1. **Python面试策略**

首先要根据自己做自我介绍时引入的相关Python知识去逐一分解，并且在简历中要有体现。比如这样介绍自己：

“你好领导（或者提前问好姓名，比如xx哥），我先自我介绍一下，我毕业于xxx大学，我所学专业是xxx。在校期间我通过课程及自我主动学习了xxx、xxx、Python编程，并且利用Python做过爬虫项目和写一些渗透测试poc，我还通过自己写的poc验证了学校xxx服务的漏洞，并提交给系主任，获得了学校的通报表扬”

注意，自我介绍时不需要说流水账，什么学生会荣誉、帮打扫卫生阿姨的倒垃圾等这些不要说，要说简历相关的东西，还有就是在自我介绍时，重要的和自己很熟悉的技术要在最后说，往往面试官只记得你最后说了什么。

**二、通过自我介绍去引导面试**

假如，你在最后提到了Python编程和编写相关漏洞的poc，接下来面试官可能会问你一些Python的基础知识，下面模拟面试官提问：

1. 你做过爬虫项目是吧？用的什么框架？

注意，这时候，你不能只答“做过，用的是scrapy”！！！

面试官不是要的答案，而是你的主动性，你要这样回答，会显得你知识底蕴很好：

回答：

我曾经帮助导师爬取一些统计数据（这里不能提有关版权的东西，比如论文，也不要去延续去讲这些数据是干什么的），我当时用的是Python scrapy框架，这个框架的优点是性能好、速度快，不管是动态网站还是静态网站，他都可以爬取数据。（主动讲scrapy框架原理，说的越多越好，除非面试官打断，最好是不给他说话的机会）scrapy它有5大模块，分别是核心引擎、Spider、调度器、下载器、pipelines。他们之间是这样的一个运行流程（最好是提前准备好纸，在纸上画）：当运行scrapy爬虫项目时，引擎首先会到Spider爬虫类中找到start\_urls，然后将第一个URL包装成一个request对象，再通过引擎交给调度器Scheduler，调度器它实际上是一个URL队列，它会自动去掉重复的请求。然后调度器会将request请求对象通过引擎交给Downloader下载器，下载器通过网络去发送请求，目标网站返回的数据是一个response对象，下载器将response对象通过引擎交给Spider爬虫类，爬虫类从response对象中获取有用的数据后，把这些数据包装成一个item对象，通过引擎交给pipelines管道，在管道中可以定义数据是以什么方式保存，比如保存在文件、数据库等，这是scrapy各个模块之间运行的流程，当时我还加入了代理IP和自定义user-agent的一些自定义配置（这句话是引导面试官问下一个问题），防止对方站点出现过多的相同请求。

1. 你在哪里加入的代理IP和自定义user-agent？不加user-agent的请求是什么样的？

注意：这里不能直接说在某某文件中加入，而是爬虫运行过程中的哪一步会引入这些东西

回答：

如果定义了代理和请求头，当Spider爬虫类将URL包装成request对象发送给调度器后，调度器在交给下载器之前，request对象会加入一些自定义的headers和代理，通常我们会把scrapy默认的user-agent注释掉，然后加入自定义的user-agent，一般是在settings文件中定义user-agent，然后在中间件Middlewares中的下载中间件downloadMiddleware类中的process\_request方法中定义，这个方法的作用就是在发送请求之前包装request请求，加入一些自定义的东西。如果不加自定义的user-agent的话，scrapy发送出去请求的请求头中user-agent会带上Python和scrapy的版本，这些信息最终会保存在目标服务器的日志中，虽然我爬取信息不是以盈利为目的，但是这样大量爬虫信息显然不是太好，还容易被对方把我所在区域的出网IP封锁，所以修改user-agent和加入代理IP是为了模拟真实请求。

一般是一个项目经验面试官问两个问题就不再对这个项目关注了，那么你要引导面试官去问下面的问题，不要两个人都安静下来。

比如上面那个问题，你可以接着说，爬虫是我做过的Python项目中的一个，我在校期间或者某阶段工作中，还写了一些Python的poc，还发现了学校服务器的漏洞，当时将验证数据交给系主任后，后面还得到了学校的表扬。（不同场景灵活应变）

这时候，面试官会问你发现了什么漏洞？

答：

当时我发现学校的成绩发布网站的站点比较老，于是我用自己写的poc验证了一下，我写的poc逻辑是通过requests库发送get请求，获取返回消息体的消息头，通过消息头中的server参数验证网站的web容器是IIS 6.0，然后我就上网找了一个IIS6.0的漏洞，漏洞的原理是通过服务器WebDAV功能的PUT和move方法上传木马可以拿到网站的webshell。然后我又分析了一下消息头参数，发现服务器通过public参数开放了PUT和move的http请求方式。于是我继续用requests库发送一个PUT请求，将一段木马代码成功上传到了服务器的根目录，根据漏洞公布的原理，它还需要使用move的请求方式将原本上传的木马代码文件转成jsp或asp的网站可执行的脚本文件，但是我使用requests库的方法中没有move方法，于是我查资料找到requests库下有个request方法，它可以自定义请求方法，我尝试着用requests.request方法自定method为move，将新的木马文件名通过请求头参数Destination带入到新的请求头中，它的值是新命名的xxx.asp，第一次发送完move请求之后，返回的状态码是207，我认为有问题，没见过这种状态码，然后又发送了一遍，发现得到的状态码还是207，于是我上网查了一下，207状态码是webdav访问成功后特有的状态码，然后我尝试用webshell工具连接上传的木马文件，可以成功的连接，并且还可以看到服务器内部的文件。当时拿到权限之后我，挺激动的，因为这是我第一次真实的发现在自己的生活环境中发现了漏洞，立马找到导师，跟导师说清楚原由后，导师带着我找到了系主任，将一切问题说明后，我还跟主任讲了如何解决这个漏洞，过了一段时间，学校还公开表扬了我。

这时候，面试官可能会说，你在校期间还挺主动学习的，那你觉得如何避免这个漏洞或者修复这个漏洞？

答：

当时我跟主任说了两个方案，一个是如果webdav没有用这个服务的话可以关闭它，一个是如果用到的话，首先修改网站根目录的权限，将目录的属主改为一个普通用户，并且这个用户只能对当前目录有权限，离开这个目录用户是没有任何权限的。然后，将目录读写权限改为只读就可以了。因为这件事情，我自己更加对网络安全这方面感兴趣了，后面我还学习和实践了很多网络安全方面的技术。

这时候，面试官会问你简历上的其他技术，或者是问你都用过哪些网络安全方面的技术？

你自己接着答其他网络安全方面的知识即可