OOXX 时时真心话安全评测报告

OOXX 时时真心话功能简洁明了，较少出现低级 BUG 及意外退出等问题，但是还是存在一定的服务器端安全隐患以及轻微的涉及使用用户的隐私信息。

1、 用户隐私相关

发送短信:应用会调用系统的短信程序来发送短信

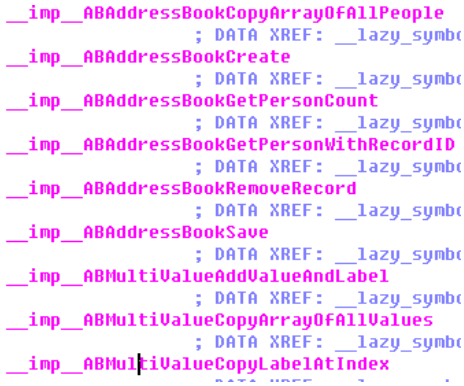
主要是好友邀请功能处使用

地理位置:会使用地理位置,您的位置会上传服务器

通讯录的使用:读取联系人数据

为了增强用户之间的交互和让用户能找到好友，OOXX 真心话可能尝试了使用通讯录对

比的功能，通过将通讯录上传（MD5）到服务器的方式，再在服务器端对比以方便用户找到好友，但是目前前台的功能还没有很好体现。



2、 软件安全漏洞

服务器端重大漏洞:

系统的服务器端存在着安全漏洞可能造成被广告群发，被恶意加好友，恶意发帖，恶意提问，恶意投票等问题。

ooxx 采用的是基于 http 的 api 接口,传输数据格式为 json,但接口效验不完善，在发送数据时没有验证会话状态(登陆验证、时间戳、数据加密、令牌等)导致他人能够获取请求地址伪造数据包对服务器端进行非正常交互,对服务数据造成破坏性的影响。

图为伪造 http 请求(HttpRequest)进行封包发送，并发送成功！

类似的功能可能还有提问、投票、push 功能等。

同样应该考虑是否对用户做了行为限制，例如：短期内高频提问、短期内高频评价、同 ip 大量提问及评价等等恶意行为判定，同时政治敏感词、色情图片的过滤也是需要系统提前考虑的！