网络安全面试指南 By FEEI

一、网络安全现状

1.1 理解网络安全行业现状

行业处于起步阶段@2019

从业人员薪酬高

从业人员良莠不齐

安全水位难衡量

安全建设驱动因素转变中

安全圈子文化氛围浓厚

学历相对不重要@2019

1.2 安全从业人员如何选择公司

业务对安全是否强诉求

优先选择互联网行业

甲方好于乙方，公司赚钱才能更容易高薪

钱和成长兼得

文化氛围至关重要

岗位契合度是重中之重

反向调查公司

1.3 安全从业人员必备素质

基础：渗透测试和软件开发

热情：兴趣驱动是最长久的

成果：没有结果的优秀是空谈

其它：优秀特质越多成长越快

1.4 安全从业人员能力分层

业余安全爱好者

安全工程师

高级安全工程师

安全专家

高级安全专家

资深安全专家
安全研究员
安全领袖
二、安全面试经验
2.1 安全招聘渠道
内部员工推荐
安全招聘网站
高阶岗位另辟蹊径
2.2 如何优化简历让你在应聘者中脱颖而出
简历是一切的开始
简历基本要求
讲清楚你的独特价值，而非堆砌信息
找专业的人给你的简历提意见
简洁明了的简历模板
2.3 一些通用安全面试经验
企业面试官考察点
校招与社招考察点
软性考察点：可以有缺点，但不能无法改变
面试方法
STAR面试法
行为面试法
压力面试法
应聘者面试过程经验
提前准备
面试过程
面试结束
理解背后的意思
甄别岗位、团队和同事
三、网络安全面试题目
3.1 基础素质问题
3.2 安全面试的本质
应用安全面试题目

安全运营
- 安全理念
- 安全意识
- 安全规范
- 安全评估
- 安全解决方案

安全资产

渗透测试
- 常规漏洞
- 业务逻辑漏洞
- API安全
- 协议漏洞

业务风险

算法安全
- 加解密

供应链安全

安全扫描器
- IAST
- SAST
- DAST

应用安全防护
- RASP
- WAF
- 安全头
- 修复组件

漏洞处置
- 漏洞管理
- 应急响应
- NDAY情报

其它应用类型

前端/移动端安全

基础设施安全面试题目

零信任
网络与主机
办公设备
威胁感知与响应面试题目
威胁安全认知
流量采集与清洗
人机识别
风险识别与应对-移动端
风险识别与应对-网络侧
风险识别与应对-主机侧
风险识别与应对-应用侧
威胁溯源
威胁情报
数据安全面试题目
安全责任与意识
数据采集使用
权限
数据安全综合
安全合规面试题目
安全合规
安全蓝军面试题目
蓝军认知
信息收集
漏洞原理
攻击入口
出网
行为
安全开发面试题目
JAVA基础
网络与多线程
数据结构与算法
业务基础

业务安全
安全管理面试题目
安全认知
组织架构
安全架构体系
四、网络安全行业趋势

https://feei.cn/sig/

本指南旨在为网络安全领域从业者提供一份全面的面试指南。我将从行业、企业和从业者的角度来介绍当前情况，分享面试和招聘经验。指南将围绕各个细分安全领域的体系、实用且高质量的题库和思路提示展开，以便你能够更加全面系统地理解和吸收各种经验。

在指南中，我将以面试者的视角全流程地讲解面试过程。此外，我还将穿插企业、HR和技术面试官的视角，以便你能够更好地理解和适应各种面试环节。核心题库将不断更新，增加新的题目、调整题目难度，并根据时效性剔除不合适的题目。所有题目都来源于真实工作经验，以确保能够真实地反映应聘者的能力水平。

我希望通过这篇指南能够为你提供帮助，让你在面试中更加游刃有余。如果你有任何问题或想要进一步交流，欢迎在评论中提出。我会及时回复你的留言，谢谢！

一、网络安全现状

1.1 理解网络安全行业现状

行业处于起步阶段@2019

现代网络安全行业发展的时间相对较短，许多企业由于资源投入和建设时间限制，导致安全建设的广度和深度还有挺大提升空间。甚至一些国内大厂的安全水平可能并不如我们所想象的那样高。很多企业的安全水平仅能够对抗一些初级白帽子级别的攻击，而面对专业的黑客团伙持续定向攻击，大多数企业则无法有效防御。在HW以及各家SRC的数据中能反应出目前的安全状况。

从业人员薪酬高

由于安全行业起步较晚，安全人才供不应求，导致安全从业者的薪资水平不断攀升。在所有行业中，互联网行业被公认为薪资最高的领域之一，而在技术类岗位中，安全工程师的薪资水平更是普遍高于其他技术人才，与当前发展迅猛的AI行业能一较高下。优秀的信息安全本科毕业生可以获得每月2万到3.5万的起薪（当然这里可能受到行业内部竞争的因素影响，一些公司采用入职即巅峰的招聘策略，后续薪资增长有限）。努力工作三四年后，薪资可能达到每月4万到6万。成为安全团队的管理者后，年薪可达百万水平，成为行业顶尖人才后，年薪可达千万（后面章节中，会解释不同薪资水平对应的能力结构需求）。随着越来越多的学校开设信息安全相关专业，越来越多的培训机构提供信息安全课程，以及越来越多的人选择学习或转行从事信息安全工作，整体安全人才供需状况将会得到改善。

从业人员良莠不齐

安全行业的迅速发展带来了一些利好，例如吸引了更多人加入安全领域、整体安全水位明显提升。然而，这也带来了一些明显的不利因素，比如人员紧缺和急需填补的岗位。这导致了许多能力参差不齐的人涌入行业，他们的明显特征是在技术细节方面无法进行深入交流。当你谈论技术细节时，他们只会谈论行业热点；当你谈论行业热点时，他们只会谈论合规套话；当你谈论监管合规时，他们只会谈论行业八卦。更甚者，他们可能只是照搬理论而并未深入理解就拿来卖弄。尽管这么说可能会得罪一部分人，但这是目前存在的现实。有人会问，难道入职后他们的真实水平不会暴露吗？在老板非技术人士前提下，很难察觉到。主要原因是前面提到的安全水位很难衡量，而实际的安全风险通常是小概率事件。在许多情况下，运气成为了实现目标的关键因素。

安全水位难衡量

很多情况下，我们可以通过结果来判断安全建设的水平，但在安全领域，这种判断变得困难。许多团队的绩效指标是”零安全事故”，也就是不出现任何安全问题。这种指标导致了吹嘘拍马的人混的风生水起。然而，随着实战红蓝演练的普及以及国家级别实战攻防演练的规模和范围扩大，逐渐借助模拟实战的方式来评估防护和应急的效果。这种趋势在一定程度上有助于改善上述情况。

安全建设驱动因素转变中

在早期，安全是个奢侈品。仅在金融、电商、游戏等少数行业存在，它们都面临着黑灰产的威胁，对安全有天然的需求，属于实际业务安全威胁驱动安全建设。在前些年，陆续各类安全法律、法规、标准出台，许多企业开始了满足合规要求而进行安全建设，甚至有些企业会购买大量安全产品，但只是为了应付监管检查而不真正使用这些产品来提升安全水位。随着乌云等公共漏洞报告平台的兴起，各家企业的安全建设又上了一个台阶，这种模式属于白帽子安全漏洞驱动。在最近几年的行业中，由于国家攻防演练的普及，行业风气逐渐变得更加务实，并且逐渐演变为由实际风险驱动的安全。

安全圈子文化氛围浓厚

安全领域是一个小圈子，圈内的事件传播非常迅速。例如，哪家企业的数据库泄露了、哪家企业遭受了薅羊毛行为、哪个安全专业人士被抓等负面新闻，圈内人很容易得知。同样，在这个小圈子里，人们可以快速了解行业中的新技术、新方向和新政策，也能轻松获悉每家公司的安全建设情况。你可以了解到阿里安全与公安部门合作的强大手段，了解腾讯的安全响应中心如何运作得如此出色，还可以与百度的安全专家讨论如何将机器学习应用于安全产品。在安全圈内，这些交流都非常容易实现。此外，众多安全会议的举办也使你能够学习到每家公司的经验，无需自己摸索。这些都是小圈子的好处。

当然，小圈子也存在明显的弊端。总有一些人追求所谓的“圈子文化”，他们经常参加各种安全会议，主动结识圈内人（这里并不是指SRC运营同学，他们的工作本来就是去结识不同公司的人）。往往以自己认识谁、和谁熟为荣，不断形成各种更小的圈子（往往都是同一批人），很难看到开放、包容和共享。

学历相对不重要@2019

安全圈内存在许多没有学历或学历较低的牛人。这些人可能年龄较小，工作经验也不长，但他们通常是出于兴趣驱动，早期就投入了大量时间和精力在安全领域。因此，他们在安全方面取得了显著的成就。当他们的长处特别突出时，往往能够突破企业对学历的一些要求限制。例如，在岗位学历要求为本科学历时，候选人出色的安全能力可以降低对学历的要求。

然而，我们也必须正确认识低学历对工作的影响。在当前安全行业逐渐细分、安全建设越来越深入的趋势下，安全从业者不再只需要擅长挖掘漏洞。随着越来越多的院校开设信息安全专业，越来越多的人进入安全行业。未来企业在招聘安全人才时，学历要求肯定会像其他行业一样成为基本筛选要求，以降低招聘成本。因此，我建议低学历的候选人可以尽早通过自考等方式系统学习英语、数学、计算机基础等学科，并获得国家认可的成人教育学历。这样，学历问题的影响就不再成为问题。

1.2 安全从业人员如何选择公司

我们都知道选择比努力重要。在人生中，我们不断面临大大小小的选择，而选择下一家公司则是其中最重要的之一。这个选择将关系到你未来几年甚至整个职业生涯的成功与否。不论是技术能力、管理经验、薪资水平，甚至与另一半的关系，都会受到这个选择的影响。选择一家合适的公司将让我们在接下来的几年里获得事半功倍的成长。

业务对安全是否强诉求

在选择公司时，如果只保留一条原则，最关键的一点是要考虑公司业务对安全的强诉求程度。

那么如何判断公司业务是否对安全有强烈的需求呢？从安全的角度来看，几乎所有公司都有敏感数据，都会提供网络服务，都需要安全人员来保护。然而，实际情况往往并不像我们期望的那样，尤其在公司快速发展的情况下。在业务对安全非强诉求的公司中，安全部门往往被视为支撑部门，一旦公司面临困境需要裁员时，安全部门往往是首先被裁减的部门。同时，从资源投入的角度来看，这类公司对安全的投入相对较低。

一般来说，那些管理大量资金或数据的公司对安全有强烈的诉求。这些公司也受到政府监管，安全被要求成为必备部门，比如大型互联网公司和金融行业。或者哪些容易拿到投融资的新型行业，比如新能源、AI等。**这些行业的公司赚钱相较于其它行业更加容易，这也导致加入这些公司更容易拿到高薪。这些公司通常非常重视安全，并愿意持续、大量地投入资源。对于从事安全行业的人来说，这意味着我们可以更深入地更长期地从事更具挑战性的工作。**

优先选择互联网行业

从行业历史发展的角度来看，计算机无疑是发展最快的行业之一。尽管近年来受到996工作制、价值观冲突、裁员、反垄断等负面事件的影响，但我们不能否认计算机行业仍然是一个朝阳行业，发展趋势持续向好。这一切的核心在于计算机技术的边际成本可以降低到近乎为零的程度，只需要几十人就可以服务几百上千万人，同一份软件可以卖出一百份而成本差异并不大。同时，随着万物互联的发展，计算机技术的应用范围也越来越广泛，从最开始的计算机，到手机、电视机、音箱，再到汽车、商店甚至工厂机器人，计算机的渗透程度越来越高。可以预见，计算机行业将继续不断地进化。

相比之下，在传统行业工作五年后，人们的情况并不会有太大的差别。然而，在互联网行业，你永远无法想象自己五年后会是怎样的。互联网行业给予了你无限的可能性。二十多年前，我家里开了一家服装加工厂。除了在我还小的时候，那时服装产业非常火热，工厂赚了一些钱外，就再也没有取得太大的发展。其他一些开厂的亲戚朋友也没有赚到什么钱，反而是通过卖掉厂房赚了不少钱。在这些工厂中，无论是一线专业工人或管理者，他们的投入产出和工资增长速度是无法拿来和计算机行业对比的。我的哥哥是一名公务员，很多人都会羡慕他的工作轻松稳定，但工资的涨幅和职位的升迁都是可以预料到的，职业空间的发展有限，并不是每个人都能接受的。

甲方好于乙方，公司赚钱才能更容易高薪

互联网行业可以分为甲方和乙方。由于乙方主要以销售为导向，所以在员工的技术深度和薪资水平上相对甲方会有明显差距。同时，由于乙方赚钱都不那么容易，对支出比较敏感，普通员工的薪资上限较低，高薪的人才往往比较少。因此，优先选择甲方是一个明智的选择。我面试和接触过很多

乙方人员，虽然不可否认其中有很优秀的人才，但受限于乙方的工作形态，大多数人还是在做一些基础且重复性的工作。长期在这种环境下工作只会破坏个人的发展。

在选择公司时，可以考虑选择巨头或潜力股。互联网甲方可以大致分为综合体巨头、大型平台经济公司、细分独角兽和初创公司。对于多数人来说，按照从左到右的优先顺序选择是最佳选择。这些公司往往自身业务赚钱比较容易，因此员工也能更加容易拿到高薪。收入的天花板比较高，可以更加长期持续的工作。然而，也存在例外情况。选择独角兽公司有可能为你带来更大的资金收益（期权价值增长）和综合能力的成长（安全广度和空间）。通常，在热门的细分领域，明星初创团队更容易取得成功，但也有可能成为过气的独角兽。

在我刚开始工作的那几年，我在许多小型互联网公司工作过。这么多年过去了，仍然留在小公司的前同事的薪资仍然只有两万多。而在巨头公司的热门职位上，应届生的薪资都高于这个数额，这就是小公司的薪资天花板。由于业务规模的限制，技术深度和薪资水平很容易达到天花板。随着时间的推移，你的技术热情也会减退，学习能力也跟不上，年龄也成为进入大公司的瓶颈。

我庆幸在2014年加入了当时还小但有潜力的独角兽公司蘑菇街，并陪伴蘑菇街一路走向上市。有潜力的公司能让你快速成长，跟随公司一起成长会更加顺畅和扎实。当无法判断公司潜力时，选择某个细分领域的独角兽公司会更加稳妥。后来我进入了蚂蚁集团，大公司经过了初期的建设阶段，能让你更专注于某个细分领域的深入。同时对安全的资源投入上是持续的，同时薪资和晋升机会也能得到保障。

努力提升自己，尽早离开小且没有潜力的公司，否则不要期望人生有什么改变。

钱和成长兼得

钱不多的地方，往往也学不到什么。很多刚毕业或老一辈的人认为只要能够学到东西并得到锻炼，薪资多少并不重要。然而，对于互联网安全岗位来说，这种想法是错误的。如果一家企业对安全人员的薪资并不高，那往往意味着安全在这家企业并不被重视，那又如何学到东西得到锻炼。

金融、电商和游戏等行业很早就开始设立安全岗位，这是因为他们在业务上对安全有很强的需求。这些行业的企业往往盈利较多，因此对员工的待遇也相对较好。这些行业的安全岗位薪资的上限也较高，可以长期稳定地工作。另外，由于对安全的重视程度高，这些行业企业会投入更多的资源来提升安全，更容易有机会去建设更加深入的安全能力。

然而，我见过很多公司的安全建设并不是基于解决实际安全风险的出发点，而是开拓了一些伪需求。所做的事情对最终的风险控制没有任何帮助。我们不应该只服务于伪需求，因为这既会伤害公司，也会伤害我们自己。

文化氛围至关重要

在选择工作时，我们应该先排除掉从事黑灰产业务的公司，以及那些在法律上打擦边球的公司。如果公司的文化不正，就会出现一些让安全人员做违法事情的情况，虽然短期内可能赚到一些钱，但习惯于赚取这种非法收入后很难再回到正常的轨道上，而且很容易就得研究监狱的安全性。

团队氛围是一个非常重要的因素是工作开心与否，它决定了我们能否长期从事这份工作。包括大家相处的融洽程度、领导能力、安全建设深度、工作方式方法以及团队人员优秀程度等等。提前向他人打听这个团队的氛围是非常有效的方法。我很庆幸自己的兴趣和工作是一致的，这让我每天都能愉快地工作。然而，如果团队氛围不好，就像跟不喜欢的人一起玩游戏一样，工作会变得非常痛苦。正向的文化和氛围有助于我们在工作中更长久地待下去，这样我们的技术也会一并深入。

岗位契合度是重中之重

在选择岗位时，首要考虑的是岗位是否与自己未来的职业发展规划相匹配。如果选择了不合适的岗位，就无法发挥出自己的才能，从而导致成长相对较为困难。其次，还需要关注自己擅长的技能是否与公司的需求相匹配，这样才能发挥出最大的生产力。

我见过许多上班如上坟的同事，也见过之前很优秀的人到了某个公司后突然沉寂了。当然，也有一些团队能够根据人员的特长来安排岗位，充分发挥出最大的效率，这样可以弥补企业中的短板，发挥最大生产力。

适合的岗位往往比较稀少，对于大部分成熟的公司，其核心岗位基本没有空缺或不会空缺很久，因此不要将找工作当成百米速跑，而应该当成一场马拉松，持续关注并等待那个合适的岗位到来。

反向调查公司

类似公司对自己进行背景调查，在接受一家公司offer前，也可以通过各种渠道背调该公司，主要集中在该公司的实力、风险、氛围。

- **财报**，重点看看其业务增长、营收、人员薪资投入等。避免加入未盈利且未来发展预期不大的企业。
- **脉脉/微博**，慎重加入在该公司普遍负面情绪公司。
- **企查查/天眼查**，重点关注企业纠纷数量，尤其和员工存在劳动纠纷案件。
- 996.ICU，慎重加入黑名单公司。
- **搜索引擎**，查询创始人介绍，慎重加入创始人为销售背景公司；避免加入黄昏产业；
- **面试**，慎重加入通过面试套取解决方案的公司（如果一个企业靠这种方式去解决问题，可想其能力与氛围状态）；慎重加入面试过程中套取前公司保密信息公司；慎重加入面试官技术能力不行的公司（往往是你之后的老板）；慎重加入发薪日在次月中旬之后的公司；慎重加入办公

环境和氛围让人不悦的公司；避免加入试岗的公司；避免加入试用期超过3个月的公司；避免加入无背景的小微创业公司（<20人，无任何优势资源）；

1.3 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。

回顾从业安全行业十来年，做出的所有成绩并不是因为我更聪明、技术更好、更有天赋，而是每件事我都充满了热情，不断的迭代希望做到最好。

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

1.4 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，不同层级更重视怎样的特质。

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。

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。

业余安全爱好者

待补充

安全工程师

一般为应届211/985信息安全专业的研究生或优秀的本科生，安全技术功底扎实，能在别人带领下高效完成一些明确的任务。

高级安全工程师

一般为应届博士或优秀本科研究生或社招工作5年内，专业能力比较突出，能够在细分子领域独当一面，能够辅导安全工程师进行工作。

安全专家

专业精深，应届凤毛麟角或工作10年内，某个安全细分方向负责人，虚线带领一些同学解决某方面问题。比如SDL负责人、某个重要产品负责人。

高级安全专家

一般某个安全领域工作十年以上，安全下某个大领域负责人，一般实线带人。应用安全负责人、移动安全负责人。

资深安全专家

待补充

安全研究员

待补充

安全领袖

待补充

- 以上仅代表个人观点，非官方标准；
- **人数比例**为个人观察的主观数据，在各部门存在误差；
- 各层级**薪资信息**及和其它公司**层次对照**信息，可参照 SalaryFly <https://salaryfly.com>或对标 <http://duibiao.info> 。

二、安全面试经验

2.1 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 安全行业垂直招聘网站
- 拉钩 互联网垂直招聘
- Boss直聘 和负责人一对一沟通
- 猎聘 猎头招聘
- 智联招聘、前程无忧、LinkedIn、脉脉

高阶岗位另辟蹊径

上面传统的求职方式是多数人的选择，但不是找工作的最好方式，尤其是高阶岗位。多数工作，尤其是好工作，可能并没有在招聘网站公开宣传。因此必须要跳出僵化的传统方式，以下我亲身经验为例，不一定适合所有人，但不失为一种有效路径。

挑选某一个领域，成为该领域的专家。需要注意的是，在现如今安全已非常细分了，非安全负责人或安全架构路线不建议将领域范围扩太大。需要做的是明确自己细分领域，成为该领域专家。领域越细分，越容易成为该领域的佼佼者。

通过自我营销，建立同业人脉。仅仅成为领域专家还不够，有太多更加努力的人、更加聪明的人、背景更好的人，我们需要突出自己，想到该领域时就能想到你，扩大自己同业人脉和声誉。作为安全从业者，可以通过创造有价值的内容，比如可以通过参加安全会议分享有见地的观点、系列博客、开源项目、制作视频、写书、写文章、挖0day、刷排行榜等等许多方法来提高你的声望，迅速让同业人员认识你，积累起知名度，并和大量背景相似的人建立起良好的人际关系。这是一个缓慢的过程，播种价值，收获声望。

让工作找上门来或水到渠成，而不是自己去找工作。此时的你是领域专家且颇有声誉，会有不断的猎头和同行主动找上门来。当人脉中有相关岗位需求或遇到该领域问题时，大家往往会想到你。当恰好他们听说你也在找工作时，一定会优先拉你进他们团队。

我自己其实就是个典型，通过不断的参加各种安全会议分享我的经验、实践和见解，并把一些有价值的项目开源出去，认识了一大批安全行业专家。后来由于当时所在公司蘑菇街业务不景气，希望换个更大的平台，于是我和业内几个朋友透露了希望换工作的想法，就有多位业内朋友帮我物色岗位，也接触了几家大型互联网企业。恰巧此时蚂蚁集团一位资深安全专家在组建网商银行的安全团队，得知我有换工作的想法，随即一拍即可，有一号位的认可后续的流程就很顺利的通过了。后来，我才得知，在我入职前招聘其他同学时，有个面试问题是你业内的偶像是谁？居然有两位同学都提到我，相信这件事在我面试过程中极大增强了面试官对我的声誉的信任。

2.2 如何优化简历让你在应聘者中脱颖而出

简历是一切的开始，如何从面试官角度去优化简历，避免出现底线以及低级问题，有哪些点可以作为加分项。内容能够更加聚焦展现亮点而非堆砌信息，能体现独特价值，让自己在一众应聘者中脱颖而出。同时也有真实简历模版以及资深专家真实简历供参考。

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，面试时候反正也会细问，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。好的简历能让自己在众多应聘者中脱颖而出，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，尤其是校招，面试官会收到大量的简历，在进行初筛的时候，一天甚至需要处理上百份简历。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。这个过程中，为了降低筛选成本，一些硬性条件开始逐渐出来，比如学校是否985、专业是否对口、是否研究生、研究生是否专业对口、是否有大厂实习经历、是否有与岗位匹配的经验、是否有一些亮点成绩（比赛、开源、顶会等）。简历就是广告，需要在一两页纸上呈现你的优势，把自己销售出去。

简历基本要求

- **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，见过很多看其简历和我所理解的那个人大相径庭的情况，一旦提交简历和后续背调不符，基本与这份工作就无缘了。其次所提到的工作成果也应如实讲，虚假信息很容易被资深面试官通过一些技巧询问出来，同时安全作为一个小圈子，也很容易打听到。

- **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且不注重细节的人。
- **确保基本信息没有遗漏**：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，这会导致增加面试成本，有可能在一开始筛选时就丧失了机会。
- **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，使用简洁清晰的布局来组织信息，逻辑结构清晰，信息密度高，正常一到两页。避免花里胡哨或过于复杂，避免冗长和不相关信息。
- **展示个人品牌**：有GitHub并参与过开源项目，可以写一些自己做过的项目放上去；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；使用PDF、RTF格式，避免直接使用Word；
- **突出关键技能和经验**：强调与申请职位最相关的技能和工作经验，适当使用关键词，使得简历通过最初的自动筛选。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；
- **及时更新优化**：每次提交简历前建议都仔细阅读优化下简历，确保反映了你最新的技能和经验。避免其中的一些过时的信息出现。

讲清楚你的独特价值，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，也不希望看到你讲的都是团队的成果，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，你团队干了什么，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，不要写平庸的事情，比如一些和专业不相关的实习经验、一些学校里担任职务、参与学校里举办的一些活动等，除非做出特别大的贡献或拿到非常出彩的成绩，或者判断下这件事写上到底是加分还是减分。平平无奇，没有亮点的简历，面试官并不想花费时间来进一步挖掘。尤其是当你学历等硬性条件差一些时，更应该通过其它亮点信息来进行弥补。让简历变得臃肿不堪或过多无用信息，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。这里要注意，作为应届生参与校招，简历中一切内容得聚焦在细分安全领域，千万避免什么安全方向都参与了一些，这会导致在面试时被问到太多方向的问题，最后出现不聚焦、不深入等面试评价。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

使用空无内容的模板无法完整体现简历表达的信息，因此讲自己的简历作为模板放出来。由于时间仓促，还存在较多问题，仅供参考。

吴飞飞v0.1–20231020

2.3 一些通用安全面试经验

面试也是一项技能，虽然我们无法通过不断的面试来提升技能，但可以去避免前人踩过的一些坑。包括要去理解企业面试官常常关注的考察点，使用的一些面试方法（STAR面试法、行为面试法、冰山模型、压力面试法等），以及面试过程中需要注意的事项，同时通过简短的面试反向甄别面试官的能力以及其团队的水平。

企业面试官考察点

面试官主要职责是为企业招到梦想一致的优秀人才。

校招与社招考察点

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？对校招来说，五选二是基础（名校背景+学术论文+开源成果+比赛成绩+大厂实习）。对于社招来说，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?

软性考察点：可以有缺点，但不能无法改变

- **相对容易改变的**：风险承担、引领前沿、教育、经验、组织 / 规划、自我意识 / 反馈、培训 / 发展 / 辅导、授权、团队合作、口头交流、书面交流、第一印象、关注客户、政治敏感、甄选A级员工、重新安置B级和C级员工、目标设定、绩效管理、多样性、主持会议。
- **很难改变但可以转变的**：判断 / 决策、战略能力、实用主义、良好的履历、足智多谋 / 首创精神、追求卓越、引领变革、冲突管理、兼顾需求、独立性、管理压力、适应能力、第一印象、倾听、平衡、谈判技巧、说服力、团队建设。
- **难以改变的**：智力、分析能力、创造力、诚信、独断力、远见、鼓励他人、精力 / 动力、热情 / 激情、进取心、韧性。

面试方法

面试官往往会通过STAR面试法、行为面试法、压力面试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。

另外面试官对应聘者的评价往往是相对的，**同一个面试官往往会使用相同或相似的面试题目来比较你和其他求职者**。若在相关问题中回答较好，面试官则会和历史面试者有一个比较，从而会对你有一个更好的印象。

STAR面试法

STAR面试法是一种结构化的面试技巧，有四个要素：

- Situation（场景）：描述你面临的具体情景或挑战。
- Task（任务）：阐述你的责任或需要完成的任务。
- Action（行动）：详细说明你采取了哪些具体行动来应对挑战或完成任务。
- Result（结果）：描述你的行动带来的结果，最好是具体的成果或学到的经验。

STAR面试法能够让应聘者能够更有条理的方式讲述自己的工作经验和成就，能够突出重点而非泛泛而谈。也有助于面试官更好的额理解应聘者的真实能力和潜力。

行为面试法

行为面试法是一种面试技巧，用来评估候选者在过去特定工作场景下的行为表现，本质是根据过去的行为来预判以后的行为。行为面试法往往适合在应聘者过往的项目经历中顺带提出，比如看到某个应聘者有漏洞应急的经验，那么可以问知道Lo4j RCE漏洞后你当时是如何应急的？能够一定程度上让面试官知道应聘者过去实际工作过程中的客观表现，通过具体的例子能减少主观感受和偏见，从而预测未来在相应工作场景下的表现。

压力面试法

压力面试是一种面试技巧，用来评估候选人在高压或挑战下场景下的表现。一般面试官会通过提出一些尖锐或挑衅的问题，或者模拟紧张的工作环境，或连续快节奏的提问等方式，来观察候选者的情绪和结局问题的思路和能力。这种方式一般会让面试者感到不舒服，虽然只是一种面试方法，但也意味着未来你进入的岗位会遭遇很多类似的高压场景，一般适用于管理岗位。

应聘者面试过程经验

大多数公司的面试方式都类似，以下从面试的不同阶段准备了一些关注点供参考。

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。
- 当然也有可能是电话面试或在线笔试，因此需提前准备好安静稳定的环境。

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。
- 应避免：夸大其词、占有他人功劳、全是亮点、说前老板/公司坏话、说不清为什么换工作、身边重要的人不支持其换工作、对薪酬福利追求大于工作本身。
- 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）

理解背后的意思

甄别岗位、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。这些细节如果没有合理的理由，在今后与其工作日子中会经常遇到。
- 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。虽说应聘者在压力面试下的确能看出一些心理素质，但使用这类方式的面试官往往也会在今后的工作中这么对你。
- 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。
- 此外对于企业内的一些情况也可以观察下，如果存在崇尚加班、狼性文化、家庭文化等情况，这类公司基本可以排除掉，不知道以人为本，视人为人的公司不值得我们为之奋斗。

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。

三、网络安全面试题目

3.1 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。）

提示：如何回答自己的不足是个更难的问题，可以从几乎所有事情都有积极和消极的角度来回答。比如做事情擅长抓重点，但细节跟进不够好。

- 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：

- 避免问题过多过细，也避免没有问题。

- 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。
- 但如果问到岗位职责和工作内容时含糊其辞，就可能对于你的定位并不清晰。如果没有合适你的岗位，让你先入职后再慢慢调岗，这意味着你开始的工作将会很糟糕，而且调岗比想象的时间要长，甚至根本不可能（做的好不会让你调，做的不好不会让你做）。更有可能出现的情况是，你想去的岗位他们更愿意去外面招人。
- 此外还可以借这个机会了解该企业在自己对应的岗位建设阶段，与自己规划是否匹配。
- 例子
    - 您当时被这家公司哪方面吸引了呢？以及您进入后是否有一些和之前预期不一样的地方呢？
    - 您认为我做这个岗位的话，会存在什么样的挑战呢？
    - 您团队目前业务/技术上最大的困难是什么？
    - 您对我的职业发展有什么建议吗？（让经验丰富的人在详细面试后为自己提供一些建议价值较大）

3.2 安全面试的本质

网络安全面试本质在于甄别人选能力，深入理解自己的安全方向比无脑刷题更重要，通过面试过程中的问答更好的表达自己的看法，更容易获得面试官的青睐。

面试的本质在于甄别能力。如何有效的甄别一些滥竽充数的人，最直接的莫过于Show me the Shell。但这一步往往被安排在试用期，在此之前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。

问答是更好的表达自我看法的方式。由于自己并不擅长文字，还没有能力将散落在脑海中的安全知识系统性展开著书。于是我一直思索如何将脑海中千头万绪的碎片安全知识整理成**严谨准确**、**时效性强**且可**持续更新**的文字，经过一段时间实践，非问答模式莫属。

每次面试都会从本文题库中选择一些题目，通过和面试者双向交流后，不断补充新的题目和修正完善答案，确保题目严谨准确。同时日常工作中遇到的各类安全问题、新型漏洞、创新方法等等也成为面试题目的重要补充来源，确保题目时效性。通过一个个具体的安全问题，能看到背后对安全的理解程度。

同样从应聘者角度，题目固然重要，但也不应过于寄希望于通过刷题的方式来提升面试成功率。不必追求每一道题都会，一些问题答案也许仅仅是你没经历过，同时这些你不会的问题也是你可以提

升的地方。更应该通过回答问题表达自己的逻辑思维和深入思考，体现自己优秀特质，让面试官相信你遇到任何问题都能迎刃而解。

了解面试题目而不止于题。在正式开始前，需要明确的一点是，大多数公司是没有所谓的面试问题清单的，每个部门、每个面试官都会挑选自己的面试问题，因此并不存在某个公司的最新面试题目。但各类问题本质是相同的，理解各方向的常见问题可大幅提升自身知识体系和深度以及面试成功率。

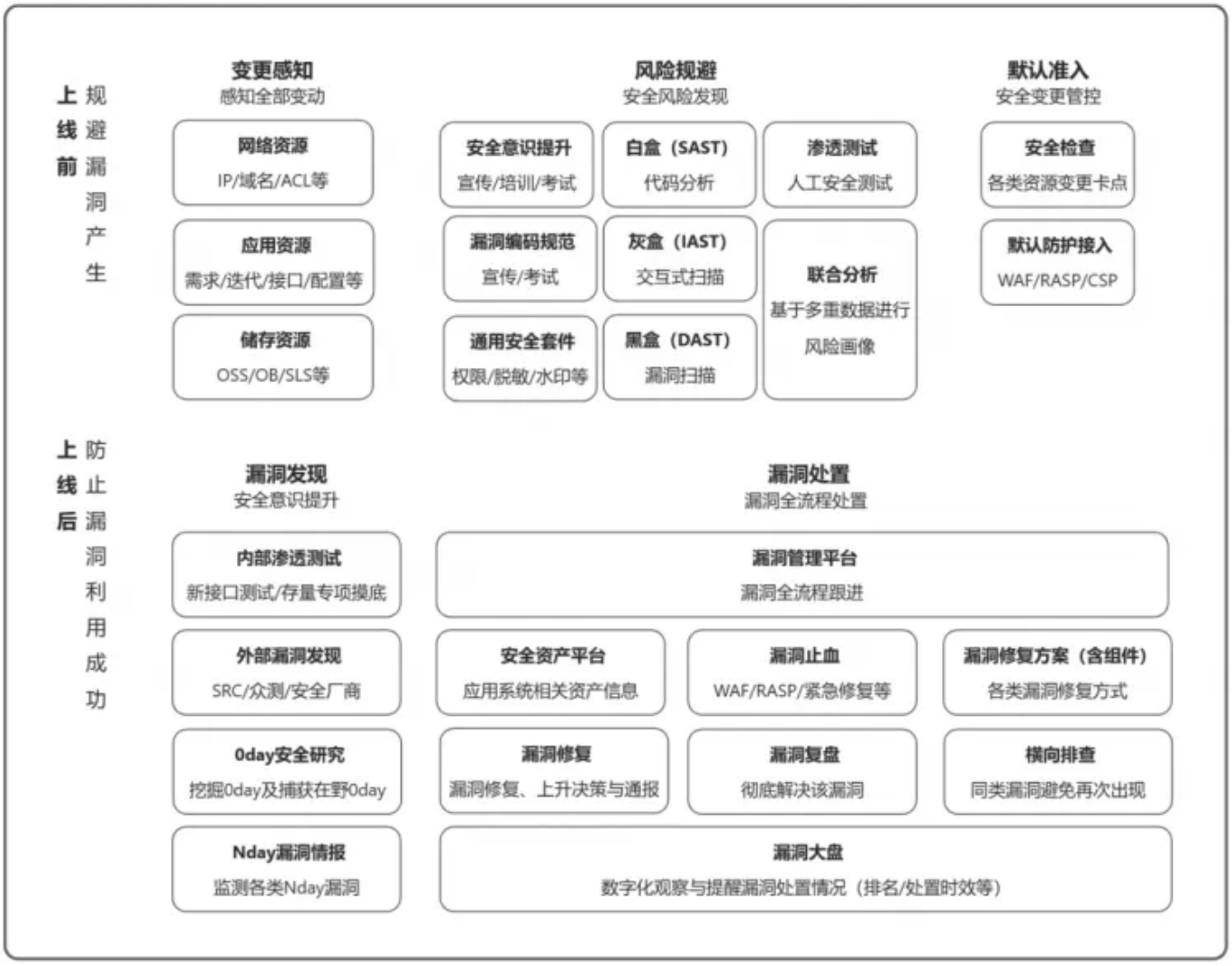
应用安全面试题目

应用安全主要确保软件应用在需求、设计、研发、测试、部署、升级等全生命周期的安全性。

应用安全往往是各家企业都有配置资源建设，且往往都是重要方向。此处应用安全定义为基础设施之上运行的软件服务，主要分为应用安全、供应链安全、移动端安全、IoT安全、Web3安全以及AI安全等方向。应用安全主要以Java/PHP/Go等语言开发的业务应用。供应链安全包括采购部署的各类开源/商业的三方应用或者服务，甚至这些应用所依赖的中间件、组件。移动端安全主要保障在Android和iOS上的App，以及在微信/支付宝等平台上的小程序，主要围绕程序保护（逆向、混淆、虚拟机等）、端环境与风险识别（应用、设备、行为等维度信息分析、设备ID、设备指纹等）、安全组件（包括滑块/投篮/选图/无痕验证码、安全键盘、安全签名验签、安全储存、安全Webview容器、加解密、恶意软件识别、钓鱼链接识别、诈骗电话/短信识别等）、端安全对抗（攻击行为采集、HotPatch等）、端代码安全扫描（包括合规扫描、漏洞扫描等）。IoT安全主要保障各类软件和硬件结合的产品，主要解决传感器安全、通用固件提取与修改、测信道、无线网络攻防、入侵检测、FIDO以及特定场景（比如工业设备、汽车等安全）。Web3以及AI安全等为近些年新出现的场景。

应用安全的建设一般分为安全能力建设岗位与安全运营岗位，安全能力建设偏向开发方向，包括建设黑白灰盒（IAST/DAST/SAST/MAST）、安全组件、SDL平台、安全资产平台、应用安全防护能力（RASP等）、漏洞管理平台等。安全运营岗位偏向机制建设与运营，包括建设应用安全流程、规范、机制建设（涵盖安全意识提升、安全策略运营、安全风险治理等等工作）。当进一步深入建设后，还会衍生出通用程序分析、漏洞扫描与挖掘、各类环境模拟等基础安全研究方向岗位。

应用安全岗位主要工作内容



安全运营

安全理念

★★★☆☆如何理解安全左移?

略

★★★☆☆如何系统地制定漏洞相关指标?

★★★☆☆SDL和DevSecOps有何差异?

安全意识

略

安全规范

★★★☆☆ 安全规范的意义是什么?

避免持续不断的发现漏洞、应急漏洞，而是为了让不出现漏洞建立各种规范。就像是交通法规不是为了限制路权，是为了保障人身财产安全。安全规范绝不是消灭代码的创造性、优雅性，而是限制过度灵活，推行标准化，以一种共识去写代码，提升效率。

安全评估

★★★☆☆ 抽象来看，安全评估到底要评什么东西?

略

★★★☆☆ 安全评估与渗透测试有什么区别?

★★★☆☆ 互联网应用和办公后台应用的风险区别有哪些?

★★★☆☆ 密码如何加密保存?

★★★☆☆ 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?

★★★☆☆ 哪些方法可以防止爆破?

★★★☆☆ 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?

★★★☆☆ 金融业务有何特色?

★★★☆☆ 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?

★★★☆☆ 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?

安全解决方案

★★☆☆☆ 如何规避绕口令带来的风险?

略

★★★☆☆ 硬编码密钥有何风险以及如何系统解决?

★★★★☆ 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

安全资产

渗透测试

漏洞是应用安全岗位从业基础，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。

★★☆☆☆甲方渗透测试和乙方渗透测试有何差异?

略

★★★★☆ 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，现在需要评估某个使用该技术的业务安全性，你会如何做?

常规漏洞

★★☆☆☆ Redis未授权访问漏洞有哪些利用方式?

写Crontab、写公钥、写webshell等。

★★★☆☆ SSRF利用方式及修复方案？Java和PHP的SSRF区别?

★★★☆☆ JSONP的业务意义，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?

★★★★☆ Fastjson、Log4j常见漏洞原理？如何彻底解决该漏洞?

业务逻辑漏洞

★★☆☆☆ 业务逻辑漏洞有哪些具体类型?

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?

★★☆☆☆ 身份标识明文传输会导致什么风险?

★★☆☆☆ 水平越权触发点会存在哪些位置?

★★★☆☆ 水平越权有哪几种检测方式?

★★★★☆ 通过数字加减遍历或通过两个账号互测的方式进行水平越权测试有何优劣势?

★★★★☆ 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?

★★★★☆ 流程绕过漏洞如何抽象理解归类?

API安全

★★★☆☆建设一个API网关，如何系统解决未授权访问、请求篡改、重放等风险?

传输窃取–>HTTPS；未授权访问–>API调用密钥；请求篡改–>请求签名；请求重放–>加随机数的请求签名；

★★★★☆ 设计API签名时，拼接各个参数值时为什么要排序？以及为什么要增加分隔符?

★★★★☆ 设计API签名时，随机数使用秒时间戳（timestamp/s）会存在什么风险?

★★★★☆ 设计API签名时，HMAC SHA256和SHA256区别是什么?

协议漏洞

★★☆☆☆ HTTPS交互过程?

1. (OUT)ClientHello（Random+可接受的SSL版本及加密算法）。2. (IN)ServerHello（SSL版本+加密算法）；(IN)Certificate（包括Server Public Key，CA Sign，Domain）；ServerKeyExchange（若选择RSA加密则无此步骤，若为DHE/ECDHE，则会协商密钥而非传输密钥）；ServerHelloDone；3. ClientKeyExchange（使用CA公钥验证服务端证书是否合法，通过后计算Pre–Master Key，使用服务端证书对Pre–Master Key加密后传输给服务端。服务端收到

后使用自己私钥解密得到Pre-Master Key，通过Pre-Master Key生成Master Key，最终生成对称密钥）。4. ChangeCipherSpec（通知服务端，客户端进入加密模式），客户端对Client Finished加密后发送给服务端。5. ChangeCipherSpec（服务端收到消息后使用Master Key解密，成功通知客户端，服务端也进入加密模式），也会给客户端发送一个Server Finished消息，如果客户端能成功解密，双方密钥协商已全部完成。之后即可将数据使用对称密钥加密后传输。

★★★☆☆ HTTPS交互过程中为什么不直接使用Pre-Master Key而要再生成一个Master Key?

★★★☆☆ HTTPS握手过程是在HTTP之前的，如果一个IP上有多个域名，此时该返回哪个域名的证书?

★★★★☆ 基于HTTPS交互逻辑，如何实现让类似Burp等工具无法抓某个域名的包?

★★☆☆☆ CA到底解决了什么安全问题?

★★★★☆ 如果CA本身被攻击或有内鬼，签发了某个域名的证书如何解决?

★★★☆☆ 什么场景下HSTS会失效？如何解决该风险?

★★★☆☆ TLS1.2协议交互过程以及攻击方法?

★★★☆☆ HTTP请求走私（HTTP Request Smuggling）原理

★★☆☆☆ DNSSEC能解决什么场景问题?

★★☆☆☆ CDN场景下的HTTPS证书安全如何保障?

★★☆☆☆ DNS中（DS、PTR、TXT选其一）记录类型的常用作什么场景?

★★★☆☆ 将暂时不用的域名解析到1.1.1.1有什么好处和坏处?

★★★☆☆ OAuth除了最常见的redirect_uri绕过问题外，还有哪些风险以及如何修复?

★★★☆☆ JWT相较于SESSION优劣势?

★★★☆☆ 如何通过HTTP参数污染将uid=9527&amount=100中的uid改为10086?

★★★★★ 当网关对所有请求会进行一次强制urldecode，存在一个参数为uid=9527&remark=充话费&amount=100的接口，仅备注字段（remark）可控时，如何改变最终的金额字段（amount）？

★★★☆☆ Web缓存投毒的原理、利用和修复?

★★★★☆ Web缓存投毒中，针对200的状态错误如何彻底修复?

业务风险

★★☆☆☆ **有哪些常见的业务风险?**

赌博、色情、暗雷、欺诈、非法投资、洗钱、仿冒、刷单等。

What is FAQ?

算法安全

加解密

★☆☆☆☆常见加解密分类和算法有哪些?

对称算法，AES/DES，SM4；非对称算法，RSA、ECDH、ECDSA，SM2；消息摘要算法，SHA256、MD5，SM3；传输层安全协议，TLS、SSL，TLS1.3+国密单证书；国密证书，sha*WithRsaEncryption，SM2-with-SM3；

★★☆☆☆哪些Hash和加密算法不建议使用?

★★★☆☆ 对称加密的块式加密和流式加密相同与不同点?

★★★☆☆ DES的回放攻击如何实现的？以及如何解决?

★★★☆☆ 3DES相较于DES差异?

★★★☆☆ 3DES、AES、RSA之间的优劣势?

★★★☆☆ 有什么算法可以解决RSA私钥可能泄露的问题?

★★★☆☆ 如何增强DH，使得更短的密钥实现更安全的密钥交换?

★★★☆☆ 签名和验签的实现?

★★★★☆ 有哪些可能的绕过签名方式?

供应链安全

★★★☆☆引入三方商业软件，部署时如何进行安全防护?

★★★☆☆ mvn源的安全性需要考虑哪些点?

★★★☆☆如何识别依赖的三方组件（jar/pip/npm包）的后门、投毒?

安全扫描器

IAST

★★★☆☆ 灰盒相较于黑白盒的优势是什么?

略

哪个安全Hook点在常见业务场景中对性能影响最大?

SAST

★★★☆☆ 当前阶段，人工和自动化的代码审计差异点在哪里?

略

★★★☆☆ 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\:\/\/.*\.feei.cn($|(\/[^<>\'\"]*))/，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?

DAST

★★★☆☆ 黑盒如何检测XSS漏洞?

略

★★☆☆☆ 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?

应用安全防护

RASP

WAF

安全头

修复组件

漏洞处置

漏洞管理

★☆☆☆☆ 漏洞修复一般分为哪几个步骤?

略

★★☆☆☆ 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?

应急响应

NDAY情报

其它应用类型

前端/移动端安全

★★☆☆☆ 如何发现网页被劫持了?

（1）CSP；（2）Javascript performance.getEntries() or document.addEventListener('load',e => { console.log(e.target.src) }, true)；

★★☆☆☆ 前端Javascript代码如何混淆以及反调试?

★★★☆☆ 如何实现当前页面location.href改变后，仍然能执行之前页面的JavaScript?

★★★☆☆ APK反编译有哪几种路径，代表工具有哪些?

dex->class/jar->java
dev->class/jar：Enjarify、dex2jar、classyshark、jadx等
class/jar->java：jd-gui、CFR、Procyon等

dex->smali->java

dex->smali：ApkTool

smali->java：smali2java

★★★☆☆ 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?

★★☆☆☆ 静态apk反编译对抗有哪些手法?

★★★☆☆ 静态特征码对抗方式?

基础设施安全面试题目

基础设施是个很泛的概念，在不同公司这个方向的名称也不一样，有些叫做网络安全，有些则细分为办公安全与网络主机安全。此处基础设施定义为应用层以下的所有基础的安全工作，主要分为网络、系统、硬件。网络安全方向涉及的主要工作为网络区域隔离、DDoS/CC防御、网络访问控制、安全网关等。系统安全方向涉及的主要工作为基线加固、运行时防护、主机入侵防护、文件防护、数据库防护等。硬件安全方向涉及的主要工作为固件安全、芯片安全、加密计算、可信环境等。以及可能还有机房物理安全、办公物理安全等。

零信任

什么是零信任?

定义的角度：对原有的信任最小化。
实现角度来看，微隔离、端的信任替换为网络区域的信任、双向mTLS认证。

零信任解决了什么问题?

零信任理念中，人/机器/源代码的信任链和信任根是什么?

如何理解身份2.0?

持续访问控制在哪些实际应用场景中效果比较好?

网络与主机

- ★★★★☆ DDoS/CC如何有效防御与应急?

提示：小型网站可考虑通过Service Worker机制，将静态资源储存在浏览器端；

- ★★★★☆ 如何对网络区域进行划分?
- ★★★☆☆ 经典网络与VPC的优劣势
- ★★★☆☆ 主机最重要的基线是什么?
- ★★★☆☆ 禁止出网的价值有哪些?
- ★★★★☆ 云原生下的网络和主机差异是什么？会有哪些新的风险?
- ★★☆☆☆ 如何实现反向HTTPS代理
- ★★★☆☆ 如何通过技术手段避免非预期端口开放?
- ★★★☆☆ 一个仅有一台服务器的网站，如何安全地解决登录SSH?

提示：（1）更改端口；（2）IP白名单、VPN中转；（3）TCP连接敲门；（4）TCP Over HTTP；（5）SSH Private IP；（6）Cloud SSH；

- ★★★☆☆ 容器存在哪些特有安全风险?
- ★★★☆☆ 运维白屏化的难点是什么?
- ★★★☆☆ 不同语言对于系统CA证书的信任情况有何不同？如何让各语言信任系统CA证书?

提示：Java JDK自己维护CA证书，默认不使用系统CA证书，可通过keytool导入CA证书；Python下各包CA证书逻辑不一致，可通过设置系统环境变量CURL_CA_BUNDLE让所有包信任系统CA证书；nodejs默认不信任系统CA，可通过设置系统环境变量NODE_EXTRA_CA_CERTS让所有包信任系统CA证书；

- ★★★☆☆ **简单描述有哪几种方式实现服务器截外联，各自利弊是什么?**
- ★★★☆☆ **如何实现在办公网区域无感访问国外互联网?**

办公设备

- ★★★★☆ 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?

威胁感知与响应面试题目

主要以威胁生命周期进行防护，包括威胁情报（外部贩卖数据、黑灰产手法、0day/nday漏洞、威胁IP/域名/app/账号/手机号/电话号码/身份证等数据）、攻击链路中各阶段蜜罐（包括无交互、

轻交互、服务蜜罐、交互式蜜罐等）、威胁感知（采集网络、主机、终端等各层数据，汇总分析、研判与处置）、黑客溯源、红蓝对抗（内部与红队进行常态红蓝演练）。

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?
- ★★☆☆☆ WireShark如何抓取非浏览器的HTTPS请求流量?

人机识别

- ★★☆☆☆ 哪些场景容易出现机器自动化?

提示：功能自动化（自动聊天、游戏外挂、恶意点击等）、稀缺抢购类（抢红包、秒杀等）、数据爬取类等

- ★★☆☆☆ 端上有哪些常用的自动化实现?

提示：按键精灵、触动精灵、Auto.js（iOS）、UI Automation（iOS）、伪造指令（辅助功能/sendevent/构造点击事件）、无障碍模式、adb、Instrumentation单元测试框架、Hook、API接口调用、物理点击（点击器/筋膜枪）、AI+iOT

- ★★☆☆☆ 抢购类人机识别有哪些策略比较有效?

提示：操作链路是否符合正常业务逻辑（还未开始就调用最终抢购接口等、未经过正常业务入口进入等）；操作累计行为是否符合正常人（1s点击次数、单日观看次数、多日累计交易额等）；精细化对抗（多层CNN-BASE网格手势路径识别、利用加速度陀螺仪传感器数据进行AHRS算法求解姿态角）等。

风险识别与应对-移动端

- ★★☆☆☆ 端上有哪些风险特征?

提示：root、hook、debug、多开、模拟器、虚拟容器、注入、重打包、调试等；业务行为特性（访问业务序列是否存在固定路径；单账号访问某一个服务大于正常阈值）；物理行为特征（重力加速度/陀螺仪等姿态传感数据，亮度传感器，手势传感器；手机电量，充电状态，网络状态，硬件信息，锁屏等）

风险识别与应对-网络侧

- ★★☆☆☆ 常见的C&C通道种类和特征?

提示：特征从上行比下行大、长连接、心跳、没有js等资源引用等方面来看。

- ★★★☆☆ 如何在加密流量中检测出恶意流量?
- ★★★☆☆ 新企业应监控哪些主要行为特征?

提示：出站流量；HTML响应大小；登陆地异常；数据库读取量级异常；同一接口的大量请求；等

- ★★★☆☆ 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?
- ★★★★☆ 如何挖掘某个恶意APP、钓鱼网站背后团伙?

提示：首次安装使用该APP、钓鱼网站的人大概率是黑产团伙。同时通过有交集环境（网络、设备）挖掘同伙，以及通过社交、资金记录交叉圈定。

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?

数据安全面试题目

数据安全主要围绕数据流转的全生命周期进行保障，主要工作包括数据分类分级、数据流动链路、权限管控、加密脱密、数字水印、虚拟环境（虚拟桌面、虚拟App运行等）、文件分发（又叫摆渡）、生态安全、隐私计算以及数据行为采集与分析。

安全责任与意识

- ★★☆☆☆ 安全心智的目标是什么?

提示：避免低级问题、避免问题重复出现、纠正错误观念（理解自己的责任和义务）、了解安全团队工作，打造团队形象等。

- ★★☆☆☆ 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

- ★★☆☆☆ DAC（Discretionary Access Control）自主访问控制 和 MAC（Mandatory Access Control）强制访问控制 优劣势?
- ★★★☆☆ ABAC（Attribute Base Access Control）基于属性的权限控制 的特点?

提示：ABAC：集中化管理；可以按需实现不同颗粒度的权限控制；不需要预定义判断逻辑，减轻了权限系统的维护成本，特别是在需求经常变化的系统中；定义权限时，不能直观看出用户和对象间的关系；规则如果稍微复杂一点，或者设计混乱，会给管理者维护和追查带来麻烦；权限判断需要实时执行，规则过多会导致性能问题；

- ★★★☆☆ 为什么ABAC没有RBAC（Role Base Access Control）基于角色的权限控制流行?
- ★★★☆☆ 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?

数据安全综合

- ★★★★☆ 数据安全治理可以用什么思路做?

安全合规面试题目

安全合规主要保障业务开展过程中符合国家法律、法规。往往分为业务合规与技术合规，主要工作包括取得并维护各类安全认证（SOC2、ISO、等级保护等），以及检查不合规并推进整改，以及协作各方完成监管相关检查落地。

安全合规

- ★★☆☆☆ 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
- ★★☆☆☆ 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
- ★★★★☆ 如何平衡监管合规和业务发展的关系?

安全蓝军面试题目

蓝军认知

- ★★★★☆ 安全蓝军和常规渗透测试的差异是什么?

提示：

- 攻击目的的差异：渗透测试是为了发现安全漏洞，红蓝对抗是为了获取最终数据或资金等目标；
- 攻击方法的差异：渗透测试主要是通过网络在线的手段进行，而红蓝可以使用包括物理渗透、社工攻击等手段。
- 攻击覆盖度的差异：主要差异在目标的功能覆盖全面性和可能存在的风险全面性上，渗透测试侧重于尽量全面的测试系统的所有功能来发现各类安全风险，红蓝对抗更偏向于定向攻击。
- ★★★★☆ 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

- ★★☆☆☆ **如何通过程序判断一批域名是否是泛解析域名?**

提示：查询一个绝对不存在域名的A记录，比如enumsubdomain-feei.feei.cn，根据是否返回IP来判断是否是泛解析（若返回IP则是泛解析域名）。

- ★★☆☆☆ **单机上进行域名爆破存在什么缺陷?**

提示：会导致IP的遗漏，有些域名为增加网站的访问速度，会针对不同线路（电信、联通、移动、教育）解析不同IP。

- ★★☆☆☆ **GitHub中可根据企业哪些特征进行搜索?**

提示：内部域名，内网接口使用的域名、测试域名等，比如feei.cn；外部域名，对外使用的域名，可以选一些风险较高的，比如mail.feei.cn；代码版权，代码头部注释中的版权声明，比如Copyright 2018 Feei. All Rights Reserved；主机域名，服务器HOST域名，比如goods.db.feei.host；代码包名，Java代码包名，比如com.feei.goods；

- ★★☆☆☆ **如何找到某个人的联系方式?**

提示：新浪微博私信、知乎、搜索引擎、公众号、LinkIn、天眼查、Whois、上市财报等渠道

漏洞原理

漏洞原理部分同**应用安全岗位**

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?

安全开发面试题目

JAVA基础

- ★★☆☆☆ equals与==的区别
- ★★☆☆☆ Java虚拟机区域如何划分?
- ★★☆☆☆ 方法重载与方法重写的区别?
- ★★☆☆☆ 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?
- ★★★☆☆ 挑一个设计模式（工厂、单例、适配器、观察者）进行讲解

网络与多线程

- ★★★☆☆ synchorized如何使用？Object的wait、notify方法有什么作用?
- ★★★☆☆ sleep() 和 wait() 有什么区别?
- ★★★☆☆ 什么是幂等性？一般有什么方式实现?

数据结构与算法

- ★★★☆☆ 大文件小内存的排序如何做?
- ★★★☆☆ 有1亿个数字，其中有两个是重复的，如何快速找到？要求时间和空间最优。
- ★★★☆☆ 如何遍历二叉树?
- ★★★☆☆ 1亿个随机生成的无序整数，找出中间大小的值。

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
- ★★★☆☆ 利用HTTPS交互过程中的特性，如何实现让常见抓包工具无法抓某个站点?
- ★★★★☆ 上面方式会引发什么新的问题，以及如何解决?
- ★★★☆☆ OAuth2.0交互过程及其中可能存在的配置不当安全风险
- ★★☆☆☆ 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 和 Cookie的区别?
- ★☆☆☆☆ 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?

安全管理面试题目

当面试网络安全管理岗位时，会遇到哪些面试题目呢？这里就比较偏对安全的理解程度，对所属领域的经验，以及一些安全管理动作是否成熟等。

可以挑选的问一些前面四星及以上的问题，以确保在各个方向上比较均衡

安全认知

★★★☆☆ 安全的本质是什么?

安全的本质是对抗，是智能化的知识对抗。从过去的人与人之间的对抗，到自动化之间的对抗，以及到来的智能化的对抗。对抗的是知识，无论是漏洞利用手法、入侵思路、工具脚本还是威胁情报，又或者是统计分析、算法模型、规则策略等。而谁能掌握更多知识，就能在对抗过程中获得更大的优势，安全的攻防本质是知识的拓展。**知识来源于数据，谁掌握数据多更有优势。**比如对代码逻辑的分析，知道其中存在水平越权漏洞。对流量数据的分析，发现有爬虫风险。拥有更多的数据，将在对抗中拥有更大的优势。**智能化对抗程度决定安全水位。**从人到自动化到智能化的对抗程度逐渐递增，智能化对抗比例越高。如果用智能化的防守面对自动化攻击，就属于高维打击。只有源源不断的增强从数据中提取知识，才能持续维持安全的水位。

★★★☆☆ 网络空间安全和现实中生物安全异同?

★★★☆☆ 威胁、漏洞、风险三者的区别?

组织架构

- ★★☆☆☆ 如何设立安全组织以便于更好的推动安全建设工作?
- ★★☆☆☆ 大安全领域的最优划分? 信息安全领域的最优划分?

提示：大安全：隐私与合规安全、业务安全、信息安全；信息安全：数据安全、基础设施安全、应用安全、蓝军、安全研发；

- ★★★☆☆ 网络安全和数据安全的组织架构如何设计以便于更好协作?
- ★★☆☆☆ 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

安全架构体系

- ★★★★☆ 影响安全建设有效性的关键因素有哪些?
- ★★★☆☆ 如何设置最优安全架构以应对高级持续威胁?
- ★★☆☆☆ 你如何理解纵深防御的?
- 提示：纵深防御不是简单的堆叠多层，而是利用好每一层的优势来降低整体被突破的可能性；每类安全产品有其优势和弱势的地方，我们要利用好优势并使用其它安全产品来弥补弱势；
- ★★★☆☆ 万物皆可安全，依靠什么原则来决策先做什么?
- 提示：由外而内；先底后上；能口不点；
- ★★★☆☆ 传统IDC、云上、混合云架构的安全差异和各自挑战是什么?
- ★★★☆☆ 云原生技术下的安全变化?
- ★★★☆☆ 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?
- ★★★★☆ 漏洞发现在甲方和乙方做有什么区别?
- ★★★★☆ 如何防止0day攻击/业务逻辑滥用/社会工程学/供应链攻击（任选一）?
- ★★★★☆ 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
- ★★☆☆☆ 误报和漏报如何权衡?
- 提示：宁愿漏报也不要出现大量的误报，当出现大量的误报情况下会导致真正有用的东西埋没在报警消息中，宁可牺牲部分漏报也要保证足够好的误报。
- ★★☆☆☆ 白名单和黑名单如何选择?
- 提示：目前整个安全领域都在从基于攻击特征的黑名单专项基于行为的白名单可信，黑名单加不完永远有各种遗漏和绕过的问题；能用白名单（除了白名单都为黑名单）解决的不用黑名单，比如暴

露在外网的只允许80/443端口，其它端口发现一例关闭；

- ★★☆☆☆ 专家经验和机器学习差异
- ★★☆☆☆ 安全产品是自研还是外采?
- ★★★★☆ 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?
- ★★★★★ 大公司像Facebook、Google、花期银行等都出过安全事件，我们如何确保自己不出安全事件?
- ★★★★★ 实战攻防的价值和不足?
- ★★★★★ 如何证明/衡量我们的安全水位?
- ★★★★☆ 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?

四、网络安全行业趋势

IT转向DT、万物互联和地缘政治摩擦的大趋势下，安全问题在国家、企业和个人层面都受到了前所未有的广泛重视。各种细分严苛的安全法律、监管要求、行业标准、认证测评以及实战赛事相继出台，个人对隐私保护的意识也不断提高，产品的安全性逐渐成为企业间的竞争优势。随之而来，对安全岗位的需求将越来越多，安全从业人员的数量也大幅增长，安全对抗的深入也导致了安全细分领域的增多。这些网络安全趋势意味着什么呢?

回顾我刚接触安全领域的时候，许多安全从业者能够凭借兴趣和爱好在行业内取得一定成就，先发优势使我们很容易取得一些成绩，甚至在不同的安全子领域都能有所建树。然而，参加最近几年的招聘，我明显感觉到越来越多专业精深的安全人才，已经脱离了仅依靠兴趣爱好就能取得成功的时代。

作为新人，我们应该借助这个网络安全趋势，抓住时机，打好安全基础，深入研究新兴领域，快速学习他人的经验，抓住每一个成长机会，扩大安全影响力。

未来的安全发展属于你们!