

EXIF : Sensitive Data Exposure

What is EXIF Metadata?

EXIF stands for Exchangeable Image File Format. It is a record which shows the digital SLR camera settings used to take a particular photograph. This data is recorded into the actual image file.

Therefore each photograph has its own unique data. EXIF data shows photo information such as camera model, exposure, aperture, ISO, what camera mode was used and whether or not a flash fired. The below image is an example of how EXIF Metadata looks like.

Camera:	Canon EOS 400D Digital
Exposure:	0.005 sec (1/200)
Aperture:	f/11
Focal Length:	100 mm
ISO Speed:	100
Exposure Bias:	0/3 EV
Flash:	Flash fired
Orientation:	Horizontal (normal)
X-Resolution:	72 dpi
Y-Resolution:	72 dpi
Software:	Adobe Photoshop CS2 Windows
Date and Time:	2008:01:06 20:59:54
YCbCr Positioning:	Co-Sited
Exposure Program:	Manual
Date and Time (Original):	2008:01:06 14:47:06
Date and Time (Digitized):	2008:01:06 14:47:06
Shutter Speed:	500948/65536
Metering Mode:	Pattern
Color Space:	sRGB
Focal Plane X-Resolution:	4433.295 dpi
Focal Plane Y-Resolution:	4453.608 dpi
Exposure Mode:	Manual
Compression:	JPEG

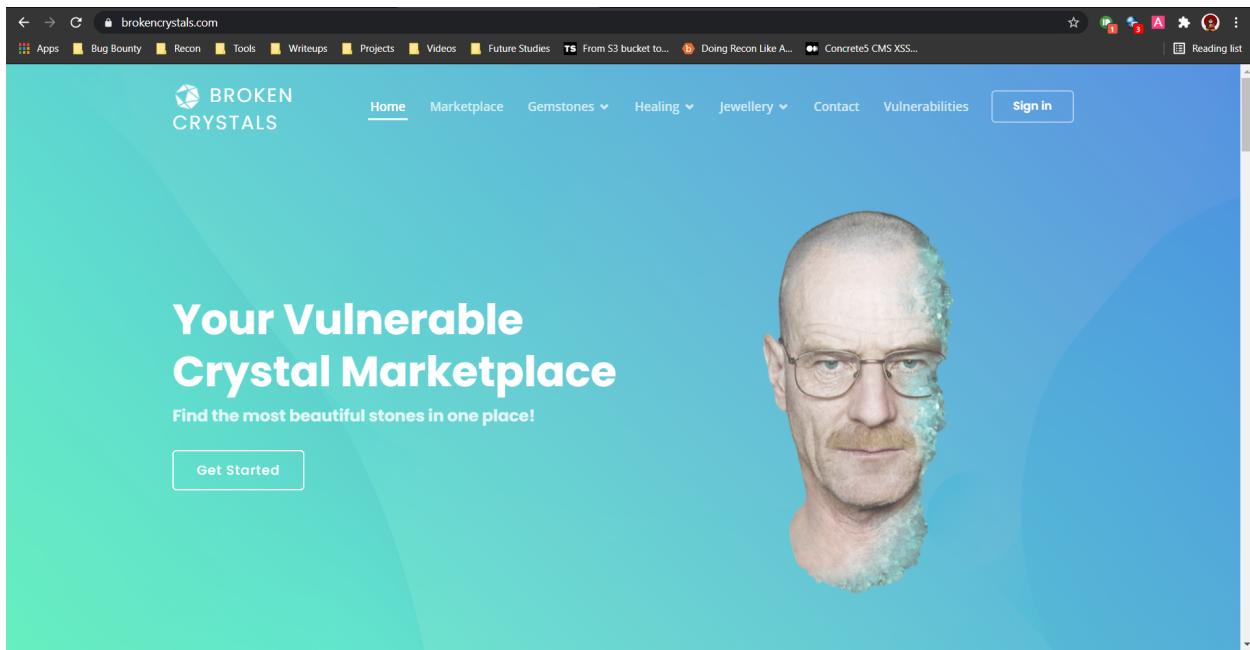
What is EXIF Data Exposure?

EXIF Data stores sensitive information like Geo-location, Date, Name of the camera, Modified date, Time, Sensing Method, File Source, Type of compression etc. in the photos you click. Now this data resides in the every photo you take using cameras.

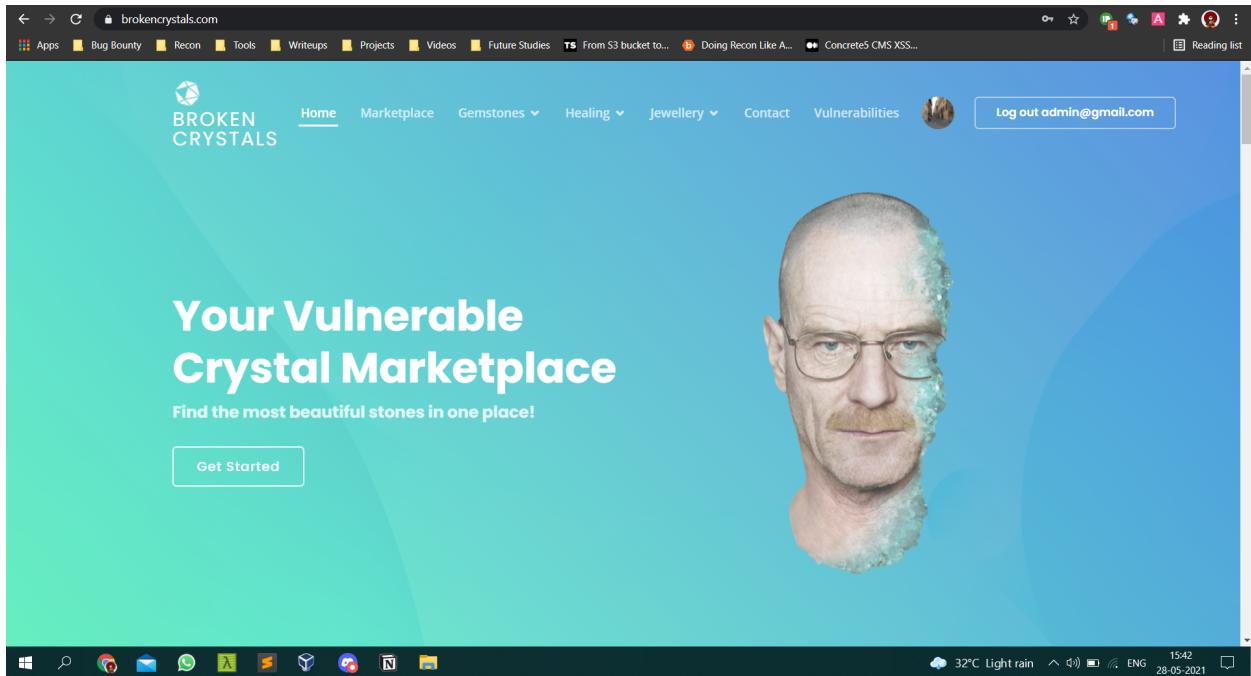
Whenever you upload a picture on a website and if the website does not strip these sensitive data then this could lead to sensitive data exposure like the Geo-location, Date of the photo, Time of the photo, Camera used etc.

Let's understand using an example

So currently I am on a vulnerable website which is: <https://brokencrystals.com>



Let's quickly Sign In!



Notice we can upload an image! Let's quickly upload an image which contains some sensitive meta-data to check if web application strips meta data is being stripped or not.

But before uploading let's check out what sensitive data our image contains. You can do this by simply visiting <http://exif.regex.info/exif.cgi> and uploading your image or pasting the URL link.

Not secure | exif.regex.info/exif.cgi

Apps Bug Bounty Recon Tools Writeups Projects Videos Future Studies From S3 bucket to... Doing Recon Like A... Concrete5 CMS XSS... Reading list

If you have questions about this tool, please see the FAQ.

Basic Image Information

Target file: DSCN0010.png

Camera:	Nikon COOLPIX P6000
Lens:	24 mm (Max aperture f2.7)
Exposure:	Auto exposure, Program AE, 1/75 sec, f/5.9, ISO 64
Flash:	Off, Did not fire
Focus:	AF-S, Center AF Area Mode: Single Area
Date:	October 22, 2008 4:28:39PM (timezone not specified) (12 years, 7 months, 5 days, 18 hours, 47 minutes, 16 seconds ago, assuming image timezone of 1 hour ahead of GMT)
Location:	Latitude/longitude: 43° 28' 2.8" North, 11° 53' 6.5" East (43.467448, 11.885127)
	Map via embedded coordinates at: Google , Yahoo , WikiMapia , OpenStreetMap , Bing (also see the Google Maps pane below)
	Timezone guess from earthtools.org: 1 hour ahead of GMT
File:	640 x 480 JPEG 161,713 bytes (158 kilobytes)
Color Encoding:	WARNING: Color space tagged as sRGB, without an embedded color profile. Windows and Mac browsers and apps treat the colors randomly. Images for the web are most widely viewable when in the sRGB color space and with an embedded color profile. See my Introduction to Digital-Image Color Spaces for more information.

Extracted **160 x 120** 6.5-kilobyte "EXIF:ThumbnailImage" JPG
Displayed here at 200% (25% the area of the original)

Click image to isolate, click this text to show histogram

Main JPG image displayed here at 70% width (49% the area of the original)

Woah! This image contains our Camera Name, Lens used, Location and a lot more sensitive details!

Quickly! Let's upload the image on the vulnerable website and check if it strips these data or not!

brokenocrystals.com

Home Marketplace Gemstones Healing Jewellery Contact Vulnerabilities

Your Vulnerable Crystal Marketplace
Find the most beautiful stones in one place!

Get Started

Open image in new tab
Save image as...
Copy image
Copy image address
Create QR code for this image
Search Google for image
AdBlock — best ad blocker
Block element...
Download with IDM
Pushbullet
Inspect Ctrl+Shift+I

32°C Light rain ENG 28-05-2021

Once uploaded, Right Click on the image and click on `Copy image address`. Alternatively you can `Save Image` and then upload it on <http://exif.regex.info/exif.cgi>

The screenshot shows a web browser window with the URL <http://exif.regex.info/exif.cgi>. The page displays basic image information for a file named `download.png.txt`. The camera settings listed are: Camera: Nikon COOLPIX P6000; Lens: 8.1 mm (Max aperture f2.7); Exposure: Auto exposure, Program AE, 1/123 sec, f3.7, ISO 64; Flash: Off, Did not fire; Focus: AF-S, Center, AF Area Mode: Single Area; Date: October 22, 2008 4:45:21PM (timezone not specified) (12 years, 7 months, 5 days, 18 hours, 37 minutes, 49 seconds ago, assuming image timezone of 1 hour ahead of GMT); Location: Latitude/longitude: 43° 28' 6.1" North, 11° 52' 53.9" East (43.468365, 11.881635). Below this, there's a note about embedded coordinates and a timezone guess from earthtools.org. The file is a 640x480 JPEG, 150,301 bytes (147 kilobytes). The color encoding is noted as sRGB without an embedded color profile, with a warning that Windows and Mac browsers treat colors randomly. To the right, there are two thumbnail images: one labeled "Extracted 160 x 120 5.5-kilobyte 'EXIFThumbnailImage' JPG Displayed here at 200% (25% the area of the original)" and another labeled "Main JPG image displayed here at 70% width (49% the area of the original)". Both thumbnails show a narrow street scene with buildings.

Notice all sensitive data was not stripped from the image. This makes the web application vulnerable to EXIF Data Exposure.

Exploiting EXIF Data Exposure

Exploiting EXIF Data Exposure is very simple. You just need to find an entry point where you can upload an image. Such entry points can usually be in `User Profile Image` or `Comments` field which allows you to add files.

The steps to exploit this vulnerability are:

- Find an entry point for uploading an image
- Upload image containing sensitive EXIF meta data. You can find such images on <https://github.com/ianare/exif-samples>
- Once uploaded, either `copy Image Address` or `Save the Image`
- Go to <http://exif.regex.info/exif.cgi> and paste the link or upload the image.

- Click on **View Image Data** and it will give you the EXIF metadata of that image (if the data is not stripped by the server).

Severity

The severity of EXIF Data Exposure depends on two cases

1. Automatic User Enumeration P3 severity
2. Manual User Enumeration P4 severity

Automatic User Enumeration means the image you have uploaded is visible to public.

Manual User Enumeration means the image you have uploaded is not visible to other users.

Impact of EXIF Data Exposure

This vulnerability violates the privacy of a User and shares sensitive information of the user who uploads an image on the vulnerable website.

Prevention of EXIF Data Exposure

To prevent EXIF Data Exposure you can do the following:

- Disable geotagging on the digital device you use to take photographs
- Use an image processing software or EXIF data remover tool to delete metadata

References

- EXIF Data : <https://photographylife.com/what-is-exif-data>
- EXIF Data Information Leakage: <https://beaglesecurity.com/blog/vulnerability/exif-data-information-leakage.html>