- DISCLOSED VULNERABILITY REPORT -

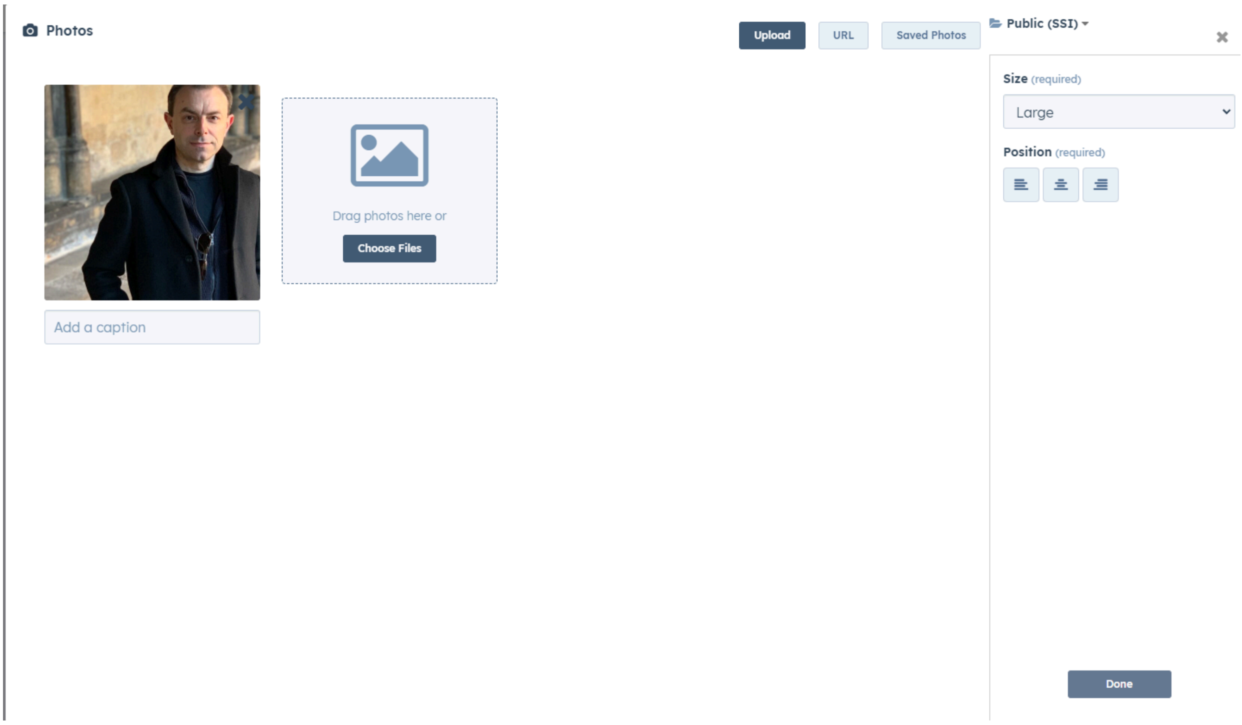
By Prv | mail | github | bugcrowd |

Name: Lack of EXIF Data Stripping Leads to User Enumeration & Data Exposure
Vulnerability type: EXIF Data Exposure on Public User Account
Severity: Low-Medium

Vulnerability Description:

Exchangeable Image File Format (EXIF) data is a standard used to specify the format of metadata in photographs. Most EXIF data contains the make, model and type of camera used, the lens settings, as well as the geolocation data. This application does not remove the EXIF data when a user uploads photographs, which could be used by an attacker to find and collect the geolocation data of users.

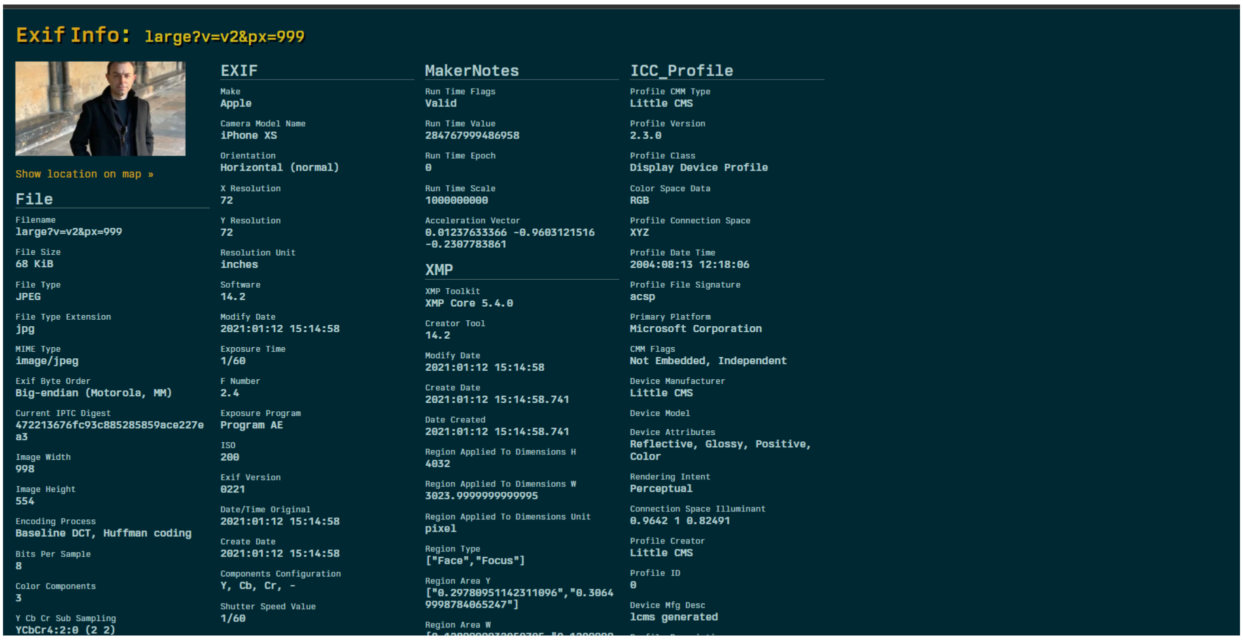
In this case, the client application allowed users to upload their own profile images:



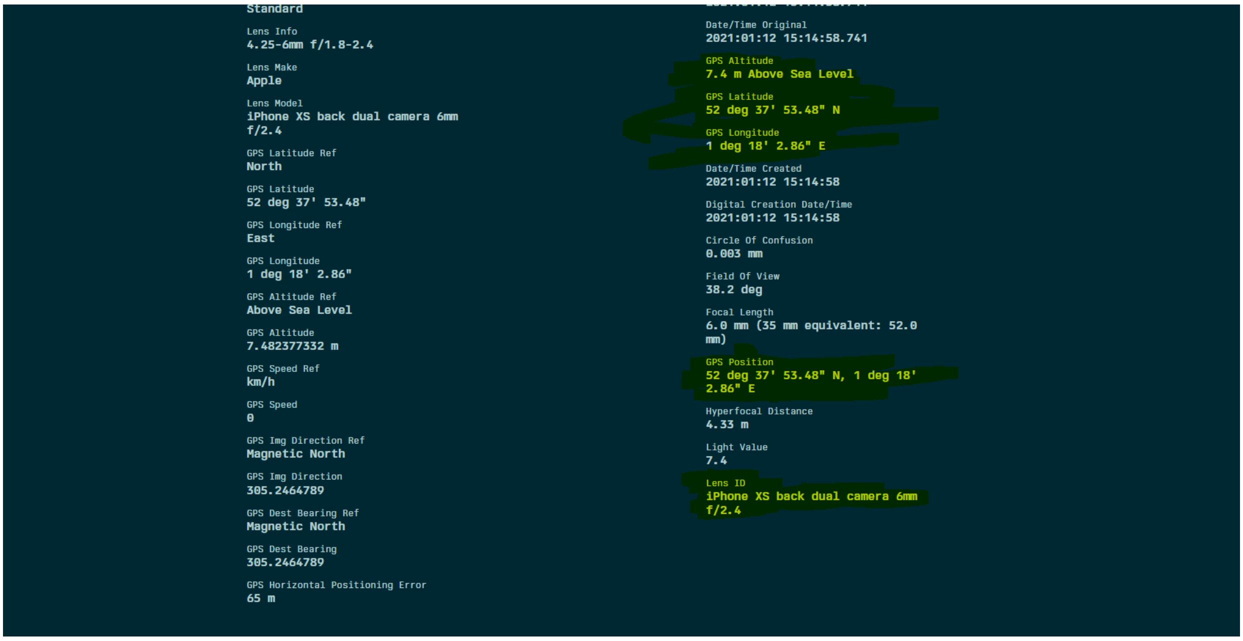
Size (required): Large
Position (required)

But filed to enforce the removal of the users EXIF data, meaning any attacker would be able to pull sensitive information of the user of the application such as:

- Exact User Agent, Phone Information & Strings
- GPS & Geo Location
- Internal Image Filenames and Directory Locations
- Modifying Date and Format/Upload Time



```
Exif Info: large?v=v2&px=999

Show location on map »

File
Filename
large?v=v2&px=999
File Size
68 KiB
File Type
JPEG
File Type Extension
jpg
MIME Type
image/jpeg
Exif Byte Order
Big-endian (Motorola, MM)
Current IPTC Digest
472213676fc93c885285859ace227e
a3
Image Width
998
Image Height
554
Encoding Process
Baseline DCT, Huffman coding
Bits Per Sample
8
Color Components
3
Y Cb Cr Sub Sampling
YCbCr4:2:0 (2 2)

EXIF
Make
Apple
Camera Model Name
iPhone XS
Orientation
Horizontal (normal)
X Resolution
72
Y Resolution
72
Resolution Unit
inches
Software
14.2
Modify Date
2021:01:12 15:14:58
Exposure Time
1/60
F Number
2.4
Exposure Program
Program AE
ISO
200
Exif Version
0221
Date/Time Original
2021:01:12 15:14:58
Create Date
2021:01:12 15:14:58
Components Configuration
Y, Cb, Cr, -
Shutter Speed Value
1/60

MakerNotes
Run Time Flags
Valid
Run Time Value
284767999486958
Run Time Epoch
0
Run Time Scale
1000000000
Acceleration Vector
0.01237633366 -0.9603121516
-0.2307783861

XMP
XMP Toolkit
XMP Core 5.4.0
Creator Tool
14.2
Modify Date
2021:01:12 15:14:58
Create Date
2021:01:12 15:14:58.741
Date Created
2021:01:12 15:14:58.741
Region Applied To Dimensions H
4032
Region Applied To Dimensions W
3023.9999999999995
Region Applied To Dimensions Unit
pixel
Region Type
["Face","Focus"]
Region Area Y
["0.29780951142311096","0.3064
9998784065247"]
Region Area W

ICC_Profile
Profile CMM Type
Little CMS
Profile Version
2.3.0
Profile Class
Display Device Profile
Color Space Data
RGB
Profile Connection Space
XYZ
Profile Date Time
2004:08:13 12:18:06
Profile File Signature
acsp
Primary Platform
Microsoft Corporation
CMM Flags
Not Embedded, Independent
Device Manufacturer
Little CMS
Device Model
Device Attributes
Reflective, Glossy, Positive,
Color
Rendering Intent
Perceptual
Connection Space Illuminant
0.9642 1 0.82491
Profile Creator
Little CMS
Profile ID
0
Device Mfg Desc
lcms generated
```



```
Standard
Lens Info
4.25-6mm f/1.8-2.4
Lens Make
Apple
Lens Model
iPhone XS back dual camera 6mm
f/2.4
GPS Latitude Ref
North
GPS Latitude
52 deg 37' 53.48"
GPS Longitude Ref
East
GPS Longitude
1 deg 18' 2.86"
GPS Altitude Ref
Above Sea Level
GPS Altitude
7.482377332 m
GPS Speed Ref
km/h
GPS Speed
0
GPS Img Direction Ref
Magnetic North
GPS Img Direction
305.2464789
GPS Dest Bearing Ref
Magnetic North
GPS Dest Bearing
305.2464789
GPS Horizontal Positioning Error
65 m

Date/Time Original
2021:01:12 15:14:58.741
GPS Altitude
7.4 m Above Sea Level
GPS Latitude
52 deg 37' 53.48" N
GPS Longitude
1 deg 18' 2.86" E
Date/Time Created
2021:01:12 15:14:58
Digital Creation Date/Time
2021:01:12 15:14:58
Circle Of Confusion
0.003 mm
Field Of View
38.2 deg
Focal Length
6.0 mm (35 mm equivalent: 52.0
mm)
GPS Position
52 deg 37' 53.48" N, 1 deg 18'
2.86" E
Hyperfocal Distance
4.33 m
Light Value
7.4
Lens ID
iPhone XS back dual camera 6mm
f/2.4
```

Resolution:

This issue was addressed with the security team of the site and a working fix was planned to be implemented, reputational rewards were given as a result of the finding and further advisories were given as to how EXIF data can be used to identify and expose users personal information.

This document is a disclosed vulnerability report by a practised security researcher, all vulnerabilities and issues mentioned in this report have been released under the permission of the owner and/or have been mitigated against and fixed before this report was written, if by any chance the contents of this report can be replicated this is due to another vulnerability or mere coincidence, please report any issues or regards: prv@anche.no