Nessus 自动生成中文报告--使用说明

**目录**

1 报告组成 1

1.1 漏洞统计 1

1.2 统计图表 1

1.3 扫描结果 1

1.4 漏洞引用表（中文漏洞库） 2

1.5 宏脚本按钮 2

2 使用步骤 3

2.1 在Nessus中导出CSV格式的报告 3

2.2 自动生成中文的“扫描结果”表（初步处理） 4

2.3 完善中文漏洞引用表 5

2.4 新漏洞的中文描述获取 6

2.5 报告后期处理 8

3 补充说明 8

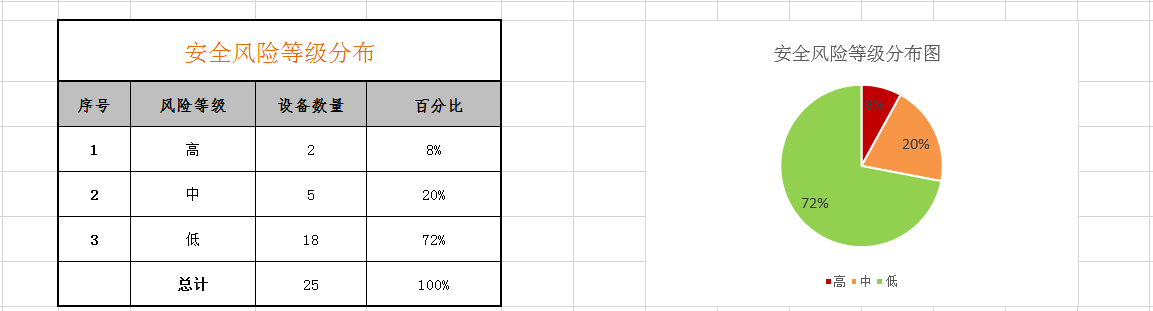
1. 报告组成
   1. 漏洞统计

通过公式自动把“扫描结果”中的数据各个IP的“紧急”、“高危”、“中危”的漏洞数进行统计，如下图：



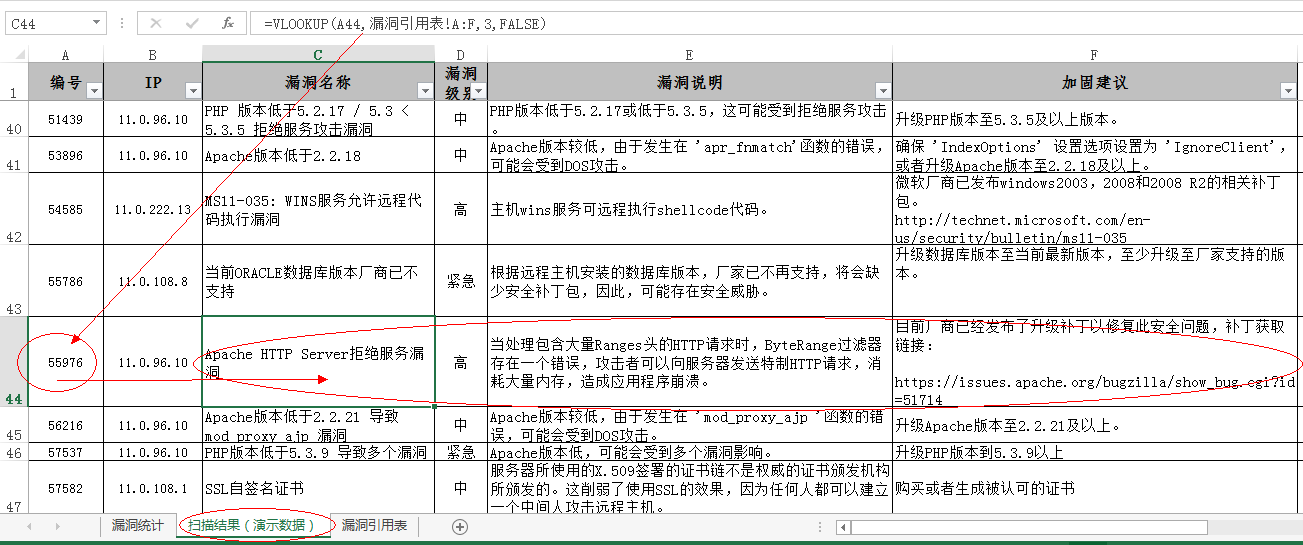
* 1. 统计图表

目前统计图表有： “风险分布比例”，有更好的图表，欢迎推荐



* 1. 扫描结果

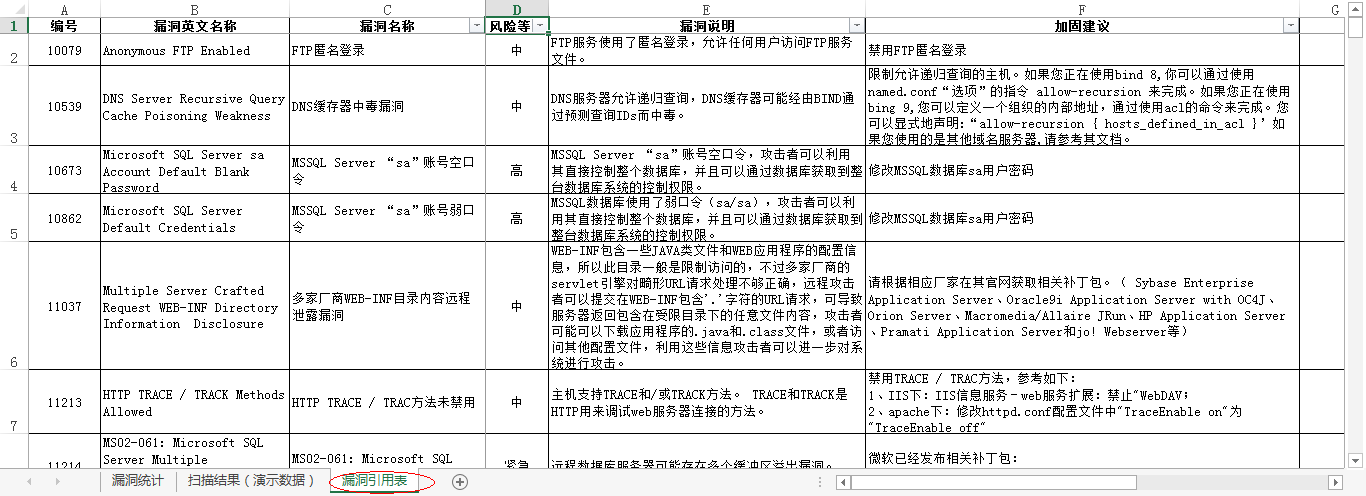
表中的编号和IP 是从Nessus 的原始报告（.CSV格式）中复制过来的。其他内容通过公式，自动根据漏洞编号从“漏洞引用表”中引用相应的漏洞信息，**从而不需要人工去一个个漏洞进行整理**。



* 1. 漏洞引用表（中文漏洞库）

该表的内容为人工整理的Nessus中文漏洞信息，包括Nessus每个漏洞对应的插件ID（唯一值，这里写为“编号”），漏洞的英语名和中文名、风险等级、漏洞说明和加固建议。

该表的内容是用于 “扫描结果” 中引用的。目前该表漏洞条目还不够完善，只有700条漏洞信息（含中危、高危、紧急），已经对内容校验过，但可能还会存在有错误的内容，有看到错误的内容，麻烦反馈一下。



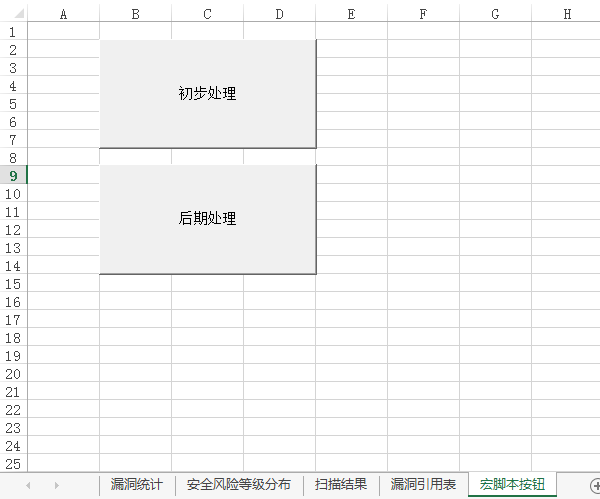
* 1. 宏脚本按钮

目前有两个按钮，“初步处理”和“后期处理”

简单的流程是这样：

1. 点击“初步处理”，筛选出“中文漏洞库”所缺少的条目；
2. 人工补充完善“中文漏洞库”；
3. 点击“后期处理”，生成最终报告。

PS:如果无缺少的漏洞条目，执行完“初步处理”后，会自动调用“后期处理”脚本。



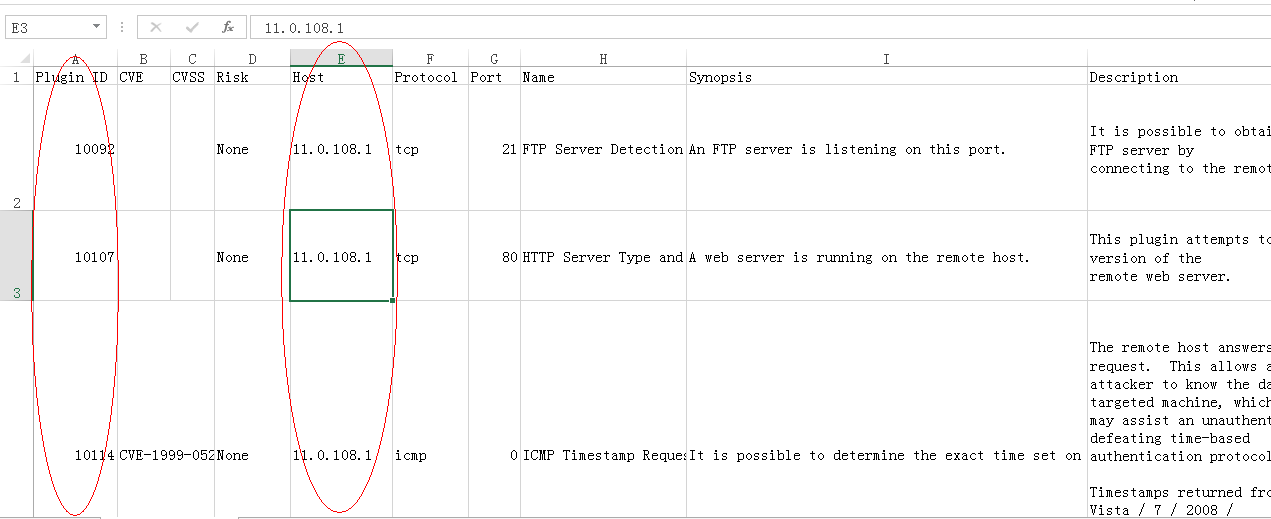
按钮页面不太美观，会美化的伙伴可以帮忙一下^\_^

1. 使用步骤
   1. 在Nessus中导出CSV格式的报告

报告如图所示：

我们会需要用到里面的Plugin ID 、 Host、port、CVE、Plugin Output等，

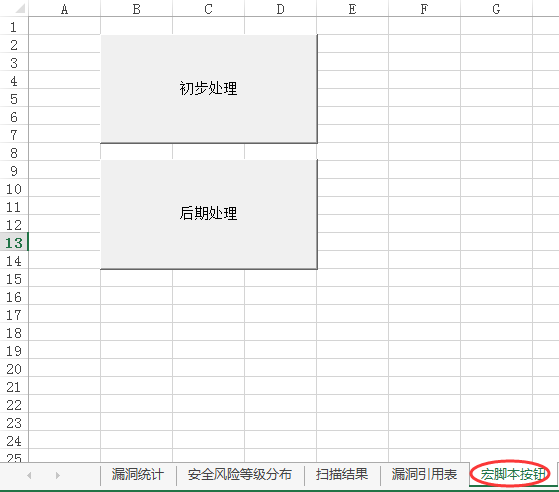
即包含存在漏洞的插件编号、主机IP、端口号、CVE编号及判断漏洞的相应输出结果



注意：导出来的CSV格式文件，请勿修改后缀名.csv

* 1. 自动生成中文的“扫描结果”表（初步处理）

1. 关闭其他无关的excel文件，
2. 打开报告模板《Nessus 中文报告自动生成.xlsm》，
3. 打开csv文件（使用excel程序打开），
4. 查看报告模板中，“宏脚本按钮”，可看到按钮“初步处理”，如下图：

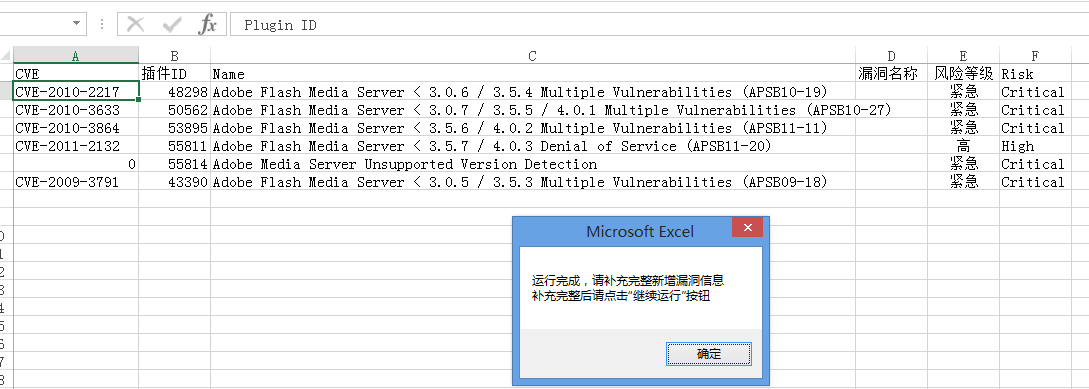


1. 单击按钮“初步处理”，将会调用宏脚本“nessus”，然后会自动生成报告。

宏脚本的处理过程包含内容如下：

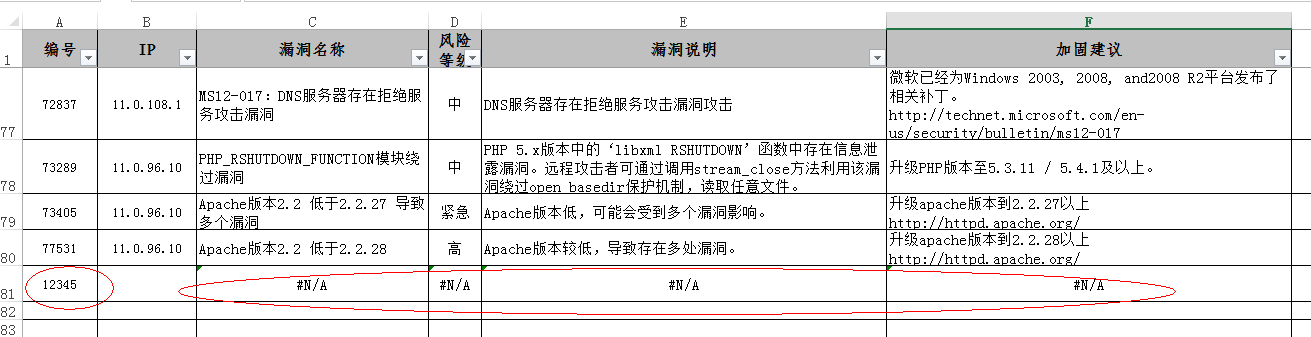
1. 在原始报告csv中，先筛选出“紧急，高危，中危”的漏洞，
2. 将Plugin ID 、 Host、port、CVE、Plugin Output 对应的列复制到最终报告中的表格“扫描结果”，
3. 根据Plugin ID，在“漏洞引用表”查找对应漏洞的中文信息，然后填充到表格“扫描结果”中，
4. 如果本次扫描结果中的漏洞在“漏洞引用表”中均能查找到，将会自动调用“后期处理”。如果出现未能查找到的漏洞，需要在“漏洞引用表”中补充相应的中文漏洞描述。

新漏洞在中文漏洞库未包含时,会筛选出来，如下图：

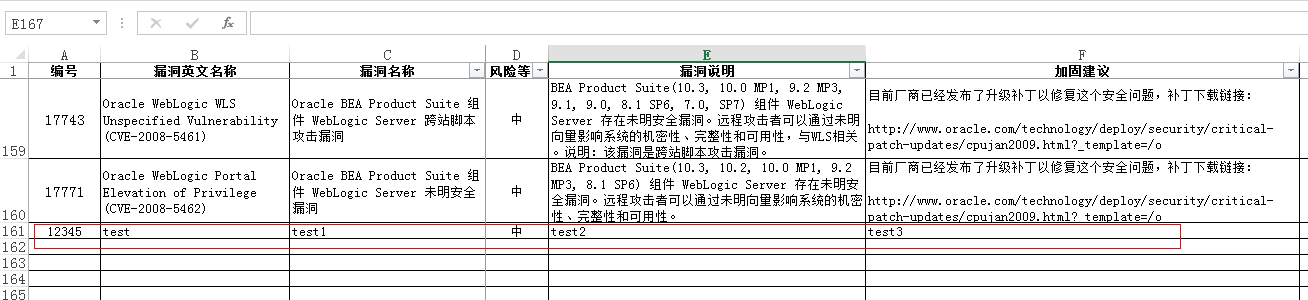


* 1. 完善中文漏洞引用表

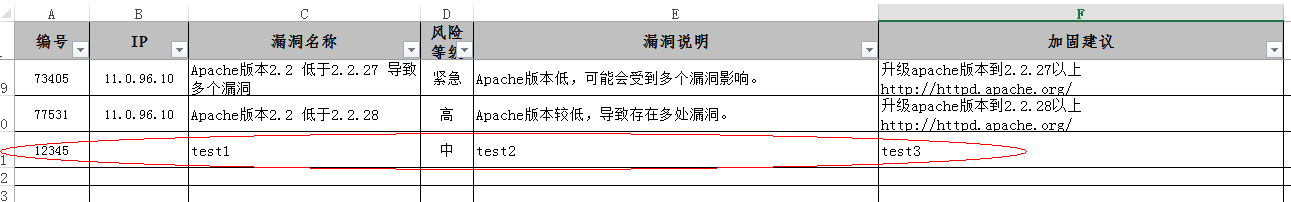
当出现中文漏洞的引用表中未包含的漏洞时，即出现有些Plugin ID 还未有相应的中文描述，如图所示：



显示#N/A 就表示暂时还未整理相应的中文描述，这个时候就需要在“漏洞引用表”中最后一行添加相应的内容，如下：



添加完成之后，查看“扫描结果”表，可以看到自动生成相应的漏洞信息了



注：由于直接把Nessus的整个漏洞库的对应中文描述都整理出来，需要花费非常大的人力成本，而且有些漏洞可能扫描中几乎不会遇到，所以采用每次扫描之后，遇到未添加的项目再进行添加即可。

每次扫描之后需要添加的条目应该不会太多，因为同个环境下，很多漏洞都是重复的，这次实际扫描了500个IP，漏洞有3千多个，整理出来不重复的漏洞也就150个左右。

大家每次扫描完成后，有添加的新中文漏洞描述，麻烦共享到我这里，然后我这边整理汇总起来，定期共享出来给大家。 通过大家在努力，现在中文漏洞库中已包含了700条漏洞，很多情况已经不需要增加新的漏洞了。

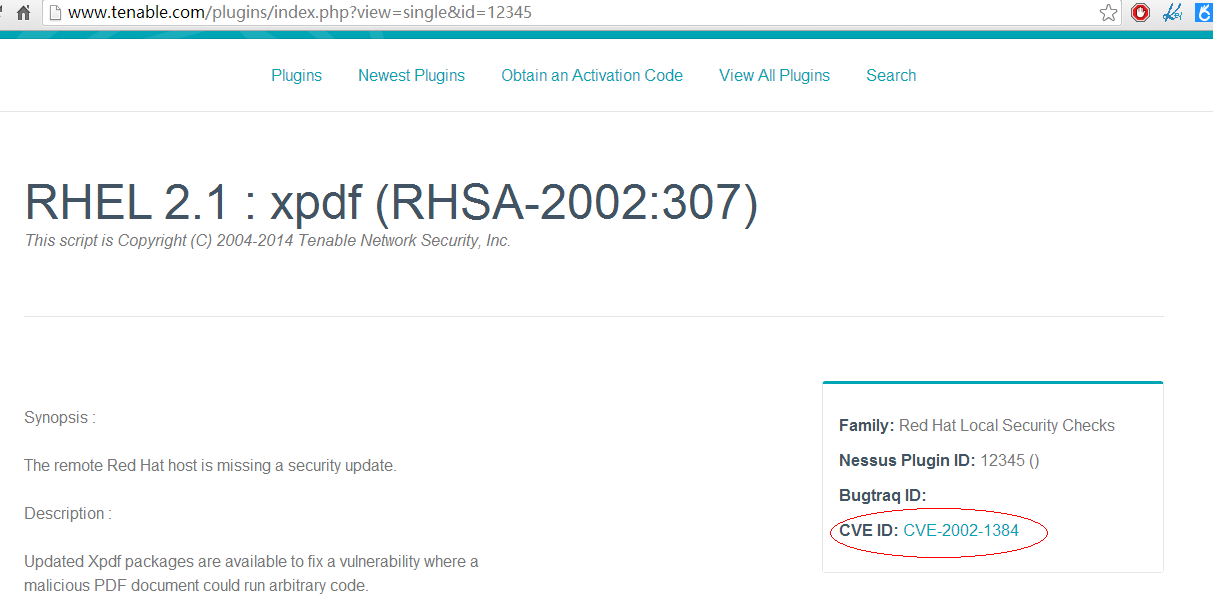
* 1. 新漏洞的中文描述获取

新漏洞的中文描述可按以下步骤获取：（大家有更好有资源的话，求共享）

根据漏洞的Plugin ID 访问，Nessus官网的漏洞详情，地址如下：

http://www.tenable.com/plugins/index.php?view=single&id=12345

参数id 大家可自行修改。



根据相应的CVE 编号获取中文描述，地址如下：

http://cve.scap.org.cn/CVE-2002-1384.html



建议查看CNNVD的

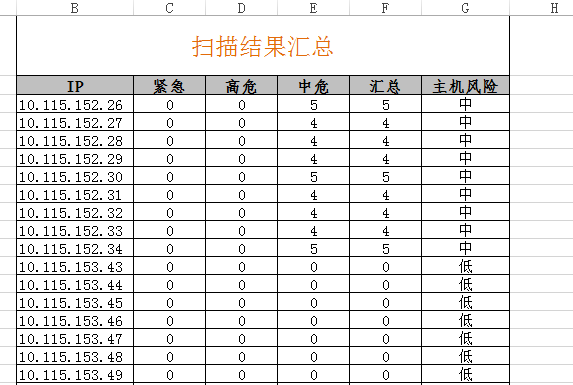


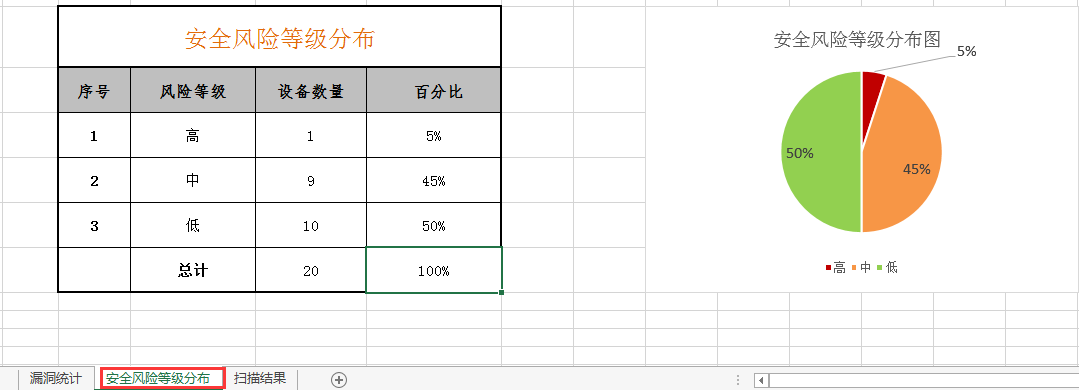
* 1. 报告后期处理

在补充完新漏洞的中文描述后，点击“后期处理”按钮，继续完成中文报告生成，得到最终报告。

“后期处理”的宏脚本包含以下内容：

1. 自动对扫描结果进行统计





1. 自动把表格中使用“公式”转为具体的值，即“公式的计算结果”。
2. 删除子表删除“漏洞引用表”和“宏脚本按钮”
3. 补充说明

该“中文报告自动生成模板”经过多人的使用反馈，在原有的基础上做出不少的优化，从而使得使用更加方便。当然，还有好多可以优化的地方，欢迎大家多提意见，让这个Nessus中文报告自动的小工具越来越方便。

最后感谢志伟、凤玲、雪琴、少波、挺达等，帮忙使用并测试，提供了大量的反馈，帮助不断优化。

有什么问题欢迎随时联系

林坤潮

微信:13822234124