



隐写术

AppLeU0
2015.4.18

sycløver

whoami

AppLeU0

Syclover

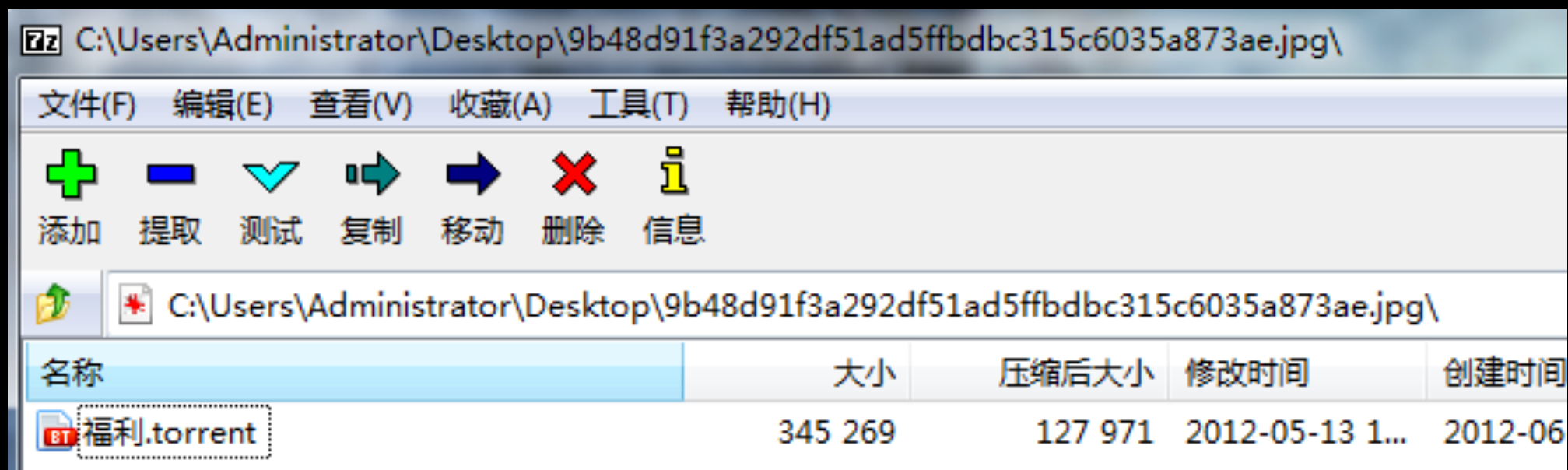
Web、渗透

CTF赛棍

隐写术

.....

图种



copy

```
C:\Users\Administrator\Desktop>copy /b 1.jpg+福利.rar new.jpg  
1.jpg  
福利.rar  
已复制                1 个文件。
```

copy /b 1.jpg+福利.rar new.jpg

binwalk

```
root@kali:~/Desktop/tmp# binwalk zip.jpg
```

DECIMAL	HEX	DESCRIPTION

29343	0x729F	Zip archive data, at least v1.0 to extract, compressed size: 13, uncompressed size: 13, name: "flag.txt"
29506	0x7342	End of Zip archive

EOI

End Of Image

000036C0	B9 6D 82 ED 60 AD 8F 52 6A 2E 7F E7 A3 7F DF 34	算傢~?.Rj..??8?弟
000036D0	5A 31 92 D9 1D F0 59 BA 9C 75 A9 F7 9F 45 FC 85	Z1拚.??Y?渦 炓u...
000036E0	0D 59 D8 6D 1F FF D9	.Y穀. ?

图像部分:

0XFF -> 0xFF 0x00

LSB

Least Significant Bit 最低有效位

颜色	二进制	十进制
红	11111110	254
绿	00000000	0
蓝	00000000	0

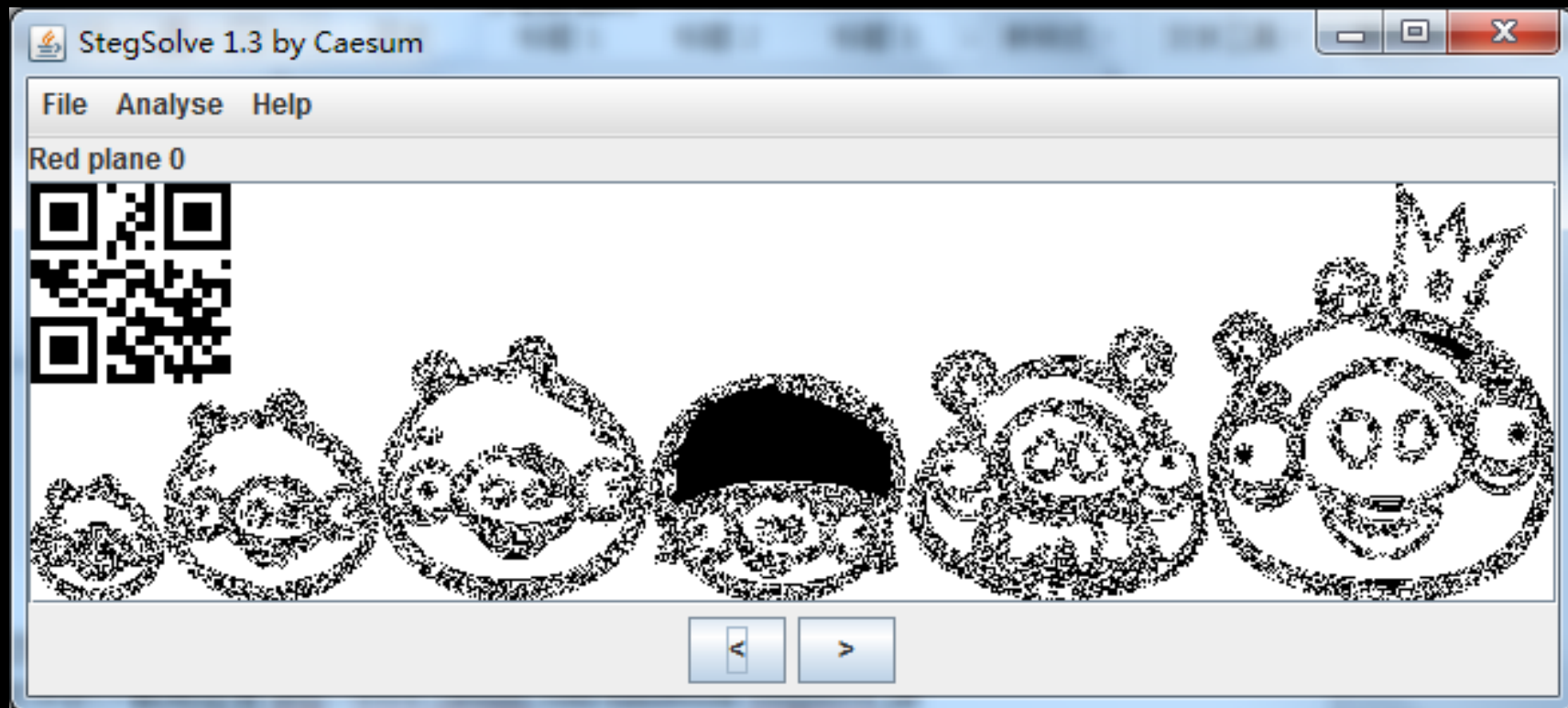
红

十进制

1111111	0
0000000	1
0000000	1
1111111	0
0000000	0
0000000	0
0000000	0
0000000	1

最低有效位 十六进制 ASCII码
01100001 = 0x61 = A

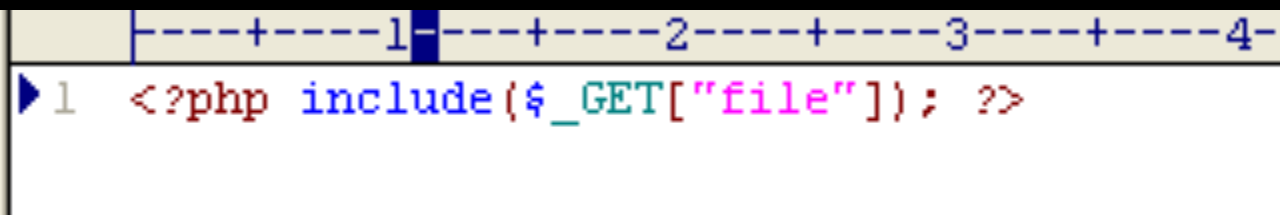
Stegsolve



无损压缩

LFI漏洞

上传图片，配合LFI漏洞



```
1 <?php include($_GET['file']); ?>
```

绕过一些waf、老版本的安全狗

解析漏洞

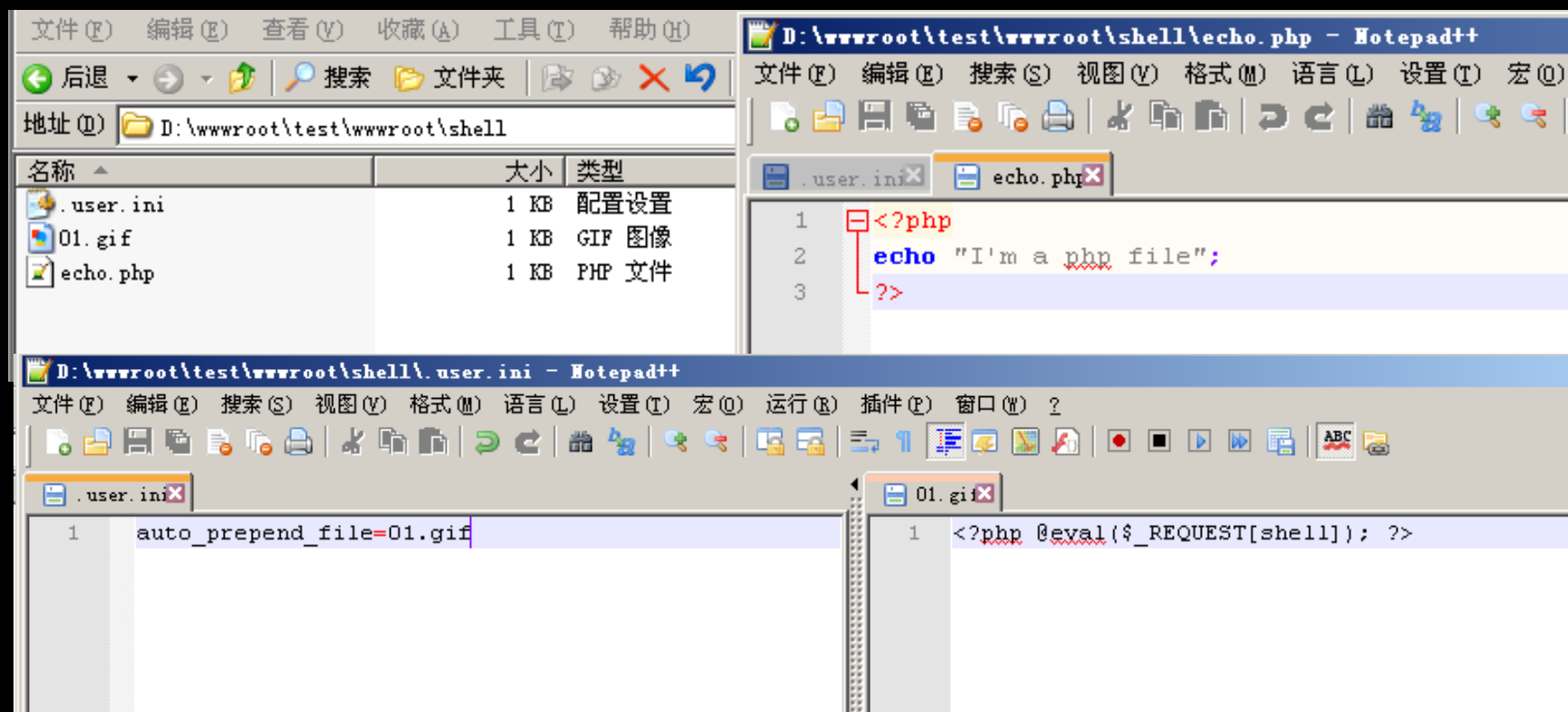
nginx解析漏洞

upload.jpg/1.php

<http://www.80sec.com/nginx-securit.html>

auto_prepend_file

留后门的时候，使用这个技巧



exif信息



30% 1:1

路径: C:\Users\Administrator\Desktop\
文件名称: 示例图片_03.jpg
图像尺寸: 333 x 500, 72dpi
文件大小: 86879 byte
创建时间: 2015-04-03 15:39:08
修改时间: 2011-02-12 15:52:02

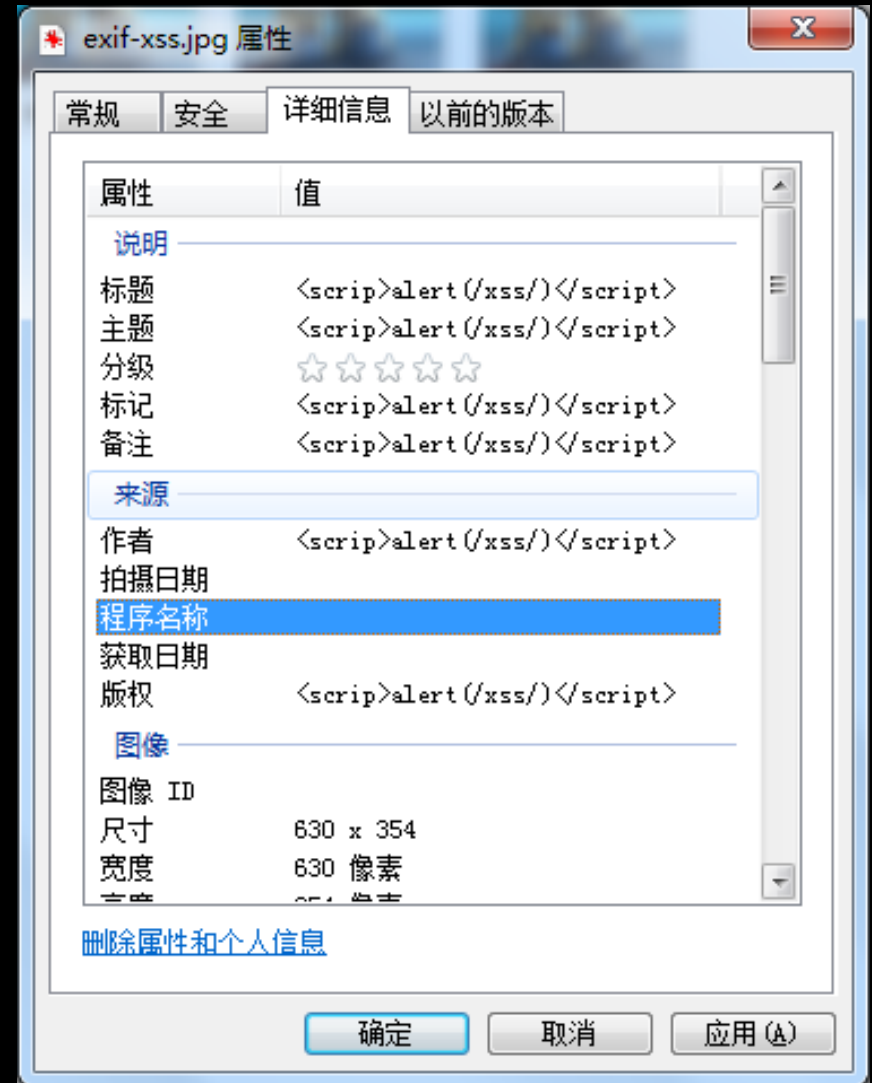
编辑 添加 标记删除 恢复删除

项目	内容	代码	Exif 规范名称	数据类型	数值
[-] 图像信息					
• 方向	上/左	0112	Orientation	SHORT	
• 软件	Adobe Photoshop CS4 Win...	0131	Software	ASCII	
• 修改时间	2009-05-07 14:56:51	0132	DateTime	ASCII	
[-] 相机拍摄记录					
• 色彩空间	未校准	A001	ColorSpace	SHORT	
• Exif 图像宽度	333	A002	ExifImageWidth	LONG	
• Exif 图像高度	500	A003	ExifImageHeight	LONG	
[-] 缩略图					
• 缩略图像	107 x 160	0001	Thumbnail	UNDEFIN...	* 5

exif导致的xss

[http://
www.wooyun.org/bugs/
wooyun-2010-07468](http://www.wooyun.org/bugs/wooyun-2010-07468)

DiscuzX2个人空间图片
EXIF信息XSS



Exif留后门

exif_read_data

```
array
  'html' => string 'width="630" height="354"' (length=24)
  'Height' => int 354
  'Width' => int 630
  'IsColor' => int 1
  'ByteOrderMotorola' => int 1
  'Exif_IFD_Pointer' => int 2134
  'Title' => string 'phpinfo();' (length=10)
  'UndefinedTag:0xEA1C' => string '????????????????????????????????????????????????????????????'
```

PHP Version 5.3.10



System	Windows NT CHINA-0C85B62AC 5.1 build 2600 (Windows XP Professional Service Pack 3) i586
Build Date	Feb 2 2012 20:26:31
Compiler	MSVC9 (Visual C++ 2008)
Architecture	x86

安卓

阿里移动安全挑战赛
演示

mp3stego

```
C:\Users\Administrator\Desktop\MP3Stego>encode -E wooyun.txt -P wooyun mp3stego.
wav mp3stego.mp3
MP3StegoEncoder 1.1.17
See README file for copyright info
Microsoft RIFF, WAVE audio, PCM, stereo 48000Hz 16bit, Length: 0: 0:22
MPEG-I layer III, stereo Psychoacoustic Model: AT&T
Bitrate=128 kbps De-emphasis: none CRC: off
Encoding "mp3stego.wav" to "mp3stego.mp3"
Hiding "wooyun.txt"
[Frame 938 of 938] (100.00%) Finished in 0: 0: 0
```

加密

mp3stego

```
C:\Users\Administrator\Desktop\MP3Stego>decode -X -P wooyun mp3stego.mp3
MP3StegoEncoder 1.1.17
See README file for copyright info
Input file = 'mp3stego.mp3' output file = 'mp3stego.mp3.pcm'
Will attempt to extract hidden information. Output: mp3stego.mp3.txt
the bit stream file mp3stego.mp3 is a BINARY file
HDR: s=FFF, id=1, l=3, ep=off, br=9, sf=1, pd=0, pr=0, m=0, js=0, c=0, o=0, e=0
alg.=MPEG-1, layer=III, tot bitrate=128, sfrq=48.0
mode=stereo, sblim=32, jsbd=32, ch=2
[Frame 938]Avg slots/frame = 383.593; b/smp = 2.66; br = 127.864 kbps
Decoding of "mp3stego.mp3" is finished
The decoded PCM output file name is "mp3stego.mp3.pcm"
```

解密

Q&A

EOF

2015.4.18