**测评能脚2**

**用户手册**

# 使用须知

* 适用报告：测评能手导出的2.0等保报告、2.0等保方案、2.0PRO报告
* 未设置任何异常处理及告警，按错没有后悔药
* 尽量在导出报告后第一时间使用，尽量不要重复使用
* 测试版本，不负责售后，出bug请自行改代码及参数（右键dotm，选择**打开**，按Alt+F11可看到源码）

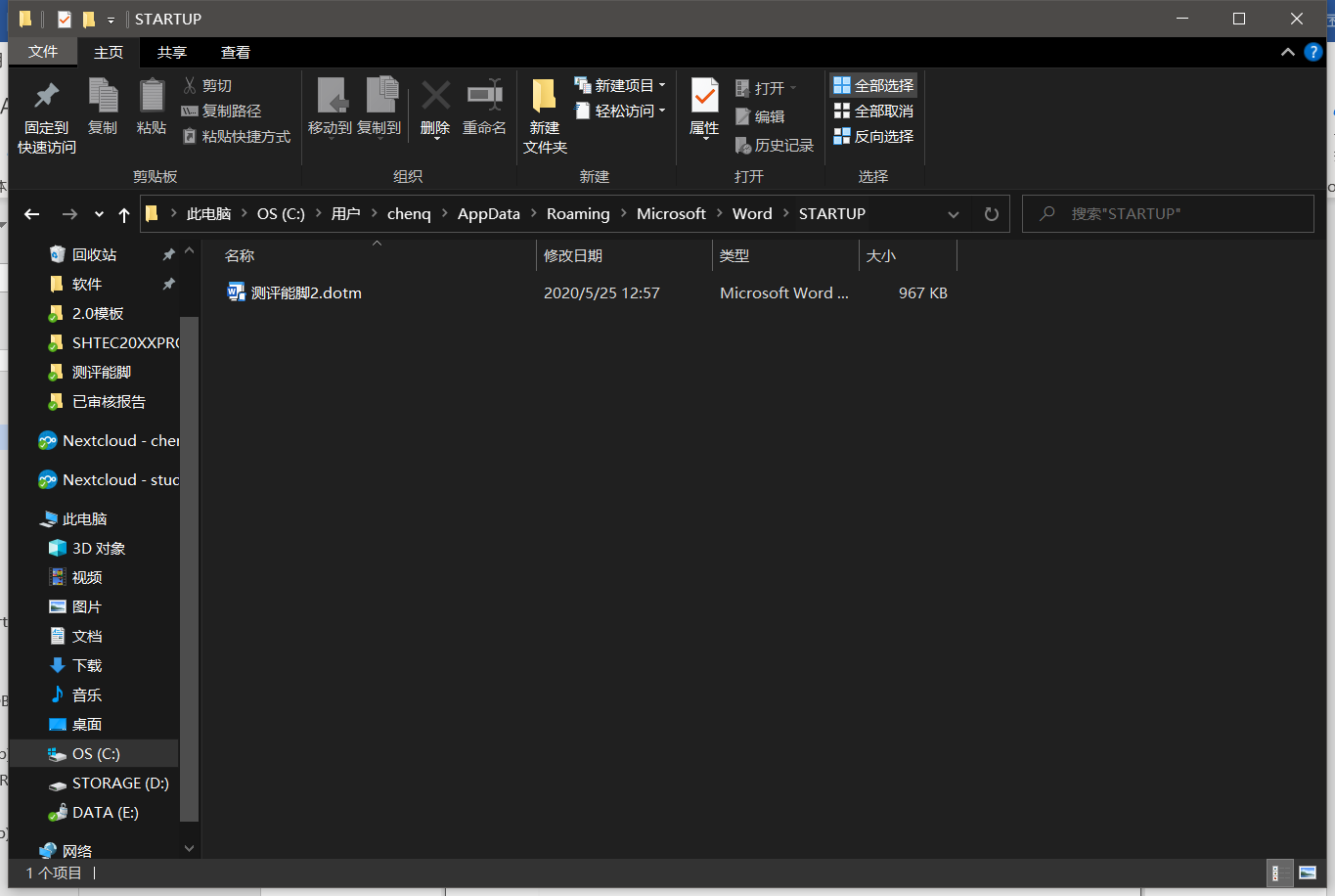
# 安装

## 复制文件

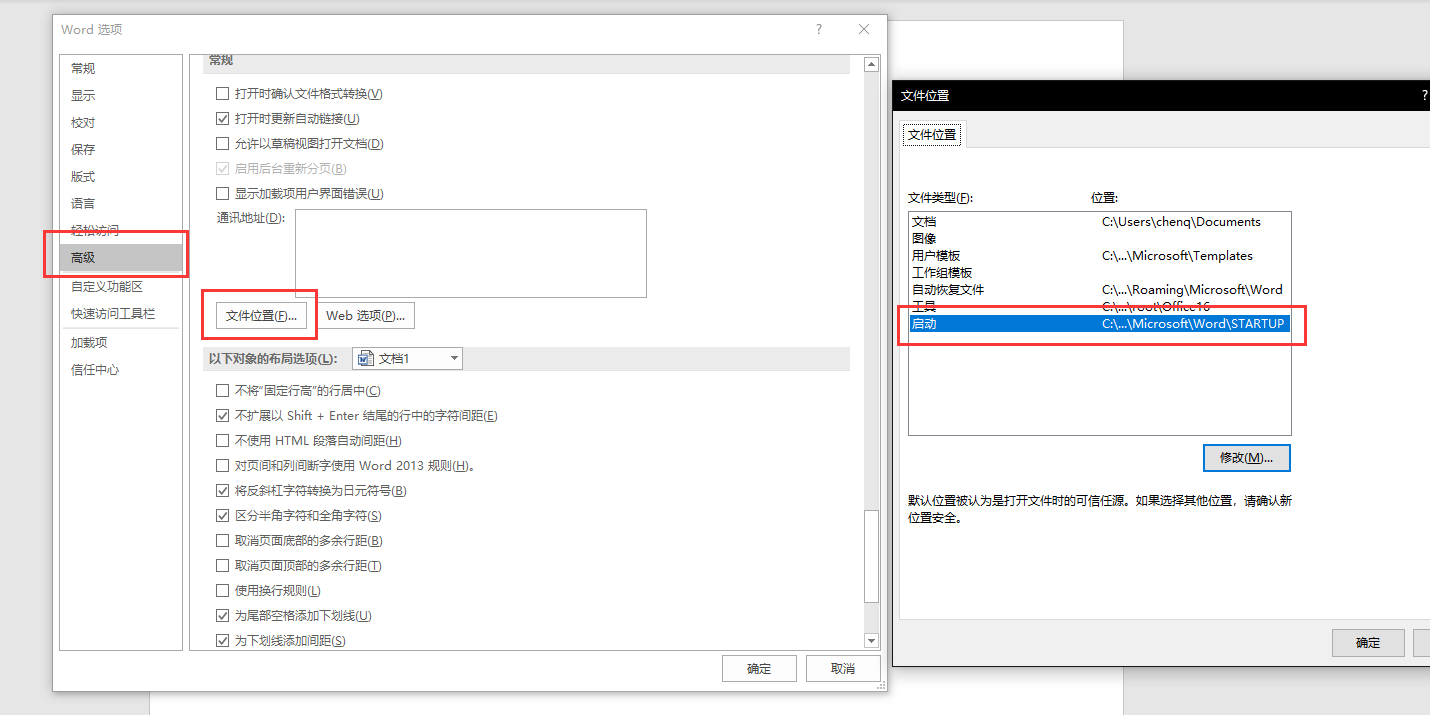
将文件“测评能脚2.dotm”复制到以下目录，**并重启Word。**

C:\Users\[当前用户]\AppData\Roaming\Microsoft\Word\STARTUP\

**注1：**AppData为隐藏目录，进入C:\Users\[当前用户]文件夹之后，直接复制\AppData\Roaming\Microsoft\Word\STARTUP\到地址栏即可访问。



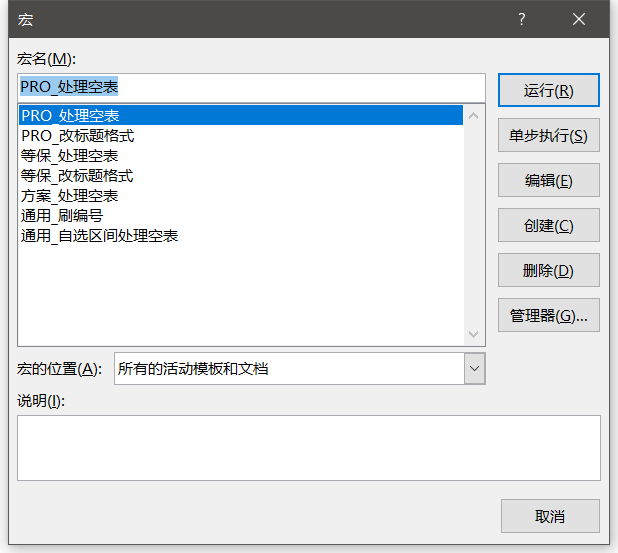
**注2：**若无法找到STARTUP文件夹，则打开“选项-高级”，打开“常规”下的“文件位置”功能，其中“启动”的内容即为所需的文件夹。



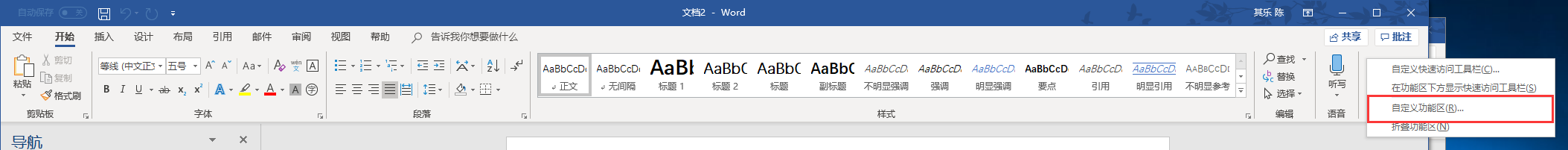
# 使用

## 快捷键调用

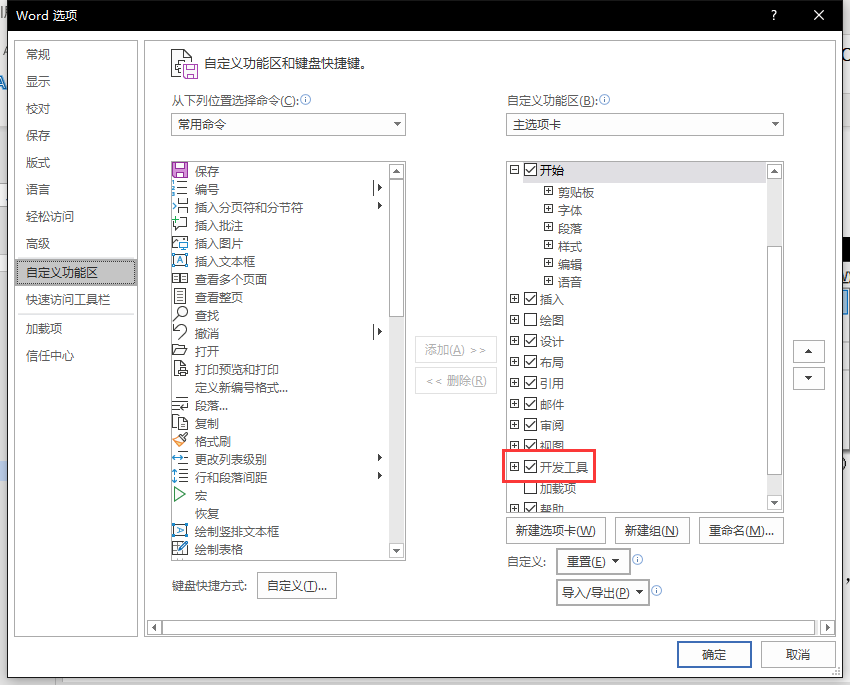
按Alt+F8，打开“宏”菜单，根据需要运行列表中的宏，具体宏功能详见第三章



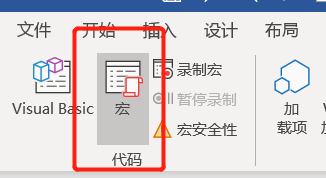
## 按钮调用



在菜单栏任意空白处右键，打开“自定义功能区”。



勾选“开发工具”



点击“宏”，可打开同样的界面，也可右键把该按钮“添加到快速访问工具栏”

# 功能详情

## 通用

### 图表重新编号(FieldUpdate.Main)

根据预定义的域情况，将正文及附件的所有图表重新编号。

注1：**不！要！手！改！**报告里的编号

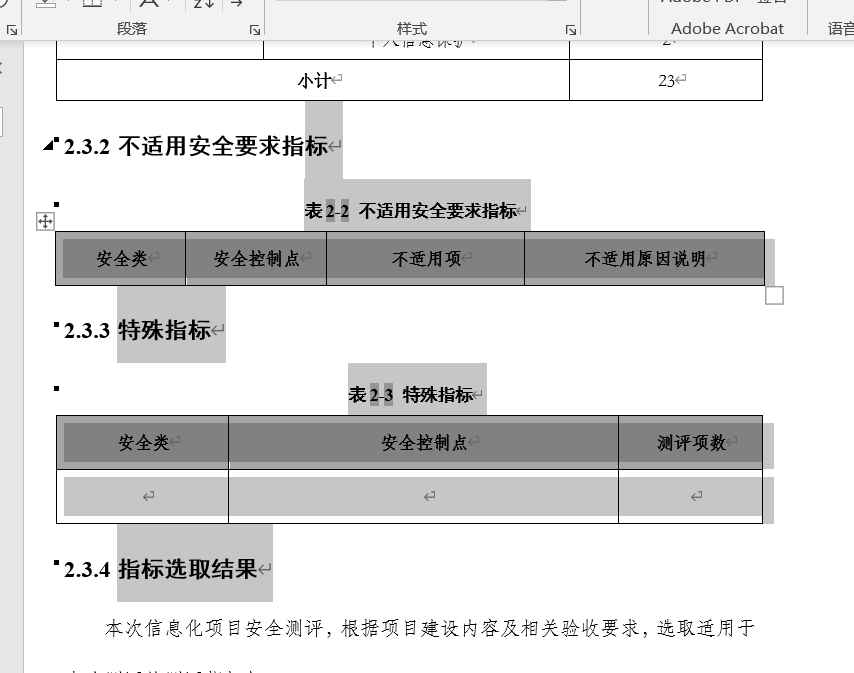
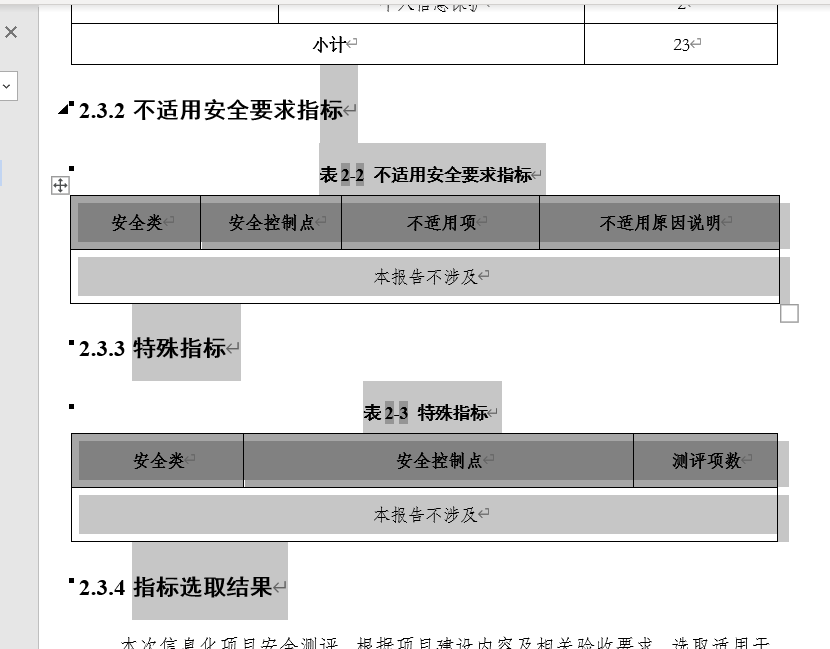
注2：如果要加图或者表，请复制已有的题注，“更新域”后会自动连续编号

注3：全选，按F9，起到同样作用

注4：宏无法自动刷新目录和索引（垃圾微软没提供API），请手刷

### 处理空表(DeleteTable.ManualMain)

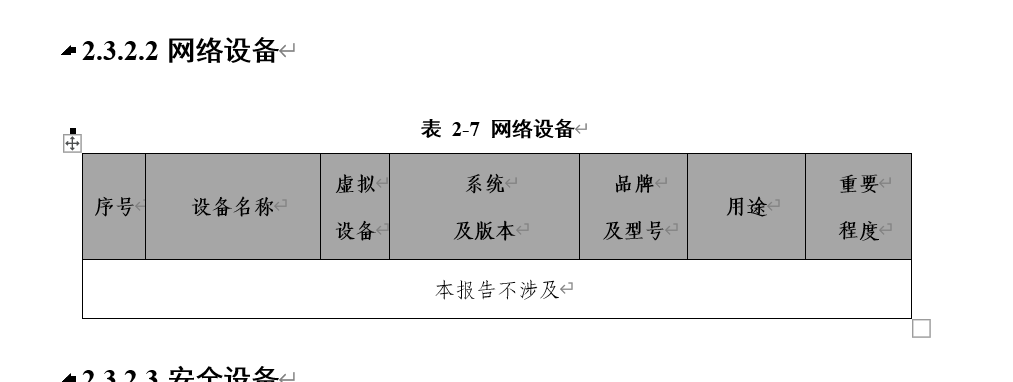
处理**光标选择范围内**的所有表格，在空表下方加入“本报告不涉及”

## 等保

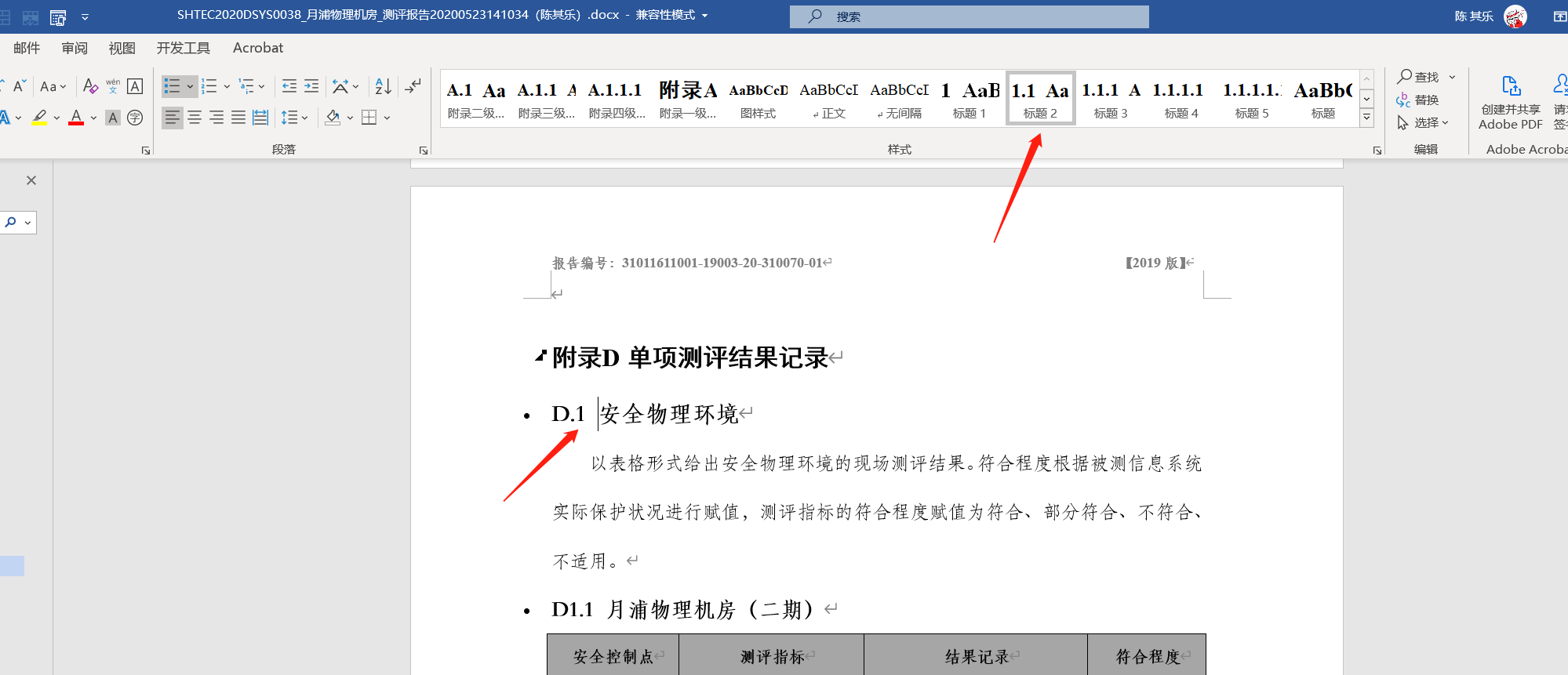
### 处理空表(DeleteTable.DBMain)【因改版暂时废弃】

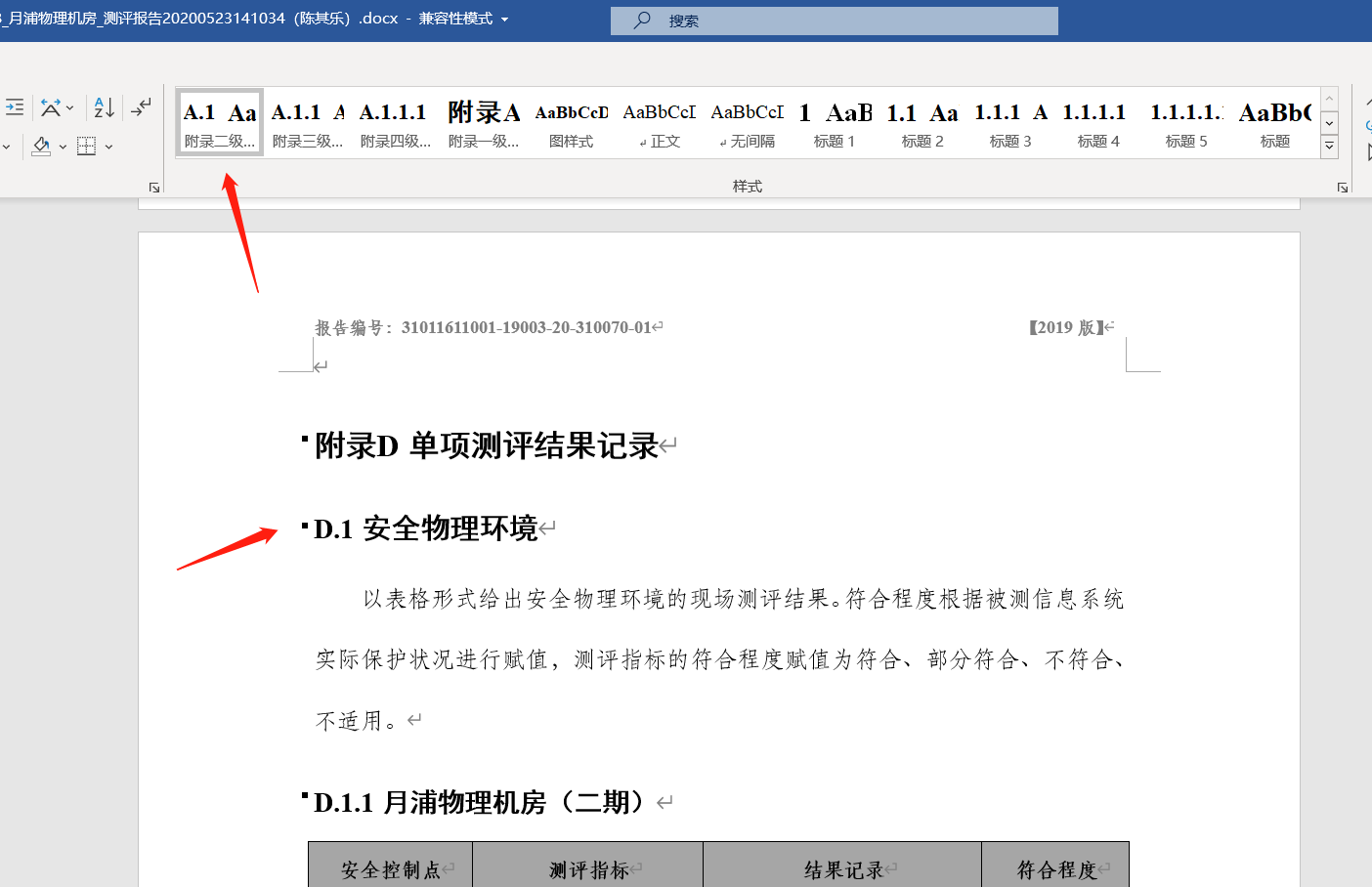
在“2.3.2测评对象选择结果”及“附录A被测对象资产”中，自动侦测所有空表，并在下方加入“本报告不涉及”



### 修改测评记录标题样式(TitleStyle.DBMain) 【已废弃】

将附录D的标题样式从“标题 2”、“标题 3”改为“附录二级标题”、“附录三级标题”并加入自动连续编号





### 修改附录C样式(Attachment.DBMain)

将测评能手导出的验证测试报告修改为等保模板的格式

**注1：**必须使用原生报告，不能有任何修改。脚本修改时不会写入原始文件，而是新建一份新的文档。

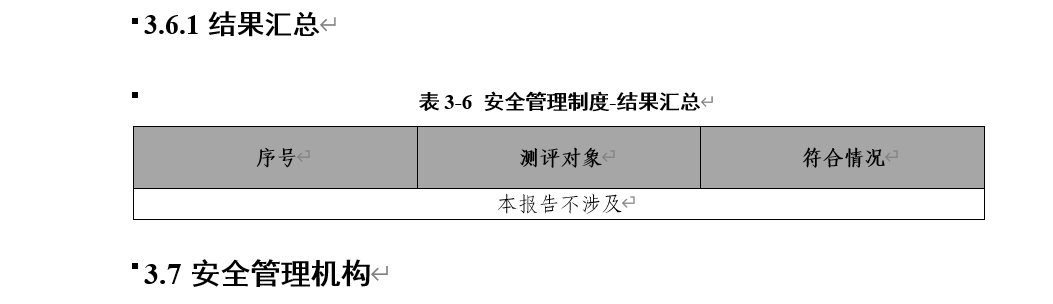
**注2：**技术上无法追溯整改前的资产。当某个资产整改了漏洞后，将无法显示在“漏洞详情-涉及信息资产”模块中，请手动添加。同理，部分整改的情况将显示为“未整改”。

## PRO

### 处理空表(DeleteTable.PROMain)

在“2.3.2测评对象选择结果”、“4 单项测评汇总”及“附录A被测对象资产”中，自动侦测所有空表，并删除

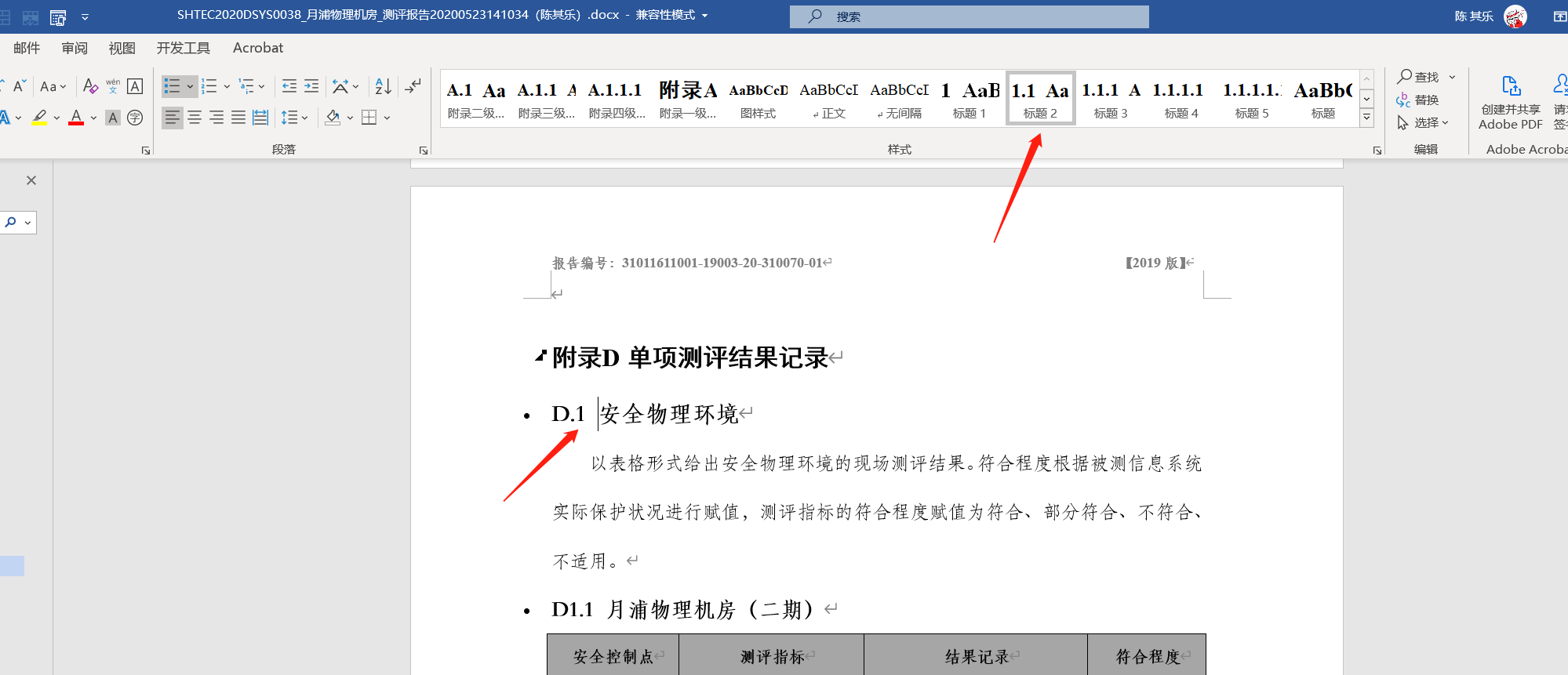


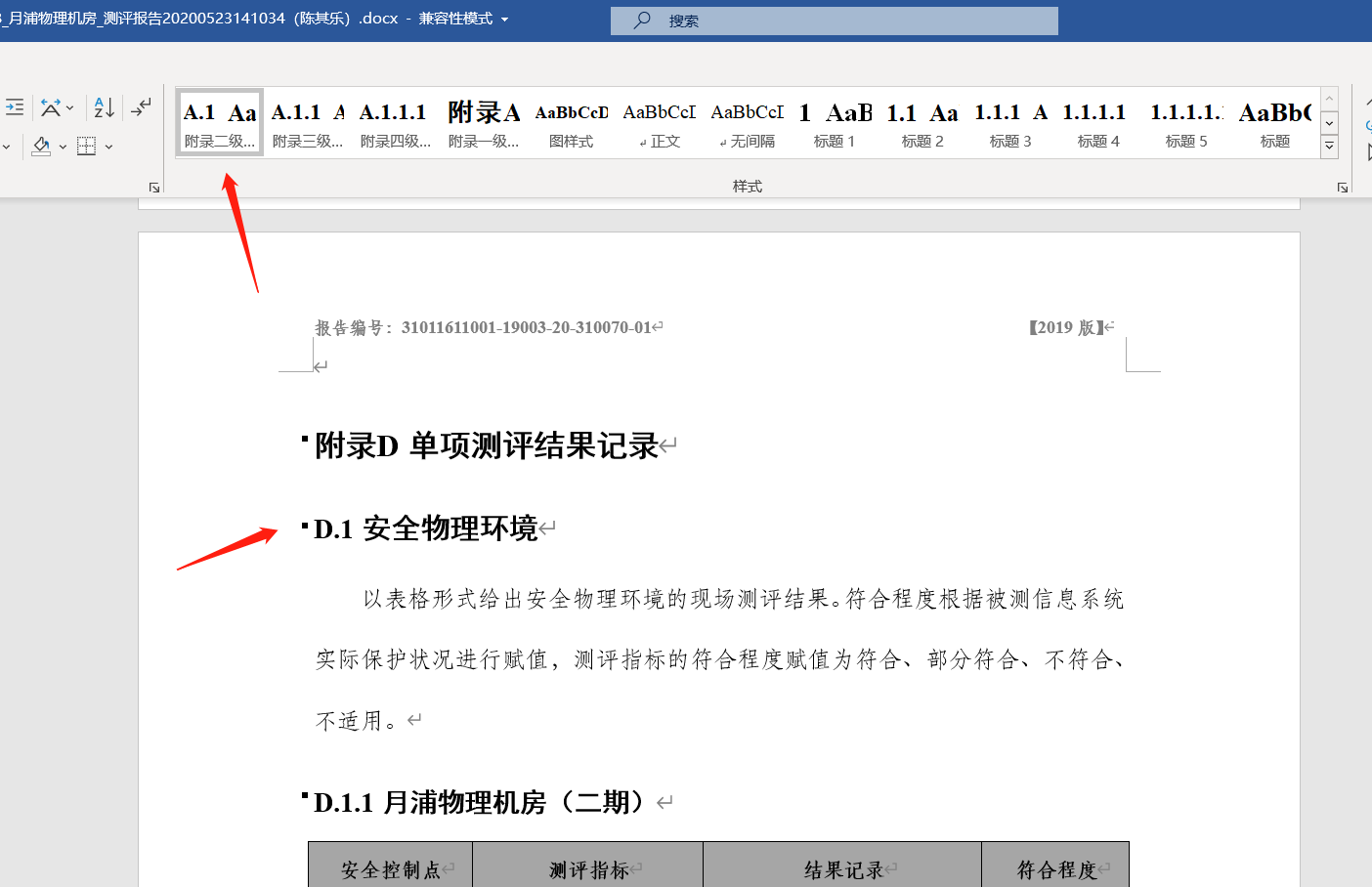




### 修改测评记录标题样式(TitleStyle.PROMain) 【已废弃】

将附录B的标题样式从“标题 2”、“标题 3”改为“附录二级标题”、“附录三级标题”并加入自动连续编号



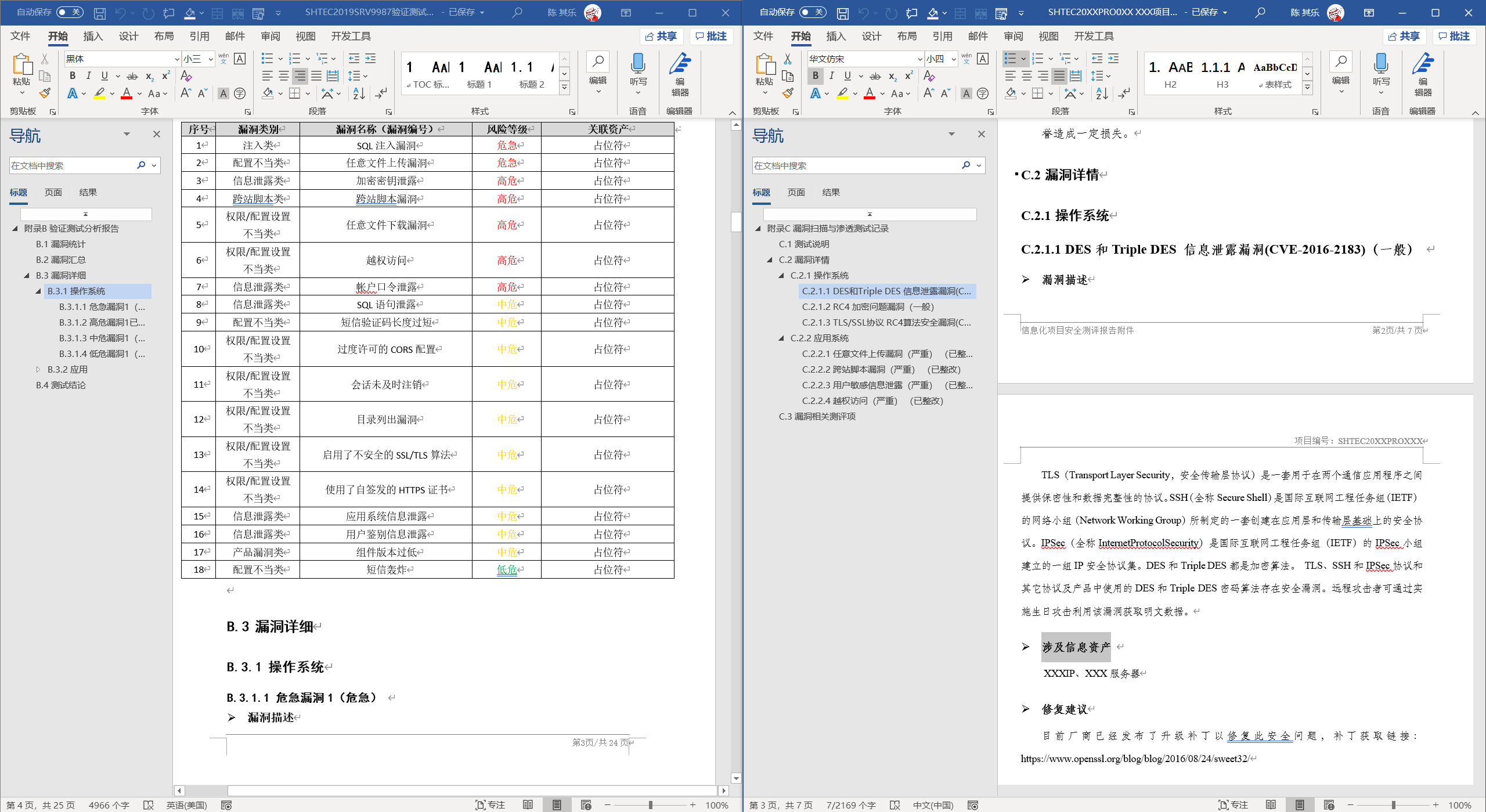


### 修改附录C样式(Attachment.PROMain)

将测评能手导出的验证测试报告修改为PRO模板的格式

**注1：**必须使用原生报告，不能有任何修改。脚本修改时不会写入原始文件，而是新建一份新的文档。

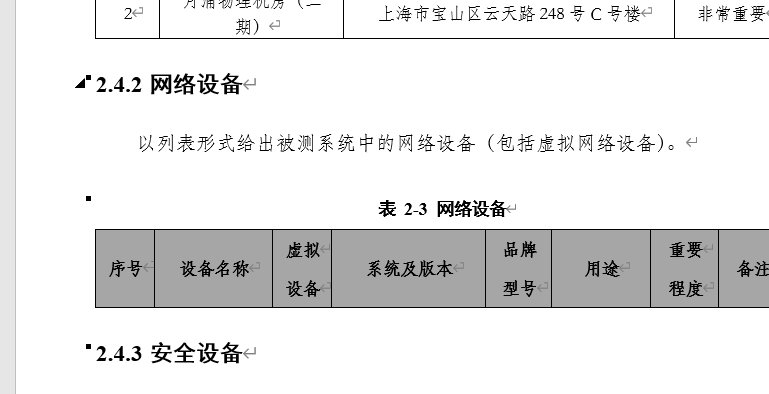
**注2：**技术上无法追溯整改前的资产。当某个资产整改了漏洞后，将无法显示在“漏洞详情-涉及信息资产”模块中，请手动添加。同理，部分整改的情况将显示为“未整改”。

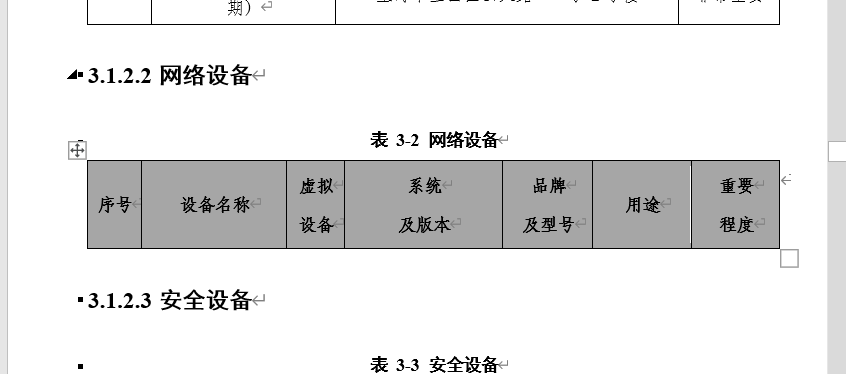


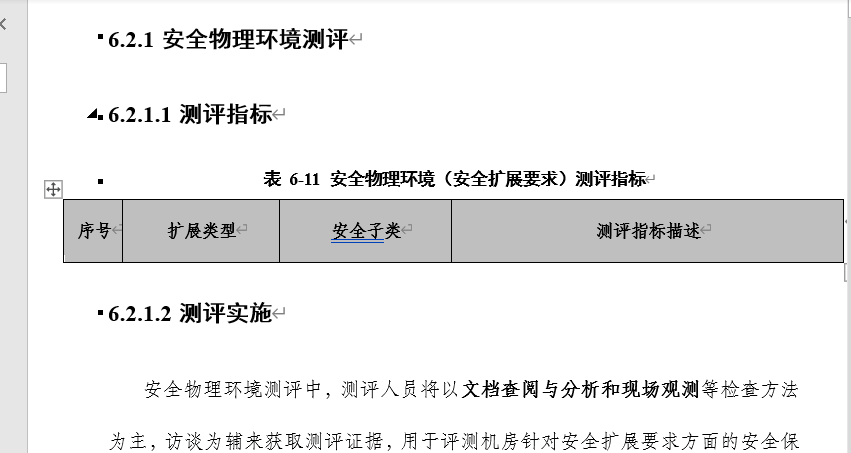
## 等保方案

### 处理空表(DeleteTable.PlanMain)

在“2.4 系统构成”、“3.1.2测评对象选择结果”及“6.2 扩展安全要求”中，自动侦测所有空表，并在下方加入“本方案不涉及”







# PRO Known Issues

1. 漏洞扫描与渗透测试记录

**测试说明**

* 测试分析所发现的【占位符：C1层面】漏洞和弱点，是基于已公开发布的有关应用、系统的漏洞和弱点，由测试工具得出的结论，不能代表系统实际存在的全部问题。另一方面，系统的漏洞和弱点将随着系统策略的调整、软件升级和配置的改变等而发生变化，因此本次测试的结果仅作为本次系统安全测评的必要验证，供管理人员配置系统时参考。请管理员根据实际情况处理。
* Web应用扫描工具是以抽样方式对目标Web系统进行安全扫描，经测试发现的问题并不能完全代表目标存在的所有安全漏洞。建议管理员根据已发现的安全漏洞举一反三，结合漏洞的攻击原理分析目标所有页面，确保类似安全漏洞不在目标Web系统中出现。
* 基于影响严重程度的安全漏洞分级定义。严重级别的安全漏洞：安全漏洞一旦被攻击者成功利用，可对目标对象造成严重影响或后果的漏洞，给予用户方经济或声誉造成严重损失。一般级别的安全漏洞：安全漏洞一旦被攻击者成功利用，可对目标对象造成一定影响或后果的漏洞，给予用户方经济或声誉造成一定损失。
  1. 漏洞详情
  2. 漏洞相关测评项

表 C-1 测评项与相关漏洞

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **安全类** | **测评项** | **相关漏洞** |
| 1 | 安全计算环境 | 入侵防范：应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求。 |  |
| 2 | 入侵防范：应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。 |  |

* 1. 【需删除】报告正文使用的内容

（尚未整改的安全漏洞数量统计表）

【占位符：C4漏洞表】

通过测试发现XXX公司的XXX平台目前仍存在以下漏洞：【占位符：C4漏洞名称】。

* + 1. 【占位符：C2层面】
       1. 【占位符：C2漏洞名称】（【占位符：C2漏洞风险】）（已整改）
* **漏洞描述**

【占位符：C2漏洞描述】

【占位符：C2图】

图 C-1 【占位符：C2漏洞名称】

* **涉及信息资产**

【占位符：C2漏洞资产】

* **修复建议**

【占位符：C2漏洞建议】

* **整改情况**

【占位符：C2漏洞整改】

1. 漏洞扫描结果记录

**测试说明**

* 测试分析所发现的【占位符：E1层面】漏洞和弱点，是基于已公开发布的有关应用、系统的漏洞和弱点，由测试工具得出的结论，不能代表系统实际存在的全部问题。另一方面，系统的漏洞和弱点将随着系统策略的调整、软件升级和配置的改变等而发生变化，因此本次测试的结果仅作为本次系统安全测评的必要验证，供管理人员配置系统时参考。请管理员根据实际情况处理。
* Web应用扫描工具是以抽样方式对目标Web系统进行安全扫描，经测试发现的问题并不能完全代表目标存在的所有安全漏洞。建议管理员根据已发现的安全漏洞举一反三，结合漏洞的攻击原理分析目标所有页面，确保类似安全漏洞不在目标Web系统中出现。
  1. 漏洞汇总

采用风险分析的方法分析系统安全测评结果中存在的安全问题可能被威胁利用的可能性和后果，综合判定给出信息系统面临的风险。漏洞情况汇总见表E-1、E-2、E-3：

* 1. 漏洞详情
  2. 【需删除】报告正文使用的内容

（接入点漏洞扫描结果统计表）

【占位符：E3漏洞表】

通过测试发现XXX公司的XXX平台目前仍存在以下漏洞：【占位符：E3漏洞名称】。

* + 1. 【占位符：E2层面】
       1. 【占位符：E2漏洞名称】（【占位符：E2漏洞风险】）（已整改）
* **漏洞描述**

【占位符：E2漏洞描述】

【占位符：E2图】

图 E-2 【占位符：E2漏洞名称】

* **修复建议**

【占位符：E2漏洞建议】