信息安全面试指南

信息安全面试指南（SecurityInterviewGuide），内容从行业、公司与从业者展开，辅以一些通用面试经验，核心是面试题库，助你你找到心仪的工作。

关于面试这件事

理解安全行业现状

如何选择公司

安全从业人员必备素质

安全从业人员能力分层

优秀的简历是怎么样的

安全招聘渠道

安全面试经验

基础素质问题

安全面试题目

- 应用安全岗位
- 网络主机安全岗位
- 威胁应对岗
- 数据安全岗
- 合规审计岗
- 安全蓝军岗位
- 安全开发岗位
- 安全管理岗

安全笔试题目

安全行业人才趋势

关于面试这件事

多年来筛选了数以千记的简历，为何很多人连面试的机会都没有？参与了数以百记的应聘者的面试，为何如此多的人没有通过最终面试？能力当然是最重要的，可我却见过很多能力不比已经入职的同事差却应聘失败的人，到底该如何做？希望这篇安全从业者面试指南能够帮到你，让你少走一些弯路。

本文目标是希望创造一份针对**网络信息安全领域**从业者的面试指南，从行业、企业、从业者等方面了解当前现状，学习通用的面试和招聘经验，核心围绕各个细分安全岗位的**体系**、**实用**、**高质量**的**题库**展开。

本文主线围绕面试者视角进行全流程讲解，其中会穿插企业视角、HR视角以及技术面试官视角，让你能够更加全面体系的理解并吸收各种经验。其中核心题库部分，会存在较强的时效效应，因此会不断的进行更新，增加新的题目、剔除不合适的题目、调整题目难度或解答提示。此外题库的来源于真实工作中，能够确保题目能真实反应应聘者能力水平。

因作者能力和精力有限，如有错漏，请通过每篇文章底部评论处反馈，感谢！

读者对象

本文内容适合应聘者以及面试官。

- 如果你是在校学生，通过阅读本文可以了解从业人员必备素质和公司考察的问题，以找到自己当前的薄弱点进行补充学习。
- 安全爱好者，如何从爱好者变为从业者？如何从业余级别进阶为专业级别？也许你能在这里找到答案。
- 其它行业有面试需求者，本质上没有某个行业的面试指南，所有面试都是相通的，你一定能从其中得到一些收获。
- 安全从业者，帮助安全从业者更从容的面试与被面试。

同时，本文也被众多企业面试官所采用，作为面试官也可以使用相关领域问题，同时也欢迎通过评论提交你觉得有价值的问题。

更新记录

- 2021-12-02 更新简历章节，完善写好简历的要点。

版权申明

理解安全行业现状

行业处于起步阶段

安全行业起步晚。安全行业整体起来才没几年，多数企业因为资源投入和建设时间原因导致覆盖面和深入度都不够，这其中甚至包括一些国内大厂，并没有想象的那么安全。其安全水位仅能应付一些白帽子级别，针对专业黑客团伙持续定向攻击，大多数都不能防御住，看HW就知道了。

从业人员薪酬高

由于安全行业起步晚，安全人才紧缺，需求旺盛，导致安全从业者薪资水涨船高。高到什么程度呢？都知道互联网行业薪酬是所有行业中最高的之一，技术类是互联网行业中薪酬相对最高的职能，而安全工程师又是技术人才中薪酬最高的，和当下发展正火的机器学习人才并驾齐驱。可能还是没概念？这么说，应届信安专业优秀本科生能拿到每月20000-35000（当然这里面有很多行业内卷的因素，一些公司的招聘策略是入职即巅峰，后面薪资就不怎么涨了），努力工作三四年的能拿到40000每月，做到安全团队管理者后能拿到百万年薪，做到行业顶尖能拿到千万年薪，后面也会讲不同薪资对应需要什么样的能力结构。随着市场调节，越来越多的学校开设信息安全相关课程，越来越多的培训机构教学信息安全知识，越来越多的人学习或转行做信息安全，整体紧缺情况有所好转。

安全水位难衡量

很多事情是有因果关系的，前面讲到的良莠不齐的根因在于很难通过结果来判断安全建设的水位。很多团队的KPI是不出安全事故——什么事都不做也不会出安全事故。于是造就了吹嘘拍马之人的风生水起。但随着实战红蓝演练的普及，国家级别实战攻防演练的规模和范围扩大，逐渐用模拟实战的方式来检验防护和应急效果，能一定程度上改善这类情况。

从业人员良莠不齐

好处是会有更多的人投身于安全，当然坏处也很明显，人员空缺与岗位的紧急程度导致存在大量能力良莠不齐的人在行业内浑水摸鱼，明显的特征是你跟他聊技术细节他跟你聊推进落地，你跟他聊推进落地他跟你聊方向把控，你跟他聊方向把控他跟你聊团队管理，你跟他聊团队管理他跟你聊行业空间，如果这些方面都能聊一点那也行，更多人是答非所问或者看似句句在理实际空洞无物，更有甚者，不知在何处听到的理论还没消化完毕，就拿出来班门弄斧。虽然这么说会得罪一部分人。有人问难道入职后不能衡量出来吗？正常老板不懂的情况下，还真不能衡量出来，主要是因为前面讲到的安全水位难以衡量，而实际的安全风险都是小概率事件。

安全建设驱动因素转变中

金融、电商、游戏这些业务类型对安全有天然诉求，作为业务的重要属性，不做安全黑灰产都会盯上来，此时属于黑灰产驱动安全。乌云等公共漏洞报告平台兴起后，各家企业的安全建设又上了一个台阶，

属于白帽子安全事件驱动。而后，白帽子驱动的模式由于合规问题也逐渐减少。更多企业只是为满足合规而进行安全建设，甚至一些企业会购买大量安全产品，但只为了应付监管检查却不使用，此时仅为合规驱动安全。最近几年的行业风气，因为国家攻防演练的增加而变得正常起来，逐渐演变为由实际风险驱动安全。

安全圈子文化氛围浓厚

安全是一个小圈子，圈内事件传播十分迅速，比如哪家企业数据库泄露、哪家业务活动被薅羊毛、哪个安全人被抓、哪个企业遭到了什么处罚等负面新闻。圈内人能够很快了解到行业新技术、新方向、新政策，能够很容易了解到每家公司的安全建设情况。你能了解到阿里安全与线下公安配合的手段之强，也能认识到腾讯的SRC如何能够运营的的这么好，更能和百度的安全人讨论如何让机器学习赋能安全产品，这一切场景在安全圈内的实现都非常容易。众多安全会议的举办也能让你学习到每家公司的经验，无需自己摸索、闭门造车。这都是小圈子的好处。当然弊端也很明显，总有一些人搞所谓的“圈子文化”，混迹于各种安全会议主动认识圈内人（当然这里不是指各家SRC运营的同学，这些是运营同学的工作一部分）。结识所谓圈内人如果出于交流技术的目的也能理解，但这些人仅仅是加上微信，发送一条打招呼的自我介绍后就再也不会有任何有意义的交流。妄图以这样的方式让自己进入圈子中心，可笑可悲。

学历相对不重要

安全圈存在很多无学历或低学历的牛人，他们年龄可能不大、工龄也短，但往往都是兴趣驱动，早期就在安全方面投入了大量时间精力，因此颇有造诣。当长处特别突出时，往往会突破企业的一些要求限制，比如岗位学历要求本科时，候选人突出的安全能力能让这项要求降低。同时也必须正确认识低学历对工作带来的影响，在当前安全行业逐渐细分、安全建设越来越深入的趋势下，安全从业者不再只是会挖漏洞就行。建议低学历候选人尽早通过自考的方式系统的学习英语、数学、计算机基础等学科，并获得国家认可的成人教育学历，届时学历问题的影响就不再会是问题。随着大量院校开设信安专业，越来越多的人进入到安全行业，后续企业招聘安全人才时，学历要求肯定会和其他行业一样成为基础筛选要求。

如何选择公司

我们都知道选择比努力重要，人生总在不断面临选择，有些选择大有些选择小，而下一家公司则是人生中最重要的选择之一，这个选择关系到你未来几年甚至整个职业生涯的成功与否，无论是技术能力、管理经验、薪资水平甚至另一半都会受到影响。选择一家对的公司会让我们接下来几年得到事半功倍的成长。

穷选互联网。从行业历史发展角度来看，互联网无疑是发展最快的，虽然已经高速发展多年但还在持续不断的进化，趋势持续向好。同样的人在传统行业工作五年前后，并不会有太大差别。但在互联网行业，你永远无法想象自己五年后是怎么样的，互联网将赋予你无限可能性。从二十多年前开始，我家里就一直在开服装加工厂，除了在我还小的时候，那时服装产业火热，工厂赚了一些钱外，就再也没什么大的起色。其余一些开厂的亲戚朋友都没赚到什么钱，反而是厂房卖了赚了不少钱。我哥哥是公务员，很多人都会羡慕他工作轻松稳定，但工资涨幅、职位升迁都能预料的到，一眼望到头的职业空间不是每个人都能接受的，在体制内你再努力都会显得那么力不从心。

甲方好于乙方

互联网又可分为甲方和乙方，乙方由于是销售导向的，所以在人员技术深度和薪资水平上相对甲方会明显差一些，因此优先选择甲方。 我面试以及接触过太多乙方人员，不可否认有很优秀的，但受限于乙方的工作形态，大多数还是在做一些基础且重复性的事情，长期在这种环境下只会毁掉自己。

选择巨头或潜力股。互联网甲方又可以大致分为综合体巨头、大型平台经济公司、细分独角兽、初创公司，对于多数人来说按从左到右的优先级选择是最优解，但也有意外，选择独角兽公司有可能为你带来更大的资金收益（期权价值增幅）和综合能力成长（安全广度和空间），当然很有可能变成过气独角兽。

刚工作那两年，我在好多个小互联网公司工作过，这么多年过去了，还在小互联网公司的前同事现在的薪资还在两万多，而巨头热门岗位的应届生薪资都比他们多，这就是小公司的天花板。由于业务规模导致技术深度、薪资水平很容易进入瓶颈期，且随着时间推移，你的技术热情也在消退，学习能力也跟不上，年纪也成为了进入大公司的瓶颈。

我庆幸的是在14年加入了当时的虽小但有潜力的公司蘑菇街，陪着蘑菇街一路到上市。有潜力的公司能让你坐上技术成长的快车，跟随公司一起成长会更顺畅和扎实。当你无法判断潜力时选择某个细分领域独角兽会更加稳妥。后来进入蚂蚁，往往大公司过了初期建设阶段，能让你更专注在某一个细分点上深入进去，同时薪资和向上发展也能得到保障。

努力提升，及早逃离小且没有潜力的公司，否则别期望你的人生有什么改变。

钱和成长兼得

金融、电商、游戏公司很早就会有安全岗位，正是因为他们业务上对安全天然有着强诉求。一方面对安全的资源投入上会大很多，能让安全话语权、事情推动上变得水到渠成。另外一方面你无需为了寻找那不存在的安全风险而努力，自然而然的会持续有大量投入进行长期建设。

见过太多公司的安全建设不以解决实际安全风险为出发点，开拓了一些伪安全需求，做和不做公司的风险都在那儿。

不要服务伪需求，害了公司也害了自己。

文化氛围至关重要

从事黑灰产的公司先排除掉，包括擦边球的，公司文化不正就会出现flanker前公司那种让安全人员做一些违法的事情，短期是能赚到一些钱，但习惯赚这类钱就很难再回去了，而且很容易就得研究监狱安全性。 团队氛围是一个很泛的概念但却至关重要，做的开心与否决定了做的能否长久。其中包括大家相处的融洽程度、做事方式方法、团队公约、人员能力等，提前找人打听下这个团队的氛围是非常有效的方式。我很庆幸自己的兴趣和工作是一件事，每天都能很开心的工作。但如果团队氛围不好，就像跟不喜欢的人玩游戏一样会非常痛苦。 正向的文化和氛围有助于我们待的更久。

岗位契合度是重中之重

岗位第一优先级需要关注是否和自己的未来的职业发展规划是否匹配，不合适的岗位发挥不出你的才能，继而成长也就相对较难。第二要关注你擅长的技能和公司的需求要匹配，才能发挥最大生产力。

我见过太多上班如上坟的同事，也见过明明之前很优秀的人但去了某个公司突然就沉寂了。当然也有团队能够因人设岗，用人之所长补企业缩短，充分发挥出最大效率。

安全从业人员必备素质

具备基础的工程师素质是从业的基础，在攻防渗透和软件开发有较为扎实的基础，同时兼备兴趣驱动和良好的适应能力上比较亮眼，则能很好的适应工作挑战。

基础：渗透测试和软件开发

首先要明确一个概念，术业有专攻在安全行业不是常态。安全本身就是一个覆盖了客户端、前端、网络、后端、服务器等涉及JavaScript、Python、PHP、Java等各语言的工作，如果非要讲究术业有专攻就没法做了，当你可以有擅长的方向，但前提是你都懂。这个“懂”不应该只停留在了解的层面，如果你是安全开发工程师，除了研发技能外，还必须知道常见漏洞的形成原因、利用方式和修复方案。如果你是渗透工程师，除了理解各种漏洞的攻击细节外，还必须有基本的开发能力。同时拥有攻防渗透和软件开发能力的人，在安全从业时的方方面面都会体现出极大的优势。

计算机基础技术要了解并持续学习，安全也是不断在进步的，几年前你很会挖漏洞就很厉害了，但今天你还是这样的话就没什么优势了。

摸黑前行最好的应对方法是你曾住过这个房子，或许你是一位资深研发工程师，但安全产品不同于用户产品，往往是没有经验也没有参照物的。所以往往需要有很强的安全背景与不断的试错调整才能开发出最好的安全产品。甚至在很多时候，沟通交流与思维方式都需要进行转变才能更好的协作，减少代沟和沟通成本。

安全行业的现状是大部分从业者都偏向于攻防渗透，如果同时拥有强大的开发技能，从业优势将非常明显。在安全产品开发、漏洞挖掘、代码审计上，不同技能的互补显得非常重要，做漏洞扫描器的同时如果在SRC挖过漏洞、做代码审计也能掌握软件开发、做合规审计的人也拥有CISP证书，工作中就会更加得心应手。

热情：兴趣驱动是最长久的

和安全产品开发一样，渗透测试也需要不断试错，我们往往在各种可能存在漏洞的地方测试数百个请求才有所收获，这需要经年累月的坚持下来，但这种坚持无法速成，而兴趣这位最好的老师就能够促使我们坚持。我对于安全的坚持就是兴趣驱动的。遇到一个线索，我会从傍晚折腾到黎明；又会因为一个突破点，从凌晨摸索到下午。我见过太多优秀的白帽子都是因为热爱，特别是他们能够跨行业地坚持热爱。

成果：没有结果的优秀是空谈

直观的成果是展示自己综合能力的最好方式，无论是在顶级期刊发表论文、知名比赛中获得好成绩、挖掘众多高质量的通用漏洞、研发Star数非常高的开源项目，还是在安全会议上分享先进理念，甚至突破了行业难题等等。

其它：优秀特质越多成长越快

- 适应能力，软件工程师普遍三年换一轮新技术，而安全工程师则是每年都有新的安全技术、安全防御手段、安全方向，而应对这些思念情况，别无他法，唯有不断学习，良好的自驱自学能力会让你更快成长。
- **智商高、情商高、乐观**、沟通交流、逻辑、影响力等

安全从业人员能力分层

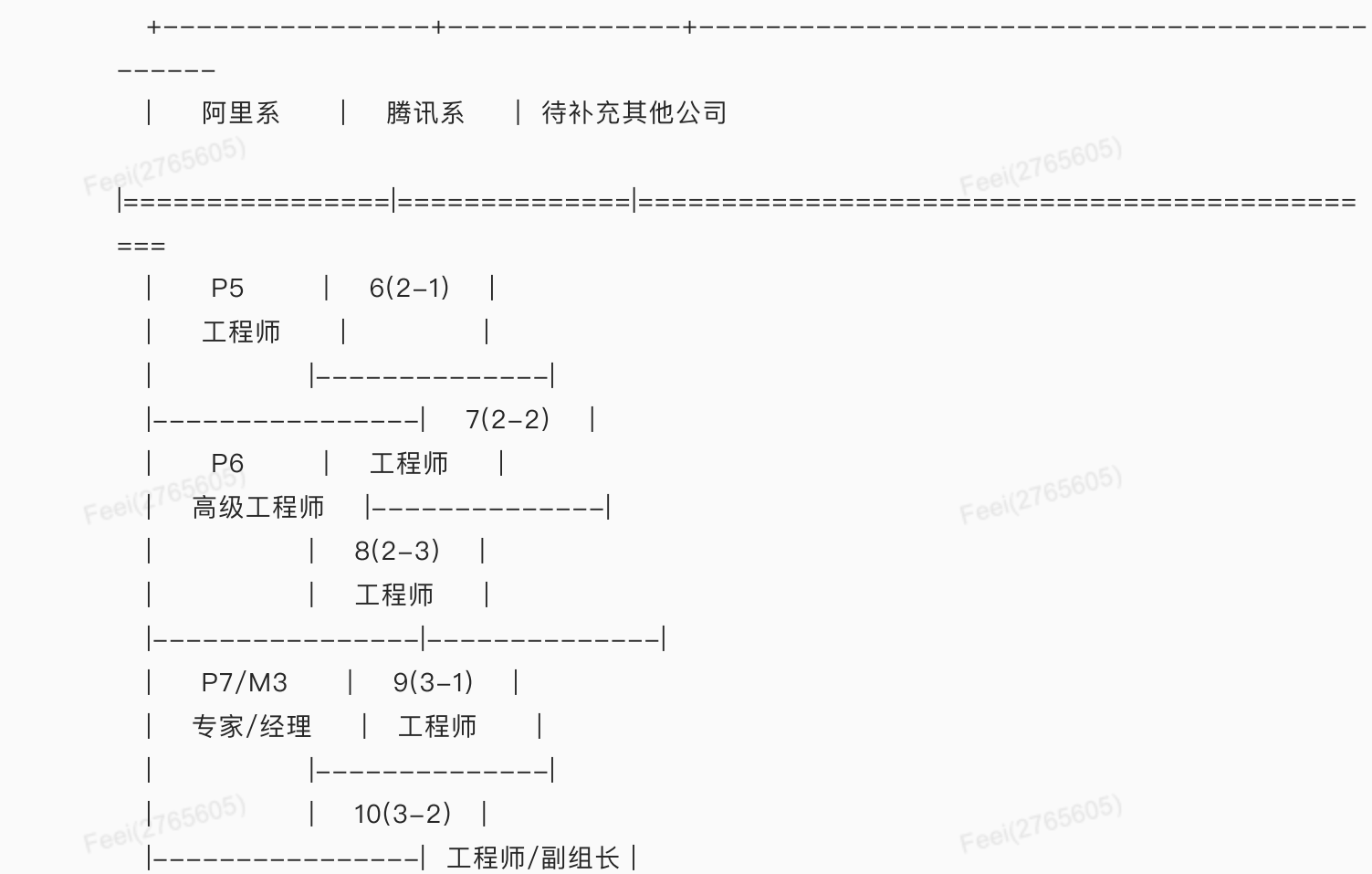
上一章节讲述了基础的安全从业者应具备的素质，如果你已经具备这些素质，那么已经踏入了安全行业的门槛。这一章将重点讲解下入门之上的能力分层，不同层级更重视需拥有怎样的特质。

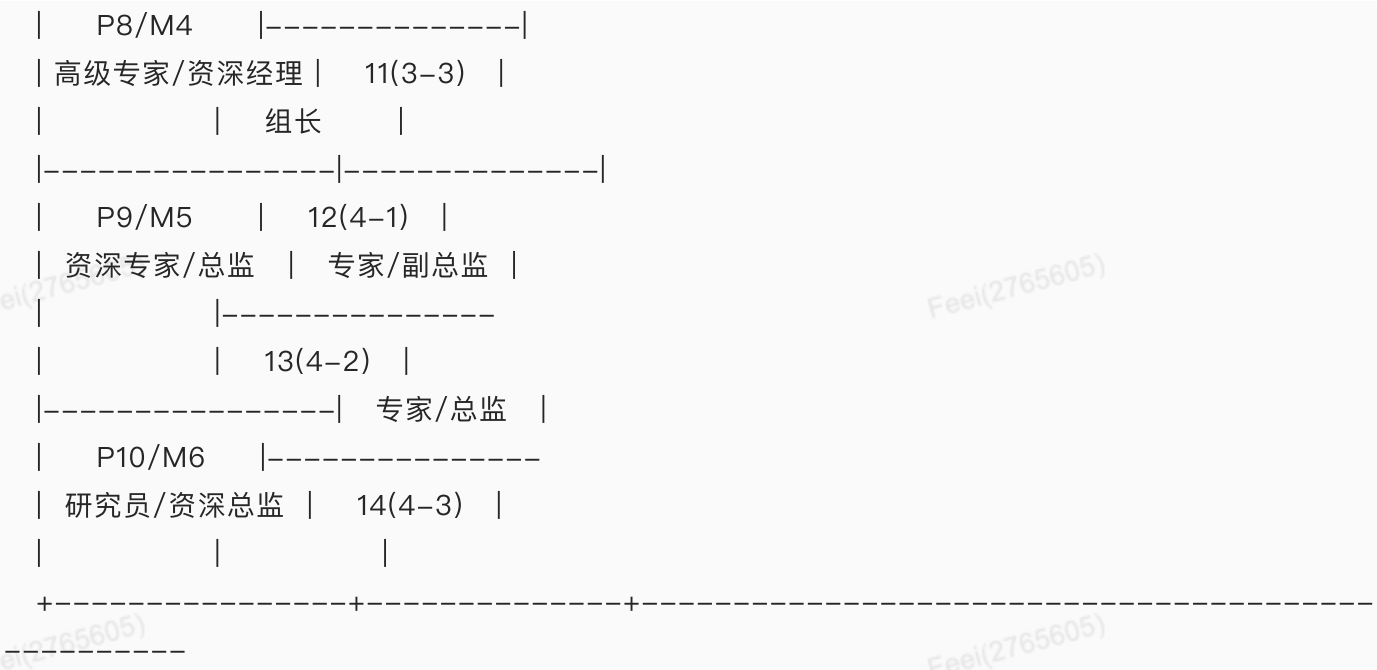
各大公司层级情况

能力分层是一件非标准的事情，很难用特定的标准方式去判断一个人的能力。看哪些方面能力、各方面能力如何衡量、最终层次划分到什么程度，这些都不是本文讨论的内容。以通过各大厂面试并顺利拿到offer为诉求，我们需要搞清楚能力分层，就需要先了解各大厂的层级情况。由于作者能力和视野原因，仅讨论国内情况。

国内公认的层级体系首当阿里系，通过公开资料可以知道阿里层级体系分为14级，其中又分为P（专家）序列和M（管理）序列，两个序列有一对一对应关系。因此我们仅讨论P序列。

层级分布情况，各大公司的层级分布并不是正态比例的。有点像政府单位，绝大部分是科员（工程师）、科长（高级工程师）和处长（专家），再向上人数就极度减少。





* 详细各公司职称对照可参照 SalaryFly <https://salaryfly.com>, 对标 <http://duibiao.info> 。

不同层次能力要求

以下为我个人定义，非官方描述。

- P5（工程师），绝大部分的校招本科和研究生会是这个层级，能力要求为上章讲到的三个点，基础扎实、兴趣驱动、有一定结果。工作职责上一般负责某个功能点，主要是完成各种交代的明确任务，以点为主。
- P6（高级工程师），一般为校招博士，或极优秀的本科或研究生。社招工作经验3-5年。能力差别上已不再是基础扎实，而是要很突出。工作职责上一般为某个系统的独立负责人，能够辅导带领工程师工作，以线为主。
- P7（专家），校招里的凤毛麟角。社招一般为10年工作经验以内的。有一定的深度，能够系统性思考。工作职责上一般会负责某个细分方向，能够虚线带领同学解决一些有挑战的问题，以面为主。
- P8（高级专家），校招不可能到达此层级，社招一般10年以上工作经验。具备深度和广度，有系统性思考和架构设计能力，对相关上下游领域都有深刻认识。一般为该行业综合能力极强的人。工作职责上一般会负责某个大方向或领域，实线带领团队，体系化建设，深度广度都有较高，以体为主。
- P9（资深专家），已经不看年限了，不是努力就能达到的位置。具备深度、广度和高度，为行业某一领域作出了突破性影响。一般为该行业技术能力最顶尖的人，工作职责上一般为大厂某条业务线安全负责人或某个大方向安全负责人。行业内大家耳熟能详的人大都处于P8和P9之间，比如猪猪侠。
- P10（研究员），已经不看年限了，不是努力就能达到的位置。能够布局未来，创造机会改变行业格局。一般为这个行业综合能力最出色的人（个位数），比如前端的玉伯、云计算的褚霸、安全的道哥。

优秀的简历是怎么样的

简历是一切的开始

在以前我对于如何写好简历并不是很在意，觉得信息写全了就够了，重要的是自己的实力，因此并未在简历上下太多功夫。直到我成了面试官，看了太多太多简历后，绝大多数人的简历简直是惨不忍睹。好的简历能让面试官看的时候就心里给你Offer了，差的简历面试的机会可能都没有，哪怕你真的很有实力。这好像是IT从业人员的同病，也许代码写的很好，但简历或者PPT一般都是一塌糊涂，对于怎么写好简历并没有什么研究。

面试季的时候，面试官会收到大量的简历，他需要快速的筛选简历判断是否适合岗位要求，在你的简历也许只扫了一眼，就会对你有一个初步看法。接下来再粗略看下每部分内容，就会决定评估不通过或是心里默许你肯定能拿到Offer。

简历基本要求

- **使简历看起来舒服**，赏心悦目在任何领域都是一大优势，整体要简洁明了，逻辑结构清晰。
- **确保信息真实性**，尤其是工作经历、学历、日期、职级等信息，现在入职背景调查是很普遍的事情，一旦提交简历和后续背调不符，基本与这份工作就无缘了。
- **确保基本信息都有**：包括姓名、ID、性别、年龄、教育背景（毕业院校、专业、时间）、联系方式、期望地点。不要期望面试官来问你没填的基础信息，这样你只会丢失这个面试机会。
- **不要有基础的错别字**：你在简历上下的功夫侧面在面试官眼里也体现你做其它事情的细致程度，错别字都有就明摆着告诉面试官我是个很粗心的人。
- **拥有更多的加分项，成为那个亮眼的仔**
  - 使用PDF、RTF格式，简洁不花哨；
  - 有GitHub并参与过开源项目，可以写一些自己做过的小项目放上去；
  - 有一些行业专业证书；
  - 参加一些行业比赛，获得好的成绩；
  - 参加一些行业会议，分享一些最佳实践；
  - 有个人博客，会写一些经验和问题的解决思路，一些深度文章等；
  - 邮箱使用gmail、foxmail或技术类邮箱（php.net）、私人域名邮箱等；

讲清楚你的价值，而非堆砌信息

这其实有点像工作中晋升时的述职答辩，面试官并不希望看到你做了各种大大小小的事情，而是关注你是否具备了下一层级能力。简历也一样，它的目的并不是告诉面试官你到底干了什么，而是你的价值是什么，他为什么要招你而不是别人。因此千万不要堆砌各种信息，让简历变得臃肿不堪或多无用信息，要想让面试官在其中发觉你的优势不如简洁明了的体现你的优势来的有效。

如何在这页纸上讲清楚你的优势，说服对方失去你是巨大损失。你历史的技术能力、做过的业绩、参加的比赛、作出的产品、参与的演讲等等是你能提供的价值基础。更关键的是你需要弄清楚对方缺什么，

突出你有什么而别人没有。

找专业的人给你的简历提意见

相信绝大多数人看完我前面的建议后，自己的简历质量会有所提升，但还是会有各种问题。所以建议最后一步是找一个专业的人给你的简历提提意见。相信我，看过上千份简历的人，只需要一眼就知道你的简历有什么问题。不要觉得麻烦别人，这种重要的事情上值得你去找他们帮忙，他会影响你的工作、薪水甚至你的职业生涯。

当然要注意，前提是你找到专业的人。不需要找文采好的，这不是写小作文。更不要找网上那种帮润色简历的人，他可能是找不到工作才做这行的，仅能找出一些细枝末节的问题或空而有理的建议。你需要的是现实中对他人简历起到决定性作用的人，这类人往往是本行业资深的专家或者招聘领域的资深HR，他们才是你的目标人选。身边没有也没有关系，可以问问身边的朋友有没有推荐的，尤其是你身边的朋友可能受过他的帮助。

简洁明了的简历模板

简历模版v0.1.pdf

点击下载源文件

- 📎简历模版v0.1.pages

安全招聘渠道

内部员工推荐

内推是优于招聘网站或猎头的，和找女朋友一样，熟人介绍的比媒婆介绍的要好，更不用说相亲网站的质量了。大企业内部大多数入职的人都是通过内推渠道进来的。对于中高端岗位公司需要支付较高的猎头费用，所以内推渠道优于其它所有。

- 找到自己倾向的公司以及对应的招聘岗位，注意岗位和个人技能及职业发展的匹配度
- 找到对应公司员工请求内部推荐简历，如果没有熟悉的人，可以通过feei#feei.cn联系我，可帮忙内推国内多数互联网公司

安全招聘网站

没有合适心仪的目标就上招聘网站。

- Freebuf <https://job.freebuf.com/> 安全行业垂直招聘网站
- 拉钩 <https://www.lagou.com/zhaopin/wangluoanquan/> 互联网垂直招聘
- Boss直聘 <https://www.zhipin.com/c101210100-p100407/> 和负责人一对一沟通
- 猎聘 <https://www.liepin.com/zpwangluoanquan/> 猎头招聘
- 智联招聘、前程无忧、LinkedIn、脉脉

安全面试经验

面试也是一项技能，可以去避免前人踩过的一些坑。

企业面试官考察点

了解企业考察逻辑，才能有的放矢。在企业视角到底需要什么样的人才？基础能力+成果+热情缺一不可。

- **基础能力**
  * 应聘者专业知识及技能，是否能胜任应聘岗位的要求?
  * 应聘者的学习能力，是否能快速适应和学习?
  * 应聘者价值观，是否与企业相匹配?
  * 应聘者认知接受能力，是否能承认错误并改进?
- **成果**
  * 略
- **热情**
  * 应聘者创造的欲望，是否有激情?

面试官往往会通过STAR面试法、行为面试法等方式来判断你过去做的事情的真实性和能力体现，以此来预判你之后的能力表现，了解这些面试方法能够帮助我们更加清楚面试官希望听到何种回答。

此外面试官经常会用到冰山模型来挖掘应聘者的能力、动力和潜力，对于表象的知识经验以及专业技能等可以培养的部分，只要达到基本要求即可，但对于潜在的态度、品质、动机等难以改变的部分会更加看重，必须满足。

面试官最终的判断依据其实会有很大感性部分，在如此短的时间内其实很难全面客观的评判。多数公司通用的录用判断标准往往是宁缺毋滥，凡是应聘者有明显缺陷都难以最终通过，除非特长特别明显。让面试官犹豫的人也容易被放弃，往往这类面试者是各方面比较平的，没有突出的亮点。

应聘者面试过程经验

提前准备

- 提前通过搜索引擎、朋友等渠道，尽可能了解所面试公司发展方向、业务模式、主要产品、公司文化、技术氛围、公开的文章、演讲、分享等信息。

- 针对面试的岗位需求以及自己工作经历准备一份简单的自我介绍，方便面试官快速准确的了解你的优点和综合素质。要能顺畅的讲出来，同时避免流水账。

- 面试官除了会看简历外，像GitHub、博客等可变内容应当提前整理维护下。

- 在日程或提醒事项中记录好面试时间、地点。

- 提前到达现场，有事情应提前电话沟通到位。

面试过程

- 自信并放松，友好的微笑，营造一个良好氛围。

- 不知面，如何被面。学习了解STAR面试法、行为面试法，能让我们更加清楚的描述做过的事情。避免使用大概、好像、很多等模糊字眼。

- 面试中的情绪控制。当面试官提出一些水平不高的问题时，应克制自己的不满情绪。

- 观察面试官身体语言。当面试官表现出兴趣时，应详细展开来讲。当面试官表现出没有兴趣时，应总结概括尽早结束该问题。

- 相互认同的作用。面试实际上就是双方互相交换意见的过程，作为候选人只有仔细聆听和适当提问，才能弄清楚面试官的真实意图。如果没有弄清真实意图的情况下就大谈特谈，是没有任何实际意义的，不必急于表达自己的观点，用提问的方式检验自己对面试官意图的理解。通过这个方式建立认同感后，才能更加自由的交换意见。

- 中高端岗位积极性的作用。往往参与应聘中高端岗位的面试者，其能力都比较好，可选择的公司也较多，因此往往会存在聊一聊的情况。此时若表现出对应聘岗位一定的兴趣，在其它条件相当时，企业会优先考虑，且有利于之后的薪水谈判。

- 面试时不透露公司敏感信息。

面试结束

- 表示对面试官的感谢

- 作为面试者，及时记录在面试过程中的不足点，针对不足点进行强化，下一轮面试中改进（往往不足点也会被面试官记录下来并让下一个面试官留意考察）

甄别团队和同事

前面章节有讲到如何选择企业，当企业符合自己期望后，并不代表企业中每个团队每个人都符合自己期望。尤其是在大公司里，各个团队的氛围、能力、价值观都会相差比较大。

在面试过程中，面试官往往是自己以后的同事、领导和HR，面试既是企业考察自己的过程，也是自己了了解”企业“的过程。理解面试是双向考察，面试官在面试我们的同时，我们也可以通过交谈、询问来观察面试官，去判断他的基础素质和专业素质，了解自己将在一个什么样的团队和一群什么样的共事。

其实完全用不上这么复杂的方式来实现这个目的，如果我们在目标团队中有认识的人就简单多了，他的长期感受会比短暂面试的判断要准确全面的多，通过向他们打听是最高效准确的办法。但更多的人是没有这方面人脉资源的，因此甄别面试官就显得尤为重要，在这里我会教大家一些判断面试官素质的经验。这里的经验侧重点并不是让我们去判断面试官的能力水平，而是让我们学会甄别那些不好的团队和人。

* 面试官时间管理经验判断，是否会提前预约面试时间、是否会准时参加面试、是否会控制面试过程避免面试者一直讲陷入细节从而超过常见面试时间等。

* 面试官面试经验判断，根据提问可以了解到其是否有提前了解自己简历中的一些信息、是否问的都是一些很简单的问题、问的问题前后没有逻辑像是模板一样一个个事前准备好的、是否通过预言方式来问问题（你会怎么做？你将怎么做？）等。

* 面试官基础素质判断，遇到自己回答不好的问题时面试官是否表现出不耐烦等负面情绪、面试官是否会无理打断自己、是否有审讯式的提问（往往通过咄咄逼人的方式提问，试图让面试者出现逻辑矛盾）、是否有质疑式提问（通过质疑、不相信的态度进行沟通，试图让面试者证明一切的真实性）、是否有打压式提问（一定要找到一些你不了解的方向但又问的特别多）、是否有高高在上（往往表现为轻蔑的语气）、是否能问出一些细节（而不只是夸夸其谈）。此处有个例外，资深的管理者往往有可能问一些低级问题，我们需要甄别面试官是真的基础素质不行还是非常资深但希望通过一些低级问题来反向考察面试者。

* 面试官技术能力判断，这个判断的前提是你是该领域专家，否则很有可能出现的情况是，其实是你没有领会面试官意图而觉得人家不专业的误判。当你对该领域很资深时，你能根据面试官的问题很容易的判断出来其对这个领域的技术水平和认知，甚至一些时候可以通过反向询问（慎用）来支撑你的判断。此外还可以通过了解目标企业的安全水位来判断他们安全技术能力程度。

* 面试官管理能力，这点非常重要，对于稍微高阶职位来讲，我们多数时候并不期望面试官中的管理者技术很强，更看重的是自己心底愿不愿意跟着他干，跟着他干是不是能有好的发展前途，是不是能有空间获得个人成长。

上面很多逻辑是一些大家都懂的道理，倘若没有准确的甄别出来，会导致你进入到错误的团队和错误的人共事，所付出的成本是极高的，同时自己会陷入巨大痛苦之中。你有可能遇到团队氛围不好死气沉沉、办公室斗争尔虞我诈、领导情绪不稳定骂人是常态、团队同学陷于日常繁琐事务没有成就、天天加班绩效也不好技术也没成长还看不到希望等。

基础素质问题

- 对前面几轮面试官的看法如何？（HR问题，考察对他人评价）

- 前几次面试中，你有了解到这个岗位的工作职责和目标要求是什么吗？（HR问题）

- 对于异地工作你是怎么考虑的？（HR问题）

- 离职原因？为什么这个阶段要裸辞？（HR问题）
  提示：不要有太多消极负面东西，点到为止。提及原公司看法时，应当客观正面，切勿有个人情绪，尤其避免对上司、同事的抱怨。

- 薪资相关问题（HR问题）
  提示：如果面试官未谈及薪资问题，切勿主动提及。回答薪资相关问题时，在保证自己基本利益的前提下，表达自己的诉求，但一定不要把话说死，给后续谈判保留空间。相信企业会给自己一个合理的回报。

- 遇到解决不了的问题怎么做？工作中遇到最大的挑战是什么，如何解决的？（考察学习能力和动手解决能力）

- 业余时间会干嘛？（考察技术热情）
  提示：真实表达。可从乌云、翻墙、写技术博客、参与开源、常浏览的网站、关于黑客电视剧、关注业内牛人等角度。

- 自认为自己比身边人的优势和不足是什么？（客观的自我评价，讲自己没有缺点的基本可以不要了。挖掘亮点，如何客观看待自己）

- 别人对你最负面的评价是什么？你自己如何看待？

- 最有成就感的事情？（考察价值观）

- 未来职业规划？也可以问长期和中短期规划各是什么？（长远思考）

- 还有什么要问我的吗？（了解面试者所关心的侧重点）
  提示：可以选择有关企业发展、所应聘岗位定位相关问题，让面试官能感觉到你在关心公司发展和岗位兴趣。避免问题过多过细，也避免没有问题。

安全面试题目

如何有效的甄别一些滥竽充数的人，最重要的肯定是面试这道坎。安全圈的东西行业内的人谁都能聊一点，所以一轮面试一定得一线安全技术负责人亲自把关，深入的问细节来判断。

但同时也建议根据实际岗位需求来平衡对候选人的要求，避免出现面试时问造火箭的技术，进来后拧螺丝钉。

应用安全岗位

漏洞挖掘、利用及修复

挑选两到四个不同方向常见和不常见的漏洞，就漏洞原理、利用方式和修复方案进行提问，然后根据回答的情况进行详细深入的二次提问。

常规应用漏洞

- ★★☆☆☆ Redis未授权访问漏洞如何入侵利用?
- ★★★☆☆ SSRF漏洞原理、利用方式及修复方案？Java和PHP的SSRF区别?
- ★☆☆☆☆ 宽字节注入漏洞原理、利用方式及修复方案?
- ★★★☆☆ 简述JSONP的业务意义，JSONP劫持利用方式及修复方案？如何设计落地一个CSRF Token?
- ★★☆☆☆ CORS原理、利用及修复?
- ★☆☆☆☆ CRLF注入原理?
- ★★☆☆☆ URL白名单如何绕过?
- ★★★☆☆ XSS持久化如何实现?
- ★★★★☆ Fastjson常见漏洞原理？如何彻底解决Fastjson漏洞?

业务逻辑漏洞

- ★★☆☆☆ **业务逻辑漏洞有哪些具体类型?**

提示：考察对业务逻辑的理解，如果只局限在越权则比较浅。凡是和业务比较贴近的漏洞都算业务逻辑漏洞，比如身份校验相关的风险（未授权访问、非正常账户态、身份可枚举、水平越权、垂直越权等）、接口逻辑实现不一致（不同协议实现不一致、同类产品不同逻辑、不同阶段逻辑不一致-流程绕过）、不安全的可信端数据（APP数据）、预设要求不符合（依赖条件不安全-业务校验属性设计、人工客服容易被骗-业务流程设计）、滥用合理业务需求等等。

- ★★☆☆☆ **哪些账户状态会导致预期外的风险?**

  提示：此题考的是当账户状态改变时，由于各个业务逻辑并不一定严格遵循该账户状态的要求导致的还可以继续进行一些预期外的操作。一般账户状态在注销、禁用、风控、司法冻结等时候，会出现该问题。

- ★★☆☆☆ **身份标识明文传输会导致什么风险?**

  提示：伪造他人身份态。

- ★★★☆☆ **水平越权触发点会存在哪些位置?**

  提示：Cookies、自定义Header、URL Path、URL Param Value、URL Param JSON、Body Form、Body JSON、Body XML、自定义协议的自定义字段等等。

- ★★★☆☆ **水平越权有哪几种检测方式?**

  提示：一般针对数字类型的越权可以通过递增枚举数字，根据响应情况可以判断是否存在越权。此外还可以通过两个账号相互访问对方创建的资源来判断，可避免不连续的数字导致的遗漏。

- ★★★★☆ **某个APP的某个功能按钮是灰色不可用状态，如何绕过其限制?**

  提示：除了修改按钮属性使其可用或分析灰色功能对应的后端接口，直接调用接口外。如果能考虑到不同协议的实现可能不一致就更加全面了，比如APP上不能用，PC上是否就能用了，PC也不能用，通过各种协议（HTTP、WSDL、REST、GraphQL）的API调用是否能绕过。

- ★★★★☆ **流程绕过漏洞如何抽象理解归类?**

  提示：流程绕过漏洞可以理解为不同阶段逻辑实现不一致，比如创建和后续状态变更时的要求不一致（一个操作创建时权限校验很严格，结果修改的时候的权限要求却不一致）、一个流程某个步骤的要求不一致（第一步要输入密码，结果第二部下单的时候并未强校验前面输密码是否完成）、并发逻辑控制（开多窗口同时支付，使一个优惠多次使用）、特殊时期的逻辑绕过（大促时期的校验机制降级）等等。

常用协议漏洞

- ★★★☆☆ TLS1.2协议交互过程以及攻击方法?

- ★★★☆☆ 若对OAuth的redirect_uri进行了白名单限制，有哪些可能绕过的方式?

- ★★★☆☆ JWT相较于SESSION优劣势?

漏洞测试软性能力

- ★★★★☆ 哪些漏洞的测试对业务有损？如何避免?

- ★★★★☆ 你之前没接触区块链/云原生/算法安全，现在需要你评估某个使用该技术的业务安全性，你会如何做?

漏洞处置

- ★☆☆☆☆ 漏洞修复一般分为哪几个步骤?
- ★★☆☆☆ 如何制定漏洞的修复时间？需要考虑哪些因素?
- ★★★☆☆ 如何有效提升漏洞修复效率?
- ★★☆☆☆ 漏洞复盘的关键是什么?
- ★★★☆☆ 如何快速有效推进修复外部厂商的漏洞?
- ★★★★☆ 外部白帽子发现某个高危漏洞，但完整修复需要多天，安全产品的止血手段不彻底，你该如何处置?

漏洞自动化发现

白盒SAST

- ★★★☆☆ 当前阶段，人工和自动化的代码审计差异点在哪里?
- ★★★☆☆ 什么类型漏洞是代码审计无法准确判断存在与否的?
- ★★★☆☆ 密钥的识别的正则如何写?
- ★★★☆☆ 正则`(a+)+`会存在什么风险?
- ★★★☆☆ 程序对读取的文件名的正则为`/\.markdown/`，如何绕过?
- ★★★☆☆ 程序对请求的URL的正则为`/^http\:\/\/.*\.paipai.com($|(\/[^<>\'\"]*))/`，如何绕过?
- ★★★☆☆ 解释型语言和编译型语言在语法树分析上有什么差异?
- ★★★☆☆ Java Web应用中的反序列化漏洞的Source和Sink是什么?

黑盒DAST

- ★★★☆☆ 黑盒如何检测XSS漏洞?
- ★★☆☆☆ 甲方黑盒是否应该有爬取流量功能?
- ★★★☆☆ 黑盒如何扫描无法出网的SSRF?
- ★★★☆☆ 黑盒如何扫描越权漏洞?
- ★★★★☆ 黑盒带登录态扫描如何规避业务影响?
- ★★★★☆ 黑盒扫描时如何避免被反制?

灰盒IAST

- ★★★☆☆ 灰盒相较于黑白盒的优势是什么?

安全评估与解决方案

安全评估

- ★★★☆☆ 安全评估到底要评什么东西?
- ★★★☆☆ 某些场景（登录、注册、修改密码、支付）会存在哪些风险以及如何防范?
- ★★★☆☆ 新应用如何评估安全风险?
- ★★★☆☆ 需求阶段、系分阶段安全评估的侧重点是什么?
- ★★★☆☆ 接口B的参数是从接口A的响应中获取的，会存在什么风险?
- ★★★☆☆ 新的API接口上线时，如何设计使其避免出现请求篡改和请求重放?
- ★★★☆☆ Docker容器以及K8s有哪些风险?
- ★★★☆☆ IPv6和IPv4安全差异?

- ★★★☆☆ 三方引入的应用和自研应用评估差异有哪些?
- ★★★☆☆ 金融业务有何特色?
- ★★★☆☆ mvn源的安全性需要考虑哪些点?
- ★★★☆☆ 如何让业务方主动找你评估?
- ★★★☆☆ 如何判断评估覆盖范围的优先级?
- ★★★☆☆ 如何降低各人检验导致评估不一致?
- ★★★☆☆ 如何系统提高安全评估效率?
- ★★★☆☆ 安全评估和人工测试以及自动化测试三者差异是什么?
- ★★★☆☆ 算法模型的安全风险如何评估?
- ★★★☆☆ 区块链安全风险主要有哪些?
- ★★★☆☆ 如何理解安全左移?
- ★★★☆☆ 安全评估的行业最佳实践是什么?
- ★★★☆☆ 如何看待未来安全评估的趋势?

安全方案

- ★★☆☆☆ 如何规避绕口令带来的风险?
- ★★☆☆☆ 硬编码密钥如何系统解决?
- ★★★★☆ 0day漏洞如何防御
- ★★★☆☆ GitHub等三方泄漏敏感信息如何体系防御
- ★★★★☆ 业务逻辑漏洞如何通过技术手段避免写出来?

- ★★★★☆ 软件供应链后门和漏洞如何系统规避

移动应用安全

- ★★★☆☆ App自检升级场景下会存在哪些风险?
- ★★★☆☆ 如何设计一套通信机制，能够保证传输过程中的完整性、不可抵赖性以及防止重放?
- ★★★☆☆ 如何进行实体检测?
- ★★★☆☆ 常见的调试方法和检测方法?
- ★★★☆☆ 如何防止Frida、Xposed等注入攻击?
- ★★★☆☆ 如何防止当前设备的数据拷贝到其他设备?
- ★★★☆☆ 外挂有几种类型的实现方式?
- ★★★★☆ 如何避免未经用户授权获取权限?

网络主机安全岗位

- 主机最重要的基线是什么?
- 禁止出网的价值有哪些?
- 如何对网络区域进行划分?
- 云原生下的网络和主机差异是什么？会有哪些新的风险?
- 如何解决员工被钓鱼问题?
- 如何解决员工通过电脑或手机外发公司敏感文件?
- 经典网络与VPC的优劣势
- 如何实现反向HTTPS代理
- DDoS/CC如何有效防御与应急?
- 如何通过技术手段避免非预期端口开放?
- 容器存在哪些特有安全风险?
- 运维白屏化的难点是什么?

威胁应对岗

威胁安全认知

- ★★☆☆☆ 你觉得事前建设和事中威胁感知的投入比例应该是怎么样的?
- ★★★☆☆ WAF是基于攻击特征黑名单的方式，也就不断会存在绕过和遗漏，它存在的意义是什么?
- ★★★☆☆ 如何衡量威胁感知能力强弱?
- ★★★☆☆ 感知规则的有效性如何系统验证?
- ★★★★☆ 未感知部分如何衡量?

流量采集与清洗

- ★☆☆☆☆ 威胁感知可以在哪些层面进行?
- ★★☆☆☆ TCP协议的流量要储存哪些关键字段?
- ★☆☆☆☆ 如何在服务器上抓取HTTPS流量进行分析?
- ★★☆☆☆ 清洗流量时可以通过哪些方式降低无用流量?
- ★★☆☆☆ 清洗流量时可以通过哪些方式降低无用流量?
- ★★☆☆☆ 清洗流量时如实现URL的去重?
- ★★★☆☆ 清洗流量时如何剔除攻击流量?
- ★★★☆☆ 清洗流量时可能会导致哪些潜在的安全风险?
- ★★★☆☆ 清洗流量时如何识别新增接口?
- ★★★★☆ 如何实现近实时风险处置?

风险识别与应对–网络侧

- ★★☆☆☆ 常见的C&C通道种类和特征?
- ★★★☆☆ 如何在加密流量中检测出恶意流量?
- ★★★☆☆ 如何识别异常服务器外联?
- ★★★☆☆ 基于网络五元组可以做到哪些风险行为的分析?

风险识别与应对–主机侧

- ★☆☆☆☆ 主机有哪些日志对风险识别有帮助?
- ★★☆☆☆ 抽象来看主机中有哪些后门实现方式?
- ★★★☆☆ 一个黑客入侵主机后植入了一个木马，并擦除了各种日志，如何找出其如何入侵的以及入侵后做了什么事?
- ★★★★☆ 某个黑客入侵主机后，拿到了root权限，如何止血?
- ★★★★★ 感知到黑客入侵了所有服务器，怎么办?

风险识别与应对–应用侧

- ★★☆☆☆ 应用相关有哪些数据可以用作威胁分析?
- ★☆☆☆☆ 如何准确识别域名探测?
- ★☆☆☆☆ 如何准确识别端口探测?
- ★★☆☆☆ 如何准确识别文件遍历探测?
- ★★☆☆☆ SQL注入拦截规则如何实现?
- ★★★☆☆ 如何实现页面篡改感知?
- ★★★☆☆ 如何实现页面挂马感知?
- ★★★☆☆ 如何确保上线的拦截规则不出现误拦截?
- ★★★☆☆ 如何识别公共和私有接口?

- ★★★★☆ 如何识别机器行为请求?
- ★★★★☆ 如何感知越权风险?
- ★★★★☆ 如何识别攻击请求是定点攻击还是随机扫描?
- ★★★★☆ 专家检验无法覆盖的风险如何检测?
- ★★★★☆ 有哪些类型应用层风险是无法在流量层较好感知的?
- ★★★★★ 如何识别客户端的系统真实类型?

威胁溯源

- ★★★★☆ 接到客户投诉，其收到诈骗电话，骗子能准确说出他在我们平台购买的商品名称、订单号、收获地址和时间信息，请问如何排查该信息泄漏途径?
- ★★★★☆ 内网论坛的截图的内容突然出现在了外部新闻网站，有多少种溯源方式?
- ★★★☆☆ 内网某台没有公网地址的服务器突然CPU异常标高，经排查发现是因为cat了某个大文件导致的，但服务器相关人员都说没有操作过，请问如何溯源出谁操作的?

威胁情报

- ★☆☆☆☆ 企业会面临哪些外部风险?
- ★☆☆☆☆ 有哪些可以收集的情报渠道?
- ★★☆☆☆ 如何快速筛选出最新的CVE对我们是否有实际影响?
- ★★☆☆☆ 爬取暗网内容是否违法?
- ★★★☆☆ 如何准确识别Telgram群里和我们公司相关的情报?
- ★★★☆☆ SaaS类情报产品的联防联控机制的缺点是什么?
- ★★★☆☆ 给定一个网站，如何自动化识别其是否钓鱼网站?
- ★★★☆☆ 如何识别仿冒APP?

- ★★★★☆ 如何识别一个没有登陆的用户的真实身份?
- ★★★★★ 如何找出对我们业务实施网络攻击的黑客真实身份?
- ★★★☆☆ 国内和国外攻击特点有什么区别?

数据安全岗

安全责任与意识

- 如何系统性提升员工安全意识?
- 如何做到针对性的安全意识提升?
- 如何衡量员工安全意识?
- 什么是安全责任制？如何落地安全责任制?

数据采集使用

- 数字水印的类型和应用领域?
- 隐藏水印有哪些实现方式?
- 如何对无显著特征的数据进行分类分级?
- 如何避免员工因非工作需要查询用户数据?
- 如何避免未经用户授权收集用户数据?
- 如何避免用户数据被超范围使用?
- 何时应该进行用户数据销毁?
- 更换机房时如何清除原机房机器数据?
- 如何让每一次后台查询数据都得到用户授权？or 如何收敛管理后台可查询任意敏感信息功能?
- 如何在不拿到明文数据的前提下，还能通过数据进行一些计算行为？如何实现合作伙伴原始数据不共享但能达成业务诉求?

权限

- 如何避免审批工单无脑通过?
- 高危害影响权限如何避免滥用?
- 如何技术手段规避未进行权限检查?
- 大数据平台的权限管控体系中最重要的是什么?

加解密

- 哪些Hash和加密算法不建议使用?
- 硬编码秘钥如何解决?
- PKI原理
- 国密的底层原理?
- 密码如何保存在数据库?
- 如何让密码轮转?
- 内网传输是否需要加密?
- 可以在哪些层次对文件进行加密?
- 如何技术手段实现全站HTTPS

合规审计岗

- 国内外有哪些网络安全相关法律?
- 金融行业和传统互联网行业合规差异
- 对于内控、合规、审计的理解（考察其对于要做的事情和岗位要求、公司环境是否匹配，考察其大局上考虑是否周全或是片面）
- 传统行业和互联网行业的安全建设的区别及各自的优劣势（是否能准确的抓住核心原因）
- 信息安全等级保护、网络安全法、GDPR，挑选一到两个问其对其的来源理解以及落地程度取舍
- 数据安全治理可以用什么思路做?
- 如何通过技术手段实现对异常操作的自动化监控?
- 如何对一个应用进行安全评估?
- 如何对一个应用进行安全审计?
- 如何理解权限分离、最小化权限?
- 考察一些CISP、CISSP的知识点
- 挑选一些较为复杂的流程，比如转岗、离职等，如何设计考虑其中的细节

安全蓝军岗位

蓝军认知

- ★★★★☆ 安全蓝军和常规渗透测试的差异是什么?
- ★★★★☆ 蓝军如何体系建设?
- ★★★☆☆ 如何在有限的人力下最大化突出蓝军价值?

信息收集

- ★★★★☆ 域名爆破中，泛域名解析问题如何解决?

攻击入口

- ★★☆☆☆ 各种常见木马的的优劣势?
- ★★★☆☆ 木马免杀有哪些方式？哪种方式最有效?
- ★★★☆☆ 木马隧道有哪些？哪种隧道在当前最有效?
- ★★☆☆☆ Word DDE和Office宏有什么优劣势?
- ★★★☆☆ 如何绕过Office受保护视图?
- ★★★☆☆ 有哪些有效的钓鱼方式?
- ★★☆☆☆ 如何绕过WAF、HIDS、威胁感知，选其一回答?
- ★★☆☆☆ BadUSB原理及局限?

出网

- ★★☆☆☆ 如何在禁止出网的机器上访问互联网?
- ★★☆☆☆ ew、frp差异?

- ★★☆☆☆ ICMP如何出网?
- ★★☆☆☆ 如何进行水坑攻击?
- ★★☆☆☆ 如何利用XSS让影响最大化?

行为

- ★★☆☆☆ 如何全流程最大限度降低被红军发现概率?

安全开发岗位

Java基础

- ★★☆☆☆ Java虚拟机区域如何划分?
- ★★☆☆☆ HashMap和HashTable、ConcurrentHashMap的区别?
- ★★☆☆☆ 进程和线程区别，进程间、线程间通信有哪几种方式?
- ★★★☆☆ Java BIO/NIO/AIO是什么？适用哪些场景?

业务基础

- ★★☆☆☆ 调试工具及异常排查流程?
- ★★☆☆☆ 如何最大限度避免故障?
- ★★☆☆☆ 数据库索引结构，什么情况下应该建唯一索引?
- ★★☆☆☆ 数据库分页语句如何写?

业务安全

- ★★☆☆☆ HTTPS交互过程
- ★★★☆☆ OAuth2.0交互过程及其中可能存在的配置不当安全风险
- ★★★☆☆ 对称加密和非对称加密的区别及优缺点
- ★★☆☆☆ 获取一个入参url，请求url地址的内容时应注意什么?
- ★★☆☆☆ 参数入库前应该如何过滤?
- ★★☆☆☆ 过滤器和拦截器原理和应用场景?

- ★☆☆☆☆ SESSION ID如何不被Javascript读取?
- ★★★☆☆ CSRF的Token如何设计?
- ★★★☆☆ 同源策略? 如何实现安全的跨域请求?

安全管理岗

安全架构方向

- **回答各方向四星以上的问题**
- 传统IDC、云上、混合云架构的安全差异和各自挑战是什么?
- 纯云业务如何设计安全架构?
- SDL中的关键点是什么以及如何解决?
- 如何防止0day攻击?
- 渗透测试、安全研发、安全运营的问题可以挑选的问一些，以确保在各个方向上比较均衡
- 对于企业不同时期、不同阶段、不同体量的安全建设的方法、区别以及侧重
- 你所做过的安全架构图和所期望的安全架构
- 安全与其他团队（运维、研发、测试、GR/PR、内控、高管及三方安全公司）的关系
- 安全建设的理念/方法论理解，纵深防御、白名单和黑名单、规则经验和机器学习、自研或者外采
- 如何制定安全的衡量指标？如何衡量企业安全建设的水平?
- 如何避免出现各种各样的惊喜？比如资产没覆盖、扫描器规则没写好、出异常了等等各类情况
- 不同公司间的安全区别或差别是什么？比如腾讯和阿里，百度和京东
- 如何制定公司安全建设的三年甚至五年计划
- 未来安全行业趋势?

安全笔试题目

渗透测试-Web方向

- 给定一个漏洞靶场，在一定时间内找出最多漏洞数
- 给定一个匿名访问Redis，请GET SHELL
- 给一个项目场景进行安全评估（e.g.与三方厂商进行API交互）
- 给定一些包含漏洞（建议SSRF、反序列化、营销活动）的代码，使其发现漏洞或风险、利用漏洞、修复漏洞

软件开发方向

- 读取一个文件第100-200行并发送到一个指定的API接口（着重考察对于各种异常情况的考虑）
- 最快的方式获取100万个子域名请求的响应内容并找出其中真实存在的子域名
- 待补充@TODO

安全行业人才趋势

IT转向DT、万物互联和地缘政治摩擦的大趋势下，无论是国家、企业还是个人层面，安全将前所未有的被广泛重视。各类细分安全法律、监管要求、行业标准出台，个人隐私保护意识崛起，产品的安全性也逐渐成为各企业的竞争优势。随之安全岗位需求将越来越多，安全从业人员数量也大幅增长，安全对抗的深入导致安全细分领域越来越多。

这些意味这什么呢？在我接触安全那会，多数安全从业者都能凭借着兴趣爱好就能在行业内做的不错，先发优势让我们很容易做出一些成绩，甚至跨子领域的成绩。但参加最近几年的校招能明显的感觉到越来越多的专业精深的安全人才，已经逐渐脱离了仅依靠兴趣爱好就能做好的时代。

作为新人我们应该把握好这个历史时机，打好安全基础、深入研究新型领域、快速学习他人经验、把握每一次成长机会、扩大安全影响力，安全的未来是你们的！