另一个面经仓库：https://github.com/h4m5t/Sec-Interview/
> 翻了一眼，感觉问题可能稍微有点旧，不过作为参考总是好的，挑了一些放到这，剩下的可移步链接自行参考

0x73 360

时长：48mins

1. 多久开始接触安全的?
2. 熟悉安全方面的哪些内容？web?逆向？IOT?在公司主要的工作内容?
3. 分析下Web框架（Django,Struct 2）出现过的漏洞，原理，分析过程，利用手法 。（因为简历有提）
4. 有没做过安全开发？写过哪些安全工具？namp扫描器原理?
5. 场景分析：360自制扫描器扫出100w个可疑URL，如何写脚本排查sqli误报？如何排查xss误报？（url中存在payload）思路?
6. 黑过哪些网站？说一次最骄傲的Hack经历(从得到域名到getshell)?
7. 如何搜集子域名？getshell有哪些方法？哪种用的最多？提权了解过哪些方法？nc反弹提权原理？一句话木马原理?
8. 内网渗透玩过没？域?
9. 逆向会不会？软件安全了解过没?
10. 想做来做哪个方向？安全开发？安服？安全研究?

0x74 哔哩哔哩

CTF 相关

- 简述 CTF 攻防赛的流程和一些技巧；

服务器运维

- 查看当前端口连接的命令有哪些？`netstat` 和 `ss` 命令的区别和优缺点；
- Linux 服务器的安全运维操作有哪些？如何保护 SSH?
- 入侵 Linux 服务器后需要清除哪些日志?
- 反弹 shell 的常用命令？一般常反弹哪一种 shell？为什么?

渗透测试

- 介绍渗透测试的流程；
- 简要介绍自己常用的扫描器和其实现上的特点；
- 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?
- 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?
- 介绍 CSRF 漏洞和常用的防护手段；
- 介绍 SSRF 漏洞，如何深入利用？如何探测非 HTTP 协议？如何防范?

安全运营

- 如何防范羊毛党（有猫池）?
- 如果 SRC 上报了一个 XSS 漏洞，payload 已经写入页面，但未给出具体位置，如何快速介入?
- 发现一个大范围影响的新漏洞，如何快速排查公司资产?
- 如果你是安全运营的负责人，简要介绍你对安全方面采取的措施；
- 发现了一个漏洞，你报告给开发人员，但是开发人员不愿意修漏洞，如何沟通？（这是个什么奇怪的问题。。。）

> 备注：从0x75~0x77均来自于lc4t师傅
> 链接1：https://blog.sakanano.moe/posts/archive_2017_spring_interview/
> 链接2：https://github.com/h4m5t/Sec-Interview/blob/main/%E9%A2%98%E7%9B%AE%E6%95%B4%E7%90%86.md

0x75 百度

一面

- 如何做扫描器 思路
- 创宇wooyun的扫描器原理
- 扫描器为什么要这么设计
- 企业安全应急响应 如何获取指纹
- 如何获取大量指纹信息
- sql注入类型
- sql注入点寻找思路
- sql如何报错
- 宽字节注入原理/在哪里编码/如何防范
- sql里面只有update怎么利用
- mysql和sqlserver注入时候的区别
- dom xss 原理/防范
- 存储型xss原理
- xss防范
- xss过滤放在输入还是输出好
- 如何快速发现xss位置
- 如何绕过http only
- xss worm原理
- 如何保护dom不被修改 防止dom xss
- sql注入思路，首先测试什么
- sql如何写shell/单引号被过滤怎么办
- 同源策略
- html5安全/websocket
- cookie参数，security干什么的
- 平时用什么语言开发
- 写过什么项目

二面

- 介绍
- 学习了多久web安全 学了啥
- （就介绍内容提问，系统观）
- webserver最重要的是什么/流程
- 熟悉的语言 写过什么
- 最熟悉的漏洞 原理 防范
- xss/sql/原理防范，利用方式，能用来干啥
- csrf如何不带referer 如何防范
- xss绕过同源策略/获取另外网站的/子站的
- 同源策略 是什么 why
- 给写php的人安全建议
- php非安全的函数

- ddos原理
- 反射原理
- dns协议在哪一层 什么时候用tcp
- 网络协议脆弱性了解
- tcp/udp区别 如何做可靠性连接 why
- tcp可不可以反射dns做ddos
- 漏洞挖掘经验
- 代码审计经验
- 漏洞深入研究经验
- 实习能来多久（小于3个月似乎不要？）
- 实习的话想干什么
- 有什么没问到的方面
- 扯到的：百度xss防范机制/大网站子站安全性

0x76 腾讯

一面

1. 自我介绍
2. ctf干啥
3. sqli测试思路
4. 黑帽子怎么用sqli
5. 拿到权限的方式
6. 有IDS怎么绕
7. webshell检测 反弹shell 一句话shell？？？
8. 对waf有什么了解
9. log清理
10. 扫描器 微内核方式 事件驱动 微服务 分层
11. 爬虫 phantomjs特点 弱点
12. 爬虫登录问题
13. 爬虫相似页面参数变化页面去重
14. 爬取和测试间隔时间长，导致cookie失效
15. 写不写c和c++
16. 堆栈反转，只能用不超过堆栈空间一半的额外空间 二分 边界 重复数
17. celery干啥 redis防护
18. cso注意事项 企业安全内部外部 协议分层
19. 如何抓到运营商劫持的证据 防护运营商劫持 dns劫持
20. web安全以后和什么技术结合
21. 在学校干啥
22. HTTP流量分析能得到啥

0x77 360

- 写过什么项目，什么功能
- xss http only如何获取cookie
- xss还能干什么
- 只有后台如何渗透
- 渗透一般思路
- 如何社工一个企业的员工信息
- csrf 如何不带referer访问

- 如何获得一个域名的邮箱列表
- 如何知道waf信息
- 如何收集子域名
- 1521是什么端口
- 用什么扫描器
- mysql4,5的区别
- mysql提权方式
- mysql udf提权 目录位置

0x78 华顺信安

1. 自我介绍
2. 红蓝队经验
3. 关于shiro漏洞了解多少~
4. 说说你APP测试的经验~
5. xposed用的什么框架有没有自己写过app解密
6. Xss SSRF SQL 产生的原因修复方案
7. 如果你Xss打了后台，发现是内网的怎么办~
8. 假设给你一个目标站，你要怎么做?
9. linux和windows提权知多少。
10. 会不会进程注入?
11. 做过几次应急?
12. 讲讲windows和linux应急你咋做的
13. 用过没用过我们家的goby和fofa?
14. 会不会apk反编译?
15. 你python水平咋样?
16. 你php怎么审的

0x79 某步

操作系统

- 问：linux命令熟悉吗?
- 问：查看进程的命令有哪些?
- 问：还有吗?
- 问：查看网络进程的命令?
- 问：linux如何加密md5?
- 问：那问个简单点的，如何快速查看文件类型?

渗透测试

渗透测试部分问的比较基础，也不多

- 问：说下sql注入?
- 问：讲下xss?
- 问：反射型xss和dom型xss的区别?
- 问：看你挖过src讲讲你挖过觉得比较有趣的漏洞?

应急响应

- 问：linux被上传了webshell如何查杀？
- 问：除了杀进程还有什么方法可以快速找到webshell吗？因为有时候占用率高的不一定是木马，也可能是业务相关进程
- 问：日志会看吗？
- 问：那这个问题跳过，你了解hw是做什么的吗？
- 问：最后一个问题，在一个很大流量的环境中，如何快速对报警进行一个判断？

> 备注：从0x7A~0x7F均来自于`hurricane618`师傅
>
> 原文链接：https://hurricane618.me/2021/12/08/2021-autunm-recruitment-summary/#%E9%9D%A2%E7%BB%8F%E6%B1%87%E6%80%BB

0x7A 绿盟

一面

25min

1. 项目1中的协议分析，协议逆向问题
2. 工控中的fuzz攻击面
3. 项目中的ida脚本的使用
4. 印象最深的复现漏洞
5. MIPS架构中的流水线处理（一般来说会先执行赋值操作再进行跳转）
6. 获取国外信息的来源 （Twitter+玄武的整合数据等）
7. 会有针对文章复现漏洞吗？
8. 反问？

介绍了一下绿盟这边IoT主要做的事情，听了之后以下几点吧。然后他们居然还有专门打比赛的人。。。我觉得还是研究真实设备好。

二面

20min

全程在问项目的相关问题，但也没有问的特别细致。。。感觉是个领导。然后问了我对绿盟怎么看？对格物实验室怎么看？

0x7B 360

一面

30min

1. IoT设备的攻击面与攻击思路
2. 最近有关注什么议题——Nas设备的攻击思路
3. 二进制里面栈溢出的利用，有没有利用的可能
4. 二进制中的堆利用方法
5. 怎么利用堆泄露信息（在tcahce中用cmalloc的方法就不会有初始化）

6. 问能不能实习
7. 问了一些web方面的漏洞利用，比如变量覆盖
8. 本科时候做web安全相关的内容，php版本的变化
9. 一些本科时候做的事情，做了怎么样的web题目

二面

15min

直接就是hr面了。。。。也不知道是什么情况。。政企安全，最后我想问是哪个实验室，也没正面回答我。。。最后还是问了360的师傅才知道是vulcan。

0x7C 奇安信

一面

30min

1. 间接跳转怎么恢复的？（如果是回调的方法怎么处理？）
2. 如果是遇到复杂的数据结构该如何处理？
3. ARM架构的栈溢出漏洞利用和MIPS的区别？
4. 复现过的漏洞讲一个
5. 如果给一个高难度目标设备，怎么去分析？（学习历史漏洞，归纳出容易出现问题的部分重点关注）
6. 反问

给了我的一些非常实用的建议，中间老板还来干扰我。。。幸好面试官人不错。

二面

20min

1. 固件分析项目中的效果如何？
2. 介绍实验室情况

似乎是一个领导，没怎么问问题就这样了。。。只稍微了解了下情况，居然问了我导师是谁？霍玮还真有名。

主要目标是有商业宣传效果的大漏洞。通常是人工审计的方法，windows和linux都有，开源的也有，cisco和华为，也有公司的产品。主要根据个人的方向来决定。

hr面

15min

1. 为什么选择北京？是否家里有亲戚在这里
2. 未来的职业发展方向
3. 其他公司的投递情况，这个hr很了解信工所呀，知道有很多师兄都去了华为 23333
4. 问了点项目中的基本情况
5. 预期薪资

0x7D 深信服

一面

45min

1. 项目介绍
2. 挑战应答过程的细节点
3. 固件分析二进制的背景，最后完成的效果
4. 路由器固件漏洞分析调试问题，如何追踪路径，以及确定触发这个漏洞点
5. 密码学中的DES和AES的区别？AES的密钥长度和DES？四种块加密方式的区别？哪种最常用？

问的好细。。。而且问到了我写上去的密码学相关的内容。。。。我应该再复习复习的。比如 密钥的长度问题。。。

二面

25min

1. 项目介绍
2. 项目中遇到的难点，最后是怎么解决的？
3. 跟踪过什么github项目吗？
4. Python的class是由什么对象创建的
5. Python的垃圾回收机制
6. 第二个项目是有几个人做的？我做了哪个部分
7. 漏洞缓解机制？以及如何突破它们？
8. 复现的比较有意思的漏洞

感觉还算不错，应该是个领导。

加面

25min

1. 项目介绍
2. 复现的漏洞
3. 挖掘过的漏洞
4. base地点
5. 职业方向
6. 有没有搞过windows相关的程序
7. 固件加密之后怎么破解

没想到还是加面了。。。有点神奇。。。不过最后的hr面忘记参加了，23333。

0x7E 大疆

一面

30min

1. 固件签名怎么做？
2. 对称加密和非对称加密的区别
3. 讲讲AES加密算法
4. 问问项目实现细节
5. 分析过哪些固件，说一说怎么分析，怎么找漏洞
6. 工控协议认证中的缺陷问题

大疆这边的安全部主要做无人机和安全产品方面的工作，还有从底层芯片到上层应用的安全测试。

二面

40min

1. 简单项目介绍
2. 最有成就感的项目，哪些工作比较有亮点
3. 针对项目介绍一个例子
4. 溢出漏洞怎么利用
5. 对大疆无人机有什么了解？怎么攻击？怎么做漏洞挖掘
6. hash计算为什么要加盐
7. mac和签名的区别
8. 防御这一块做了哪些事情
9. 漏洞挖掘中的前沿技术，有哪些团队在做
10. 最近网络安全发生的大事件或者突破性的技术
11. 未来三年的职业规划

是个小领导，我问了关于物联网安全未来的发展问题，他讲了大疆在安全对抗中做出的成绩，比如在禁飞区的对抗上，摄像头的安全，与社区的破解对抗。

三面

25min

1. 简单介绍自己研究的方向
2. 对大疆的了解
3. 平时的兴趣爱好
4. 对哪些电子产品感兴趣，以及自己对电子产品的理解
5. 对无人机如何做攻击
6. 反问

hr面是一个中年老男人，头发稀疏。。。有点害怕，但人还是很和蔼，我能感觉到他通过面试记录知道我不太了解他们公司的产品，所以我着重的又去看了一遍他们的官网，没想到果然问了，2333。比较有意思的一点，我反问了为什么他们做安全的团队会在上海而不是在深圳的总部，原来是因为历史遗留的问题，导致上海的安全部门都在上海发展。

0x7F 华为

一面

60min（主要是写题写了30min都没写出来。。。。）

1. 项目介绍，以及项目中的细节点
2. double free如何利用
3. 内核层中进程间通信怎么实现的
4. 内核中对打开文件在进程中如何共享
5. 你最熟悉的语言是什么？对C++的掌握程度

考了一道前序遍历数的验证。。。他提示了半天，我差点就写出来了，最后他说什么引用计数。。。这说法太诱导性了。完全想偏。

二面

40min

1. 项目介绍
2. 堆溢出漏洞利用
3. UAF漏洞利用
4. 栈溢出漏洞利用
5. IoT漏洞如何调试以及攻击面探测
6. 动态分析了解的情况
7. 静态分析了解的情况

考了一道括号匹配的题目，还好学长给我说过，要不然真的尴尬了。

三面

30min

1. 询问学校的专业和技能掌握情况
2. 未来的发展规划
3. 针对ASLR如何绕过
4. 针对PAC如何绕过
5. 在CTF里面获得过最好的成绩是什么
6. 老家在哪里？父母的工作情况
7. 工作地点的选择，父母有没有反对
8. 对华为的文化有什么了解？
9. 科研中遇到的问题？最后怎么解决的？
10. 对加班有什么看法？
11. 除了安全，对其他方面还有什么研究
12. 手上有哪些offer？华为给了你offer之后会怎么选择？如果华为的钱没那些公司高怎么办？
13. 反问