1.以看看视频为例

<https://haokan.baidu.com/>

关注时抓包



2.对数据包分析发现，删除数据包数据，返回不变





3.猜测BDUSS有漏洞点



只剩下BDUSS发现返回了BAIDUID

考虑这是百度数据库的核心资产 。

4.于是发现可以对BDUSS进行逐位爆破，就可以无限获取到百度内部数据的用户ID形成任意用户登陆。