秋招日寄

作者：rainb0w　博客：https://blog.snert.cn　QQ：493292651　时间：2023年xx月xx日

前言

笔者参加了今年的秋招，深刻地体会到了如今安全行业找工作的不易，也感受到了甲方安全和乙方安全之间存在的巨大差异。因此，笔者想在这里详细分享一些自己的秋招感悟和面试经验，真诚地希望这篇《秋招日寄》能够对你有所帮助。另外，这篇文章中的一些想法和观点可能不太成熟，如果你有不同的理解，欢迎与我一起交流。

秋招感悟

这次秋招我主要投递的是一些比较知名的甲方互联网企业，比如腾讯，阿里，百度，美团等等，只有少部分是乙方安全公司。以下是这次秋招结果：

```
1.美团oc
2.阿里菜鸟oc
3.知道创宇404实验室转正
4.腾讯二面挂
5.深信服三面中(不太想去乙方，打算鸽掉节后的线下终面)
6.百度简历挂
7.快手二面挂
...一些甲方小厂简历挂，一些在泡池子，一些还在简历初筛。360笔试忘做了，算了，反正也不去乙方。

今年的秋招就到此为止吧，也懒得收集offer了，打算去学点自己想学的东西
```

为什么我更想去互联网大厂呢？

1.**大厂背书**：在互联网大厂工作，不仅可以积累实际的业务经验，还能为以后的跳槽提供更多更好的机会。

2.**成就感**：当别人了解你在知名的互联网公司工作时，自然是很有成就感的。虽然同为牛马，但也要做一只有成就感的牛马不是？

3.**薪资优势**：offershow上有具体薪资，这个大家可以自己去查。

4.**接触实际业务**：甲方安全工作通常更容易接触到真实的业务，与真实业务接触较少也是我不愿意去乙方安全公司的主要原因之一。

这次秋招我从一开始投简历到获得第一个offer大约经历了一个月的时间，在这一个月的时间里，我的简历被挂了N次，大部分是一些小厂，我猜测这可能是因为小厂对安全岗位的需求较低，也有可能是因为当前的经济形势不容乐观。因此，如果你迟迟拿不到面试机会或者收不到offer call的话，不一定是因为你的技术水平不如别人，有可能是大环境的原因。在互联网企业普遍战略收缩的大环境面前，我们能做的只有祈祷。

通过这次秋招的经历，我也深刻认识到了以前存在的一些不足。在过去，我以为只要我的技术能力足够强，基础扎实，就足以在安全领域取得出色的成绩，而不需要过多关注具体的业务。这种观念在应聘乙方安全公司的时候可能没有问题，但如果希望加入甲方，特别是一些互联网企业，这种想法就显得非常不切实际。

在甲方，安全通常是依附于业务而存在的，甚至在一些甲方业务安全产品中，我们都能够看到"业务大于安全"的理念的体现，比如RASP。几乎每个RASP产品都具备开关和熔断机制。难道甲方不知道关闭RASP可能会带来安全风险吗？当然知道，但之所以会有这些机制，主要是因为RASP的存在会显著影响业务性能，因此有时为了提高业务的流畅性，也需要基于"业务大于安全"的考虑来配置RASP产品。以此为例只是想向你说明，安全在甲方只能算作产品的一个属性或者卖点，而非主营业务。因此，在甲方工作，除了具备安全技术能力，还需要理解业务需求，平衡安全与业务之间的关系，这是非常重要的。

如果你想进入互联网企业接触真实的业务，那么在解决任何安全问题时，都必须仔细考虑解决方案是否会对业务产生负面影响。再来举一个例子吧，比如前年的log4shell这个影响力巨大的漏洞。这个漏洞在刚被曝出来的时候，就有许多乙方安全研究人员迅速跟进，并提供了一些漏洞分析报告，其中包括漏洞修复建议。有一些漏洞的修复建议是这样的：关闭nolookups配置或者提高JDK的版本。但如果你是一名甲方安全工程师，在采纳这些修复建议之前，你必须仔细思考：关闭这个配置或者提高JDK的版本会不会对业务的运行产生影响？显然，提升JDK版本这个修复建议在真实的业务中是不可行的，因为业务往往不能随意更改JDK版本。那么关闭nolookups配置是否可行呢？这取决于业务是否依赖这个配置。如果业务中使用了这个配置，那么关闭它也是不可行的。所以你看，我们不能再像以前那样只是纸上谈兵，而是必须将安全措施和业务需求相结合。我们所做的一切都旨在确保业务的平稳运行。

与过去不同的另一个方面是，在甲方从事安全工作不再仅仅只是发现漏洞然后修复漏洞。我们还必须对甲方SDL的建设和DevSecOps的推进有所理解，只有这样才能真正去保护业务的安全。在甲方的面试中，很多高职级的面试官不再会问你一些基础的知识点了，而是会与你探讨SDL各流程的工作内容和作用。这不是在讲什么"互联网黑话"，而是在判断一个安全工程师对于安全行业的理解。如果你对于安全的理解只是局限于以往的漏洞利用与修复的话，那么你可能无法真正入门网络安全，更严谨一点，是没有办法真正入门甲方安全。

学习Web安全的一点经验

我略懂一些Web应用安全，内网渗透和Java安全，对移动安全也稍有研究，会一点点逆向和二进制，但只会一点，所以这里就不提逆向，pwn以及密码学这些方向了，就简单提一下Web吧。

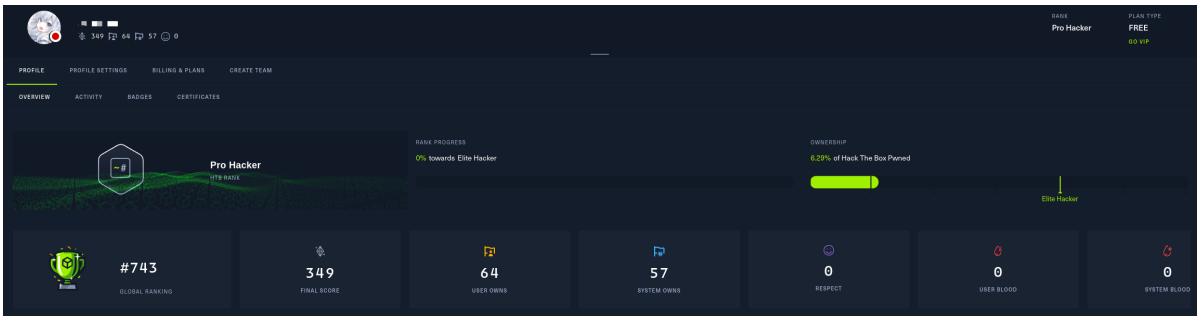
首先，我强烈建议你通过CTF竞赛的方式来入门安全。你可以专心打CTF一直到大二下学期结束或者大三上学期结束。等你大二结束时，你就已经掌握了许多Web应用漏洞的基本原理，如SQL注入、跨站脚本攻击（XSS）、跨站请求伪造（CSRF）、服务器端请求伪造（SSRF）、外部实体注入（XXE）、文件上传等。这个时候你也许还会对一些Web应用漏洞的高级利用手法有所研究。在这段CTF竞赛的过程中，你可能会自己搭建靶场，编写Dockerfile，查找安全论坛上的Writeup，这些经验都会使你受益匪浅。不过在这个过程中，你可能会遇到一些复杂或者难以解决的问题。我建议你在这种情况下，暂时放下困扰你的问题，先积累一些基础知识。一段时间后，再回过头来处理这些问题，也许你会觉得它们并没有想象中那么困难。

当你觉得自己在学习普通的Web应用漏洞方面遇到了瓶颈，或者你已经对许多Web应用漏洞的原理和高级利用技巧都有了清晰的理解，那么你可以开始探索内网渗透和Java安全方面的知识。实际上，通过这段时间的CTF经历，你的自学能力已经大大提高了，因此即使遇到一些困难，你也能迅速思考从哪里找到解决方法。

学习内网渗透的时候，建议你先去学习一些基础知识而不要直接上手靶场。比如域渗透相关的内容：

```
熟悉NTLM协议，并且知道PTH和NTLM Relay的原理是什么，有哪些利用方法？
熟悉Kerberos协议，了解Kerberos协议的每个阶段会有哪些攻击方法，并且这些攻击手法的原理是什么？
横向移动
提权
域内权限维持
Exchange
后渗透相关
```

在学习域渗透的时候，我建议你找相关的书籍进行阅读和实践。我推荐Nu1L Team的《内网渗透体系建设》或者谢公子的《域渗透攻防指南》。尽量自己搭建一个域环境，然后进行实际操作。此外，你还需要了解Linux内网渗透和普通Windows工作组环境的渗透，这部分相对于域渗透来说要简单得多。当你掌握了这些知识和原理之后，就可以开始尝试各种靶场。关于内网渗透，我推荐这些靶场：红日、Hack The Box和TryHackMe。这几个靶场我都有打过，其中打得最多的就是Hack The Box了。我曾经在Hack The Box的日本区域Rank排行榜上名列第六，Rank等级是Pro Hacker。不过后来太久没打导致Rank排名已经从第六名掉下来了，Rank等级不会跌所以还是Pro Hacker。这是最近的截图：



之后就是Java安全的学习了。为什么Java安全会放在内网渗透之后呢？因为我认为你只要掌握了上述两部分内容，那么你就已经具备一些渗透或攻防岗位所需要的技能了。学习Java安全可以让你更深入地了解在渗透过程中与Java相关的攻击方法，但它更适用于安全研究岗位。如果你在甲方工作，特别是像阿里这样广泛使用Java的甲方（阿里的面试官告诉我，几乎所有业务都使用Java，部分可能使用Golang，但绝对不使用PHP），那么Java安全应该是一个必需的技能点。

在学习Java安全之前，我建议你先熟悉Java语法以及一些Java开发框架，比如Spring全家桶、Shiro、Struts2等，然后尝试开发一个简单的后端应用。一旦掌握了这些基础知识，你就可以转向Java安全领域了，可以从JavaSec开始学习（JavaSec上的内容可能比较基础，你可以进一步扩展学习内容）。在学习Java安全的过程中，你可能会遇到很多挫折。其实我在初学Java安全的时候也经常感觉难以入门，但是在我克服了一个又一个的困难之后，我逐渐发现Java安全简直就是我的最爱，我以后也会在这个方向继续努力。

到了这里你发现自己已经熟练掌握了Web应用安全，内网渗透和Java安全，但是你也会发现自己去面试一些互联网企业（如BAT、TMD）的时候，还是屡屡碰壁，甚至直接简历挂。这是为什么呢？其实原因很简单，一是因为学历，这个只能通过考研来解决。二是因为你学到的这些东西太浮于表面了，不能真正用于甲方的实际业务。大家可能会疑惑，为什么不能用于实际的业务？其实出现这种情况的主要原因在于，很多CTF选手没有真正接触过甲方互联网企业的实际业务。所以，你有真正去了解过甲方的实际业务中最常遇到的一些安全问题吗？你可能会以为最常见的问题是SQL注入、XXE注入、文件上传和任意文件读取等漏洞，但实际情况并不是这样的。互联网企业的实际业务中最常碰到的安全问题往往是一些你瞧不上眼的漏洞导致的。比如XSS，CSRF，逻辑漏洞以及高并发场景下存在的漏洞等等。因此你需要非常熟悉这些安全问题，比如知道一个XSS的扫描器该怎么去写，防御CSRF的时候具体应该怎样落地一个CSRF Token等等。

面试经验

这些面试中有的是视频面，有的是电话面，因为我的手机设置了在接听电话时自动录音，因此电话面的那些面试问题可以直接听录音去写，但是视频面的问题就只能凭记忆去写了。

阿里巴巴菜鸟集团

阿里每个BU的流程基本相同，大概流程是这样的，首先如果你简历看得过去，那么会有一个技术面试官来给你打电话跟你约面试，这个面试官可能是你以后的mentor或者主管，又可能是你进入阿里的师兄。之后如果你第一次面试通过，那么就意味着简历初筛通过。对，没错，阿里的简历初筛不是hr筛，而是面试官来筛。当然如果你的简历不太行，比如不是92硕士，那么可能直接就被HR筛掉了。就比如阿里云集团今年就只要23所学校的硕士。阿里第一轮面试是非常非常重要的，同时它的难度相对较大，希望你

认真对待。如果你通过了第一轮面试，也就是简历初审通过，系统会给你发送在线测评和笔试（如果是安全岗位则没有笔试，只有测评）。测评完成后，你会被安排进行第二轮面试，面试官会电话联系你。如果第二轮面试通过，你的面试状态将变为“等待面试结果”，然后你只需等待后续面试的通知。如果你收到面试邀请，状态将变为“面试中”。如果在面试结束后，状态一直保持在“面试中”，就意味着你已经被挂掉了。第二轮面试结束并通过后，HR会给你打电话，然后跟你约面试并加你的钉钉号。(为什么使用钉钉呢？因为这是阿里啊.....)之后HR会创建钉钉群将你和面试官一起拉进来，三面是钉钉视频面试，这一阶段会问技术，也会聊一些职业规划和你对安全事件的看法。所以在这轮面试中，你需要表现得自信、大方。

注：今年似乎阿里所有BU的安全部门都只招硕士？反正我了解到的阿里云，淘天和菜鸟的安全部门都只招硕士，我能有面试的机会是因为有在阿里的师傅让老板把我的简历捞了一下，不然我压根就不会有后续面试的机会，我也很庆幸自己能够把握住这来之不易的面试机会，希望大家即使没有面试的机会也要好好准备，不然什么时候好运降临到头上也抓不住，那样会悔恨很久的。另外，感觉我应该会是今年菜鸟安全组唯一的本科生，是菜鸟里唯一的真菜鸟了.....

一面(电话面-53分钟)

1.个人介绍
2.你们学校现在已经有信息安全专业了是吗？
3.在404实验室主要做哪些事情？
4.除了朝阳区网络攻防演练之外，还参加过哪些比赛或者hw行动？
5.你年龄只有19周岁吗？现在你们都太年轻了
6.你在朝阳区hw主要负责哪些？
7.它这个内网是windows还是linux多一点？
8.一些挖漏洞的经历？
9.遇到的注入漏洞有哪些呢？
10.对于企业来说，更注重漏洞的修复，对于SQL注入漏洞的修复你有什么思路？
11.对于企业来说，业务很多，如果对于每个注入都要写一个防御方法其实是比较麻烦的.比如菜鸟这边可能有上百万个接口，如果每个都要跟进其实是很麻烦的，如果是提供一个通用类或者一个SDK包，对于这种场景，你有什么思路呢？
12.有挖过java反序列化的漏洞吗？
13.fastjson和java原生readObject反序列化有什么区别呢？
14.JNDI注入绕过高版本jdk的方法？
15.不出网的反序列化怎么利用？
16.JEP290怎么绕过？
17.看到你对Java内存马有研究过,JavaAgent型的内存马呢?
18.JavaAgent型内存马在jdk9以后可能会遇到哪些困难?
19.那么JavaAgent在jdk9以后怎么attachself呢？
20.有研究过它的查杀原理吗?
21.了解过SSRF的利用方式吗？
22.如果想写一个修复SSRF的SDK包的话，你有哪些思路？
23.SSRF的绕过方式？
24.DNS重绑定怎么修复？
25.同源策略有了解过吗？
26.同源策略的绕过？
27.CORS跨域或者JSONP劫持平常遇到的真实案例多吗？
28.如果菜鸟APP要上线了，让你来做测试，你的思路是什么？大概的流程是什么？要注意的点是什么？
29.越权漏洞你一般会去找哪些功能去测呢？
30.平常有没有写过一些安全工具？(我把自己写过的工具给面试官详细介绍了一下，感觉这里加分蛮多的.如果你有写过自认为比较创新的工具，请把源码公布在博客或者github上让面试官看，不然可能会减分...)
31.反问？不管菜鸟还是阿里都可以，方向不限.

一面直接秒过，跟面试官聊的时候就能看得出来面试官对我很喜欢，一直在夸我对知识的理解很深，嘻嘻~因此对于面试的结果，你在面试中就能感受到.

二面(电话面-31分钟)

```
1.个人介绍
2.你了解国家护网吗？
3.你认为国家举办它的目的是什么？
4.一些Web漏洞的原理和修复方式
5.一些内网渗透的攻击手法？
6.SDL的各个环节以及每个环节需要注意的事情？你是怎么看待SDL的？
7.你在安全行业的职业规划？(尽量说的细一点)
8.你觉得安全运营的工作应该对业务的熟悉程度是怎样的？
9.有来杭州的想法吗？
10.你去过哪些城市？
11.你是哪里人？
12.反问？
```

二面刚结束一分钟，我刷新了一下简历界面，面试状态就变成了"等待面试结果"，也就是说直接秒过，很开心。

三面(视频面-17分钟)

```
1.个人介绍
2.XSS Worm？
3.怎么修复XSS？
4.越权漏洞？
5.你是哪里人啊？
6.404实验室很知名，为什么离开404？
7.你认为自己有哪些能力或者性格可以让你比别人对于这份工作更有优势？
8.了解过菜鸟吗？
9.有没有了解过Prompt Injection？
10.反问

面试官告诉我下一个面试官是P9高管，当时听完就慌了.....
```

四面(视频面-20分钟)

```
1.个人介绍
2.你是哪里人啊？
3.你才19吗？
4.为什么不考研？
5.了解过菜鸟的一些业务吗？
6.来过杭州吗？
    没去过杭州，面试官给我介绍了杭州的风景和一些景点
7.英语怎么样？
8.你认为在甲方做业务安全和乙方做安全有哪些不同？
9.反问

面试官与我印象中雷利风行的阿里P9高管形象不太符合，待人很有礼貌.反问环节面试官给我详细地介绍了菜鸟的很多业务以及发展规划，还跟我探讨了一下阿里1+6+N改革后的前景.当时就觉得大概率能过.最后这位面试官说与上一位面试官讨论一下之后给出面试结果.
```

四面刚结束过了十分钟还是"面试中"，大概过了一两个小时再看了一下(应该是四面的面试官与三面的面试官讨论了一下)，就变成了"等待面试结果"。

hr面

```
略
```

总结

本来以为会被拷打，没想到碰到的每个面试官都很nice，他们给了我很多建议，体验感直接拉满。

腾讯

今年很多地方都在传腾讯的安全部门是不招人的，但是我还是被约面试了，不知道是谣言还是被当作KPI了。一面就直接是腾讯CSIG事业群攻防方向的leader，咱也不知道为啥boss放在第一关...

笔试

什么题目都有，范围非常非常广，还有很多AI相关的题目，可以去网上搜一下往年腾讯安全技术岗位的笔试题目做一做。

一面(电话面-48分钟)

```
1.你只有19周岁吗？
2.你是在404实验室实习吗？
3.404应该也会挽留你明年入职吧，不知道你是怎么想的？
4.介绍一个对你来说最重要的奖项？
5.朝阳区的网络攻防演练你的角色是什么？
6.除了朝阳区的演练还有哪些实战的经历？
7.你是靠是什么方式方法来积累网络安全这方面的技能的？
8.重写的ysoserial能够实现那些功能？
9.有测过可行性吗？
10.没有一些实战的环境你是怎么去学习的域渗透？
11.我们直接在实战中直接上传一个mimikatz肯定会被杀掉嘛，但是CobaltStrike的mimikatz的功能却不太容易被杀，这是为什么？利用的原理是什么？
(CobaltStrike中不仅仅是mimikatz，还有比如hashdump，ScreenShot等功能原理都是反射DLL注入.)
12.mimikatz的免杀？
13.熟悉msf吗？
14.有自己写过msf的模块吗？
(怎么可能会啊，ruby基础语法都不会)
15.有没有绕过腾讯云WAF，阿里云WAF？你的绕过经验和绕过感受是怎样的？
16.有没有总结过绕过WAF的一些通用的策略或者手法？
17.绕过RASP的一些方法？
18.编程能力大概是能够写多大规模的工具？
19.比较擅长的是用什么样的语言？
20.还有哪些我没有问到的？
21.CVE-2022-26923 AD CS域提权漏洞？
23.你钓了个鱼，并且也拿到了这个鱼的hash，有了这个鱼的一个据点，接下来你会怎么做？
24.在你用某些工具的时候，目标内网的一些安全软件可能会感知到，你钓到的这个鱼也会掉了，该怎么做？
25.假如钓了个运维，怎么扩大战果？
26.你觉得你擅长外网打点还是域渗透？
27.反问？
```

一面结束以后，感叹这位面试官不愧是腾讯的leader，相比很多小公司安全部门的leader来说，业务水平真是高出一大截，对于很多比较硬核的东西都有过深入的研究。本来以为腾讯可能到此就结束了，没想到后续仍然收到了二面电话。

二面(电话面-33分钟)

```
1.个人介绍
2.有做过一些实际的攻防项目吗？
3.在项目里面你主要做哪些事情？
4.可以详细讲一下你说的这些点上有什么比较突出的贡献吗？
5.还有一些别的项目经历吗？
6.有研究过有哪些方法去绕过disable_function吗？
7.windows提权的方法？
8.假如你有的帐号是服务帐号的话怎么去提权？
9.linux提权的方法？
10.拿到redis的口令之后有哪些方法去攻击呢？
11.如果拿到了一台非域内的机器，怎么去找域控？
12.有域森林的渗透经验吗？
13.假如你拿到了域管，知道了目标人员是谁，那你怎么定位目标人员的机器？
14.黄金票据
15.攻击exchange
16.绕WAF的一些思路
17.java内存马查杀工具，你的查杀思路是什么？主要检测哪些类型的内存马？
18.JavaAgent内存马怎么查杀？
19.反问
```

哼，腾讯，莫欺少年穷，我还会回来的。

美团

笔试

安全岗位与别的开发岗位一样，一共5道算法题目，如果只能写出第一道签到题那基本没戏，如果一道都写不出来，建议你多看看乙方的机会。我一共写了3.8道，第4道过了80%的样例，第五道没写出来。

美团的一面主要问一些难度中等偏下的技术。二面主要问一些你对自己做过的项目的理解和总结，还有一些难度中等偏上的知识点。三面主要问你一些项目经历和实习经历，并从中挑出技术点来提问。也就是说美团的三次业务面都是高强度地问你一些技术点，不聊天。因为是视频面，没录屏，所以这一部分的面经只能凭借记忆写了。

一面(视频面-50分钟)

```
1.个人介绍
2.SQL注入
3.XSS注入
4.CSRF
5.SSRF
/*以上这些并不仅仅只是问你一下原理和修复方式就结束了，还会有一些拓展*/
6.Redis未授权
7.Redis最新版怎么利用？
8.NTLM Relay有哪些限制？
9.黄金票据和白银票据的区别？
10.英语怎么样？
11.域环境下NTLM验证的流程
12.windows高版本怎么抓取明文密码？
13.怎么做信息收集？
14.怎么识别CDN？
15.存在CDN怎么获取真实IP？
16.fastjson的一些反序列化利用链
```

```
17.DNS重绑定的原理
18.介绍一下自己写的工具
19.反问

还有很多问题，不太记得了，好像还有一些java的？...
```

一面过了5分钟左右，就收到了二面的面试邀约，这流程真的快...

二面(视频面-55分钟)

```
1.关于项目的一些总结和思考
2.你在实习期间对于团队的贡献？
3.windows权限维持
4.linux权限维持
5.fastjson反序列化与Java原生readObject反序列化之间的区别
6.Redis未授权的这些利用方式都有哪些限制？
7.一些密码算法
8.黄金票据和白银票据
9.java安全的一些问题
10.审计过的一些项目
11.越权漏洞
12.反问
13.想去的base地？

这一面一共55分钟，还有很多很多问题，但是暂时想不起来了
```

这二面更是夸张，刚结束面试，然后拿起手机就收到了三面的面试邀约短信，太离谱了...个人也感觉在美团的面试中发挥最好的是二面，从头到尾面试官问的所有问题我都回答上来了，而且基本上都有一些拓展。

三面(视频面-45分钟)

```
三面主要问你一些项目经历，实习经历，并从中挑出技术点来提问.具体内容实在不记得了
```

三面结束隔了一天，收到HR的面试邀约电话。

hr面(视频面-35分钟)

```
略
```

hr面结束后的第二天就收到了意向书。不枉我天天用美团点外卖.....

深信服

笔试

深信服的笔试影响不大，我笔试了30分钟然后外卖到了果断结束笔试，结果一面面试官说我笔试只有30多分，前面好歹还有几个50多分的。哈哈哈

一面(25分钟-视频面)

```
1.个人介绍
2.你只有19周岁吗？
3.为什么离开404实验室呢？
4一些场景题目
    你现在有了一个网站的管理员账户，怎么做渗透？
    你现在有了一个登录框，怎么渗透？
    ......
5怎么笔试只有30来分，前面几个好歹还有50分，到你这儿直接30分(然后他就蚌埠住笑了...)
6.好像还提问了一些知识点，但是记不清了.
7.反问

25分钟结束战斗，我以为看我笔试垃圾直接给我拒了......
```

二面(50分钟-视频面)

```
1.个人介绍
2.CTF的一些经历
3.实习的一些经历
4.项目的一些经历
5.你人生中遇到的最大的困难是什么？你又是怎么解决的？
6.聊天
7.反问

大部分都是聊天...
```

终面(北京线下面)

```
不打算去了，反正也不去sxf...
```

快手

一面的面试官会问一些基础的Web应用漏洞，还有计操，计网，密码学都会问到，最后还出了一道极简单的算法题。一面的面试官给我带来的面试体验是极好的，即使有一些不熟悉，他也会慢慢引导你，鼓励你。

一面(视频面-65分钟)

```
1.个人介绍
2.一些基础的Web应用漏洞
3.一些基础的计算机专业知识
4.一道leetcode的easy难度的算法题(如果你这道算法题没写出来直接挂，不管你前面答的怎样)
5.反问
```

二面(视频面-30分钟)

> 二面的面试官给我的感觉非常糟糕。我在结束二面的时候气得直骂傻逼，所以请允许我使用"它"来指代这个面试官。首先它连JWT是什么都不知道，不仅仅是JWT，我提到的很多基础知识它都没听过。它甚至现场查起来了.那各位想一下，它连我提到的那些基础知识都不了解，那它提的问题会是有脑子的问题吗？虽然都是些无脑问题，但我还是强忍着怒火，礼貌又耐心地给它答完了。除此之外它还不开摄像头，说话声音极小，我跟它说了好几遍听不清，它才会稍微愿意把它的声音放大那么一点。我都纳闷了，什么勾巴面试官比我一个被面试的人都内向？最后它给我出了一道leetcode的mid难度的题目，我十分钟之内写完并给它解释了一下，它看我代码看了半天然后突然笑了一声，最后结束面试。过了几天，一看挂了.这个题我前几天刚写过，写得是正确的。

总结

我是真的后悔二面的时候没有怼那个面试官，直到现在我还记得那一天的场景。建议面试过程中如果发生了你实在忍不了的事情，那就别忍了，面试多了去了，这种fw面试官刷kpi的就得死个马。

Q&A

要不要考研？

在我没有参加秋招以前，我单纯地以为在安全行业只要技术好就可以了，即使看学历，那普通一本的学历也完全够用。但是在经历这次秋招以后，我已经完全不再赞同我之前的观点了。当然，我仍然觉得在业内工作三年比在网络安全方向读研三年的收获要大得多，但是如果你想进入头部的互联网企业(如BAT，TMD)，那么92研究生的身份就是一块不错甚至很必要的敲门砖。如果你没有进入大厂的打算，认为进入一些乙方安全公司做安研或者渗透也不错，那就不需要读研，你现在的学历已经完全够用了。如果你让我给出建议，我一定建议你去考研，而且一定要考进92，如果考研结果仍然是双非的话，那不管去工作还是去读研都无所谓了，随你。

CTF打到什么程度比较好？

如果你学有余力，打到毕业都没问题。但是CTF毕竟非常偏离实战，打得太多也会对你后续就业非常不利。可是打得太少，没拿到很好的奖项，又显得不够专业也不利于就业，这个度怎么把握看你自己咯。不过建议最少最少打到大二结束，并且也要拿到一些令自己比较满意的成绩。

安全这么多方向，选哪个？

如果你没有考研的打算，那么Web确实是最好的方向了，但是也没有那么绝对，因为目前的移动安全和二进制安全仍然有非常大的缺口(很多甲方或者乙方的安全实验室是招二进制和逆向的，只是要求可能比较高，一般本科生达不到)。如果你有考研的打算并且以后还打算往安全这个方向发展的话，那怎么选择其实看你的兴趣了，毕竟兴趣是最好的老师嘛。

安全学得不好要不要转开发？

其实你安全学得好我也会劝你转开发的，毕竟安全行业岗位实在少得可怜，发展也非常受限，别听学校那些老登(比如孙某某)说什么"安全缺口很大，尤其是顶尖人才"，我寻思这不是很容易证伪吗？你去找个工作不就明白了吗？你会发现开设安全岗位的就那几家，而且哪个岗位进去了不是被当成畜生用？找乙方安全公司的工作是比较容易的，但是找满意的工作很难。所以如果你学有余力我建议你学学开发，以后方便换行业.....

秋招个人简介怎么写？

建议做个诚实的人...有什么写什么就好。把你觉得不错的项目写上，这里不要写什么扫描器之类的，真的烂大街了。如果你自己不知道应该写一些什么项目或者什么工具的话，或者能够想到的工具都是一些烂大街的工具，那这多半是因为你积累的还是太少了，建议学体育生沉淀沉淀.....实习经验的话，如果能有国内有名的乙方安全实验室或者一些很有名的甲方大厂的实习经历的话那就可以了。

不打算去甲方互联网公司，有哪些乙方安全公司和岗位值得选择？

一些知名的乙方安全公司都是很不错的，比如深信服，绿盟，奇安信，360，知道创宇等等。

一些乙方安全实验室里的安全研究员是真的很厉害！以我之前待过的知道创宇404实验室(实验室主要研究方向是Web安全)为例，有一个研究二进制的师傅参加过很多次的Defcon决赛，有研究Linux内核的师傅，还有一些Web方向的师傅，他们对于Java安全以及内网渗透的了解真的是让人望尘莫及，而且几乎每个人都是全栈。

长亭也是很不错的，建议去长亭做安全研究，听说氛围不错.....

绿盟的实习给的太少了，这个可以去Boss上看一下。之前找过绿盟的安全攻防的实习岗位，结果hr说boss上标注的200/天是加了30餐补的，也就是说实际工资是170/天，这还是在北京的岗位，最后我以没法在北京生存为由果断拒绝了，他也表示理解说以后有机会再合作，结果过了一段时间发现他给我拉黑了.....不愧是安全界的黄埔军校，军人嘛，少给点很正常。

深信服给的薪资在乙方安全公司里还是很有竞争力的，缺点就是加班严重，另外尽量去深蓝攻防实验室。

奇安信和360这俩之前本来是一家，后来分拆了。我对奇安信的观星实验室印象还是很不错的，之前看过的很多Java安全的研究文章都是他们实验室写的，360的话其实没大家想象的那么难进，至少我是这样认为的，因此360也值得考虑.....

知道创宇的话除非是404实验室的岗位，否则别去。

安全岗位首推安全研究，其次是攻防，渗透，安全开发。为什么没提安全服务呢？因为我觉得你有这个岗位的工作经验的话，那就意味你没有安全岗位的工作经验。听起来很矛盾，但是请仔细想一下，这个岗位真的能够让你在安全方向上有所成长吗？答案是很明显的，因此即使你真的"不幸"拥有了安服的经验，我也建议你不要写在简历上，除非你真的没有别的实习经验能写了.....因为一旦你写了，那你怎么跟面试官介绍你在工作期间完成了哪些有价值的事情呢？面试官当然也知道安服实习生是做些什么牛马工作的，知道你这个工作是没啥意义的，因此反而会因为你的这段实习经验对你产生不好的印象。

如果打算去甲方互联网公司，应该做哪些准备？

除了上述提到的Web应用安全，内网渗透以及Java安全以外，你还需要对甲方互联网企业中常见的跟业务很贴近的一些逻辑漏洞有所了解，比如越权漏洞，验证码漏洞，身份认证绕过漏洞等等，你还需要对甲方的SDL建设和DevSecOps的推进有所理解。在应聘之前，先看一遍道哥的《白帽子讲Web安全》，这本书中的很多安全知识虽然已经过时了，但是其中的一些安全思想仍然非常实用。想在甲方做安全，你的计算机基础必须扎实，建议恶补计算机组成原理，计算机操作系统，计算机网络，密码学，算法，数据结构等内容。绝大部分的甲方互联网公司都有笔试，而笔试必有算法，有一些甲方的笔试题目也有刚刚提到的除了算法以外的这些基础知识。另外，如果可以的话，考个CET-4。

CTF的MISC和Crypto可以深入研究吗？

建议你不要主攻这两个方向，这两个应该是"副业"，而非"主业"。如果你打算以后往学术的路上走得更远，那你可以选择主攻这两个方向。

应该从什么时候开始实习？

如果你的大学是在北京，上海，杭州以及深圳这种互联网企业很多的地方的话，那你从大二就可以去找实习。但如果不是，也就是说每次去实习都要跨市甚至跨省，那我就非常不建议你实习了，还是顺利让自己毕业更好，然后在大三的第二个学期，从3-4月份开始向自己心仪公司的实习岗位投递简历，之后申请转正。因为这个时候去找实习的岗位是比秋招时候找工作更容易的。如果找不到心仪的，那就找一家看起来还算不错的先实习，然后等到秋招的时候就有实习经历了，可以去冲心仪的了。不过虽然不建议你实习，但是建议你每年的暑假去参加护网，并且尽量申请攻击方而非防御方，因为，一只会点鼠标的猴子是要比一只会看屏幕的猴子更有优势的。

秋招都快结束了，一个offer都没有怎么办？

9月底有很多家互联网企业的HC基本都发完了，后续还会有谈薪阶段，在谈薪阶段有很多大佬会拒绝掉offer，因此不要放弃，我们还可以捡别人剩下的不是？如果秋招真的一点机会都没了，那大不了春招呗。不过建议大家不要对春招抱有太大希望，一定要逼迫自己在秋招阶段就拿到offer，因为春招的HC不到秋招的1/3。如果秋招拿不到offer，那么春招也很难拿到。

一点小小的建议

1.少混娱乐圈，多打磨技术。

2.在研究一些漏洞或者攻击手法的时候，多去探索原理。勿做"Script Kids"。

3.漏洞分析不宜做多，如果做漏洞分析的话，建议分析一些有代表性的或者影响力比较大的漏洞。因为每年光有CVE编号的漏洞就有2w多个，除此之外还有一大批没有CVE编号的，如果每个漏洞我们都要分析的话，不仅极其浪费时间，对我们的帮助也不大。

4.近年来想进大厂已经越来越难了，尤其是在安全领域。这主要因为安全岗位相对较少，今年很多大厂的安全岗位都要求92硕士学历。与以往不同的是，如今进入大厂需要更加出色的表现和更加符合岗位要求的实习经历，并且你的知识面不应该局限于某个方向，也就是说你必须对很多方向都有所了解。

5.offer == 正确的方法 + 努力 + 好心态 + 运气

6.我们学习信息安全的目的当然不是为了与别人争个头破血流，然后拿到一个996的工作机会，而是为了培养独立思考和自由探索的黑客精神。