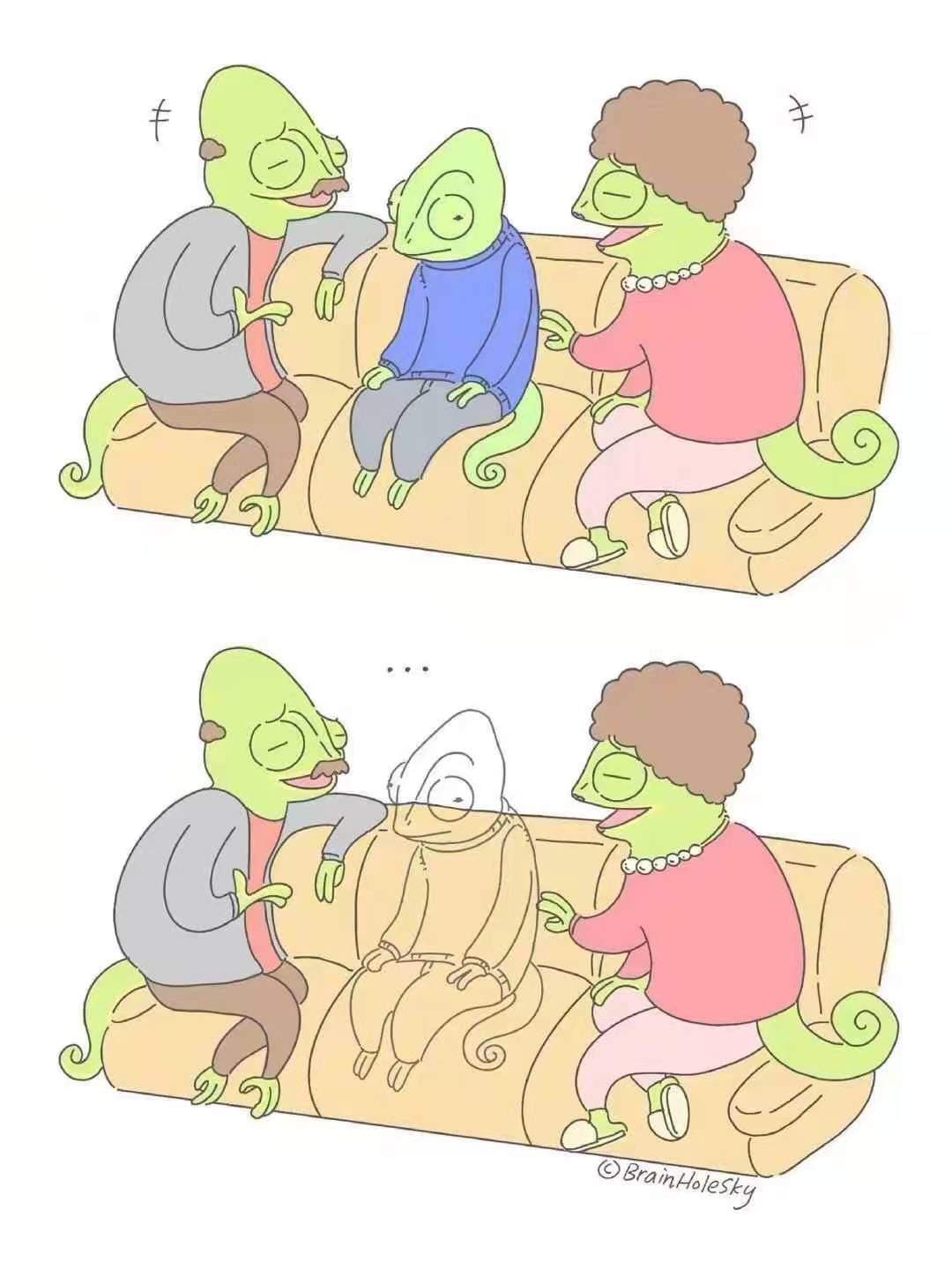
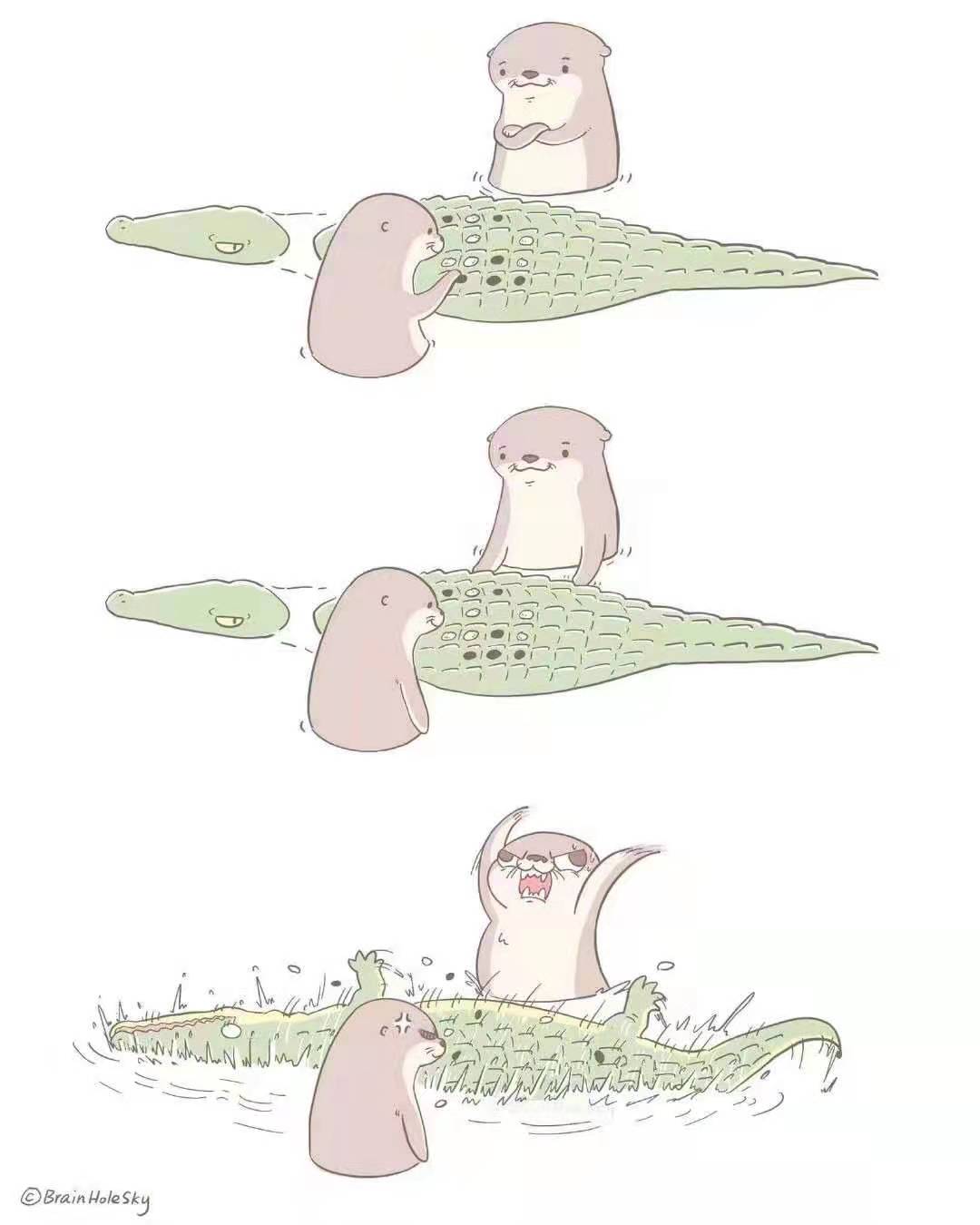
* 问：请你做一下自我介绍！
* 答：巴拉巴拉一堆简短的自我介绍，其中用了“嗯”、“然后”这些语气词来缓解我第一次面试的紧张，其实也没啥紧张的！
* 问：XXX？面试官很惊讶我的公司，很疑问的问了一下！
* 答：对的。
* 问：你在你们公司都做什么？
* 答：简单的说了一下自己的工作内容！
* 问：我以前也是做这个的！
* 答：（听到这个的时候，心中窃喜，感觉通过的希望又增加了。）
* 问：你学的是什么专业？
* 答：不是网安专业的。
* 问：那你做这个怎么想来hvv了啊？
* 答：为了学习，为了提高（当然是为了钱！！！）

**闲扯到此已经一分钟过去了！正题开始了！**



* 问：你有hvv经验么？
* 答：没有。
* 问：你看你简历，参加过SRC是吧！
* 答：挖过！（现在听录音感觉应该说参加过哪年哪月的SRC，名次是多少，当时简短的两个字的答复，后期也会问到，感觉整个过程我俩陷入了我不敢多说，他感觉我太菜不知道咋问的冷场环节！）
* 问：恩……你简历上写的src是那年哪月的啊？
* 答：去年10月的月榜。
* 问：有挖过高危以上的漏洞吗？
* 答：挖到的都是高危。
* 问：都是逻辑类的吗？
* 答：是的。
* 问：都是盲注吗？还是有其他的？
* 答：有盲注，有报错，还有其他的。
* 问：你主要是挖漏洞盒子是吗？
* 答：是的。
* 问：有没有挖过其他大厂的？
* 答：没有。
* 问：啊，行。漏洞盒子给的钱不多啊！
* 答：最近主要是为了学习，挖挖看看，而且接触安全行业时间不久！（内心：我能挖到都不错了，哪敢幻想给钱的事情啊！）
* 问：你搞安全多久了？
* 答：没干过（也算安全，只是和网络安全不沾边啊！安全行业干了十年了）
* 问：┗|｀O′|┛ 嗷~~
* 答：嗯~ o(*￣▽￣*)o（感觉我俩的语气词好丰富啊）  
  

1. 在面试官刚要提问时，我完美的抢话了，直接打断了面试官，等我想让面试官再说的时候，面试官让我先说！这点大家一定不要学，面试的时候一定要等两秒，看看面试官是不是要问问题，如果不问你在说！
2. 我巴拉巴拉说了一堆后面试官再次强调了一下，我以前也干过，说了说自己以前的工作经历！

问：你主要熟悉注入是吧？  
答：是的。  
问：怎么加快盲注速度？  
答：加快盲注速度？  
问：对啊，盲注一般比较慢么  
答：用工具（原谅我自己没忍住笑了）  
问：那你都用什么工具？  
答：BURP、sqlmap  
问：那你有没有不用工具的办法啊？  
答：就是用工具啊，也没别的啥了（经过反思，我查到了加快盲注速度的办法有以下几种，如： dnslog、sqli-Less9、二分法、二进制延时注入）  
问：你还了解其他的sql注入吗？  
答：文件上传。  
问：你说一下文件上传的绕过方式  
答：更改后缀名、00截断，换行符，（有很多当时我紧张到都说不出来了，比如： 前端js绕过，黑白名单绕过，路径截断、普通截断绕过，文件类型绕过系统解析漏洞绕过，中间件解析漏洞绕过等等）

1. 面试官在问这个问题的时候主要是要了解你对OWASP TOP10漏洞的了解及使用，当时我连敏感信息泄露都没想起来。

问：你了解反序列化漏洞吗？  
答：学过，但是记不住了。（）  
问：你了解安全设备吗？  
答：没用过，只是知道waf、防火墙。  
问：如果培训是否可以快速上手！  
答：可以！（斩钉截铁的说，这时千万不要质疑自己）  
问：你对MYSQL掌握的如何？  
答：了解基础的增删改查。  
问：你了解应急响应吗？  
答：最近了解了一下。  
问：请你说一下应急响应。  
答：首先确定攻击时间，通过攻击时间、攻击手段发现攻击线索，然后梳理攻击的方式、流程，根据预案及方案进行解决，最后开始溯源攻击者。  
问：说是这样说，但是你是否了解操作？  
答：我没操作过，但是我使用过wireshark，我觉得第一步的研判攻击流量可以使用wireshark通过函数查看相关的三次握手、四次挥手，确定是否正常访问还是攻击。  
问：我看你的学历是16-19年的？  
答：对的，在职教育。  
问：你就是自考的？  
答：对的（学历是本科，北大法学院，学历还是很装逼的，也不知道为啥问了一下这个，可能是他也第一次见到在中国总想争第一的学府）。  
问：了解反弹shell吗？  
答：反弹shell?是反弹注入么？（当时已经感觉被问蒙了，真没想出来反弹shell是什么，还是学的不扎实）面试官给我讲了一下反弹shell，我感觉我更蒙了。  
问：你了解h--w的红蓝对抗吗？说一下你了解的程度？  
答：我说的是由公安部组织的红队与蓝队进行对抗，红队负责攻击，蓝队负责防御，蓝队需要在防御的同时需要对攻击队进行溯源（我感觉我说的让面试官完全了解到我身为小白的程度）  
问：你是否了解红队的手段？怎么打进来，怎么打？或者说你了解整个渗透测试的流程吗？  
答：通过信息搜集了解公司资产，对公司资产进行端口扫面，搭建隧道，通过redis的6379端口的未验证登陆进行攻击，以及邮件钓鱼。  
问：你知道redis怎么利用吗？  
答：我不太熟悉（当时已经都蒙了，其实后来想想，应该是通过开通的22端口，可以未授权登录redis数据库，上传文件、木马并通过控制的机器访问进行提权从而获得更高的权限，等等。当时就连这个都没想起来。）

**面试到这里就结束了。感觉自己答的很乱套，基本知识掌握不牢，没有办法支撑一场真正的面试。果然熟悉并可以完整的操作整个渗透流程就已经可以实现工作的基本要求了，在下一步的学习中一定要多日站去。  
如果问到的问题一时想不起来了，可以仔细回想在渗透测试过程中如果自己怎么做的，怎么能让自己做不到。不要着急说自己不知道，最最重要的是，不要慌不要乱，否则就像我，只有尴尬的笑了！其他的专业问题求各位学长学姐学弟学妹指点，我会加快转行的脚步争取不拽你们后退**