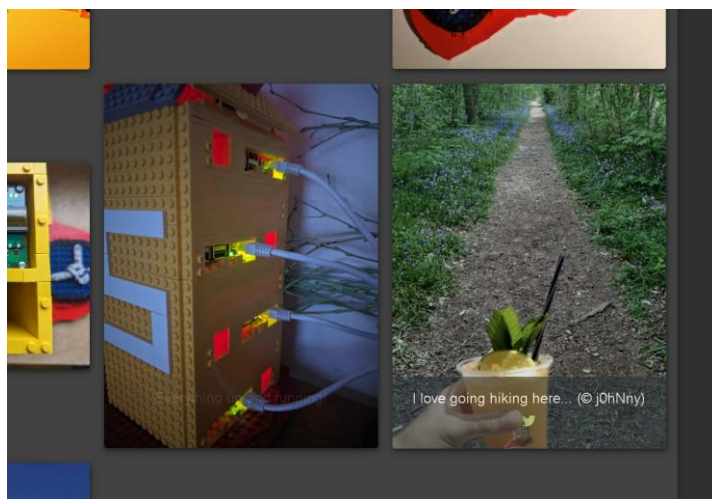


Sensitive Data Exposure in OWASP Juice Shop

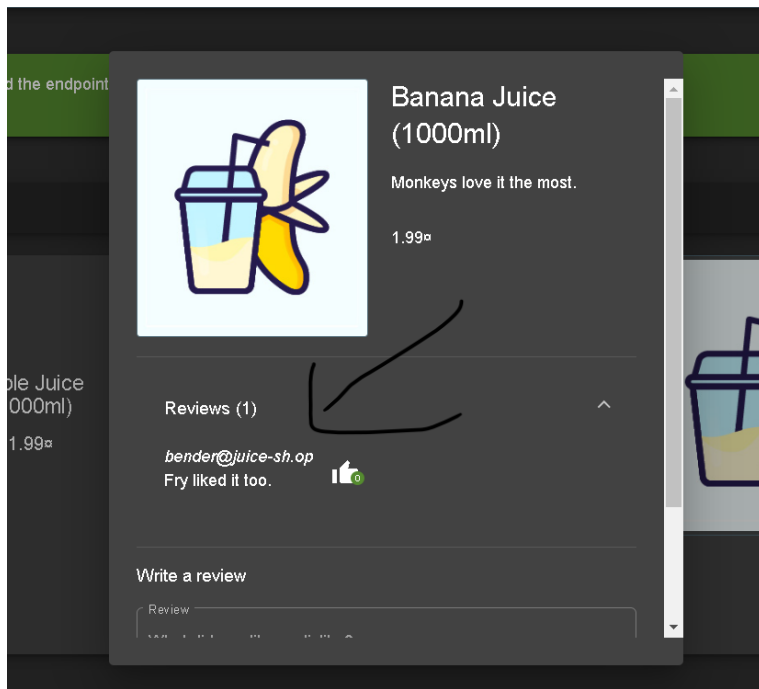


This falls under the OSINT category.

As described in the task's description, first we will go to the photo wall section to see the uploads of him we need to figure out his email and security question answer to successfully reset his password



here we can see the upload by john



From product reviews, we can see the email domain
so john's email can be john@juice-sh.op

Now Download the image upload by John
by seeing the file name of it, we can assume his security question can be
favorite hiking place



use kali linux to use exiftool on this file to see the file's meta data

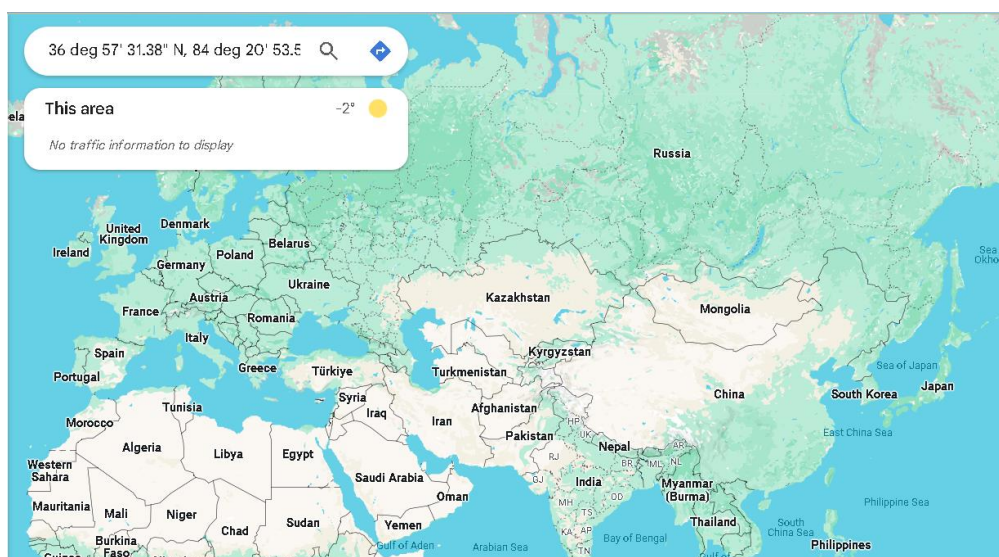
```
(kali@kali)-[~/Desktop]
$ exiftool favorite-hiking-place.png.crdownload
ExifTool Version Number      : 12.76
File Name                    : favorite-hiking-place.png.crdownload
Directory                   : .
File Size                    : 667 kB
File Modification Date/Time  : 2025:02:05 09:57:49-05:00
File Access Date/Time       : 2025:02:05 10:07:08-05:00
File Inode Change Date/Time  : 2025:02:05 10:07:08-05:00
File Permissions             : -rw-----
File Type                    : PNG
File Type Extension         : png
MIME Type                    : image/png
Image Width                  : 471
Image Height                 : 627
Bit Depth                    : 8
Color Type                   : RGB
Compression                  : Deflate/Inflate
Filter                       : Adaptive
Interlace                   : Noninterlaced
Exif Byte Order              : Little-endian (Intel, II)
Resolution Unit              : inches
Y Cb Cr Positioning          : Centered
GPS Version ID               : 2.2.0.0
GPS Latitude Ref             : North
GPS Longitude Ref            : West
GPS Map Datum                : WGS-84
Thumbnail Offset             : 224
Thumbnail Length             : 4531
SRGB Rendering               : Perceptual
Gamma                        : 2.2
Pixels Per Unit X            : 3779
Pixels Per Unit Y            : 3779
Pixel Units                  : meters
Image Size                   : 471x627
Megapixels                   : 0.295
Thumbnail Image              : (Binary data 4531 bytes, use -b option to extract)
GPS Latitude                 : 36 deg 57' 31.38" N
GPS Longitude                 : 84 deg 20' 53.58" W
GPS Position                  : 36 deg 57' 31.38" N, 84 deg 20' 53.58" W

(kali@kali)-[~/Desktop]
```

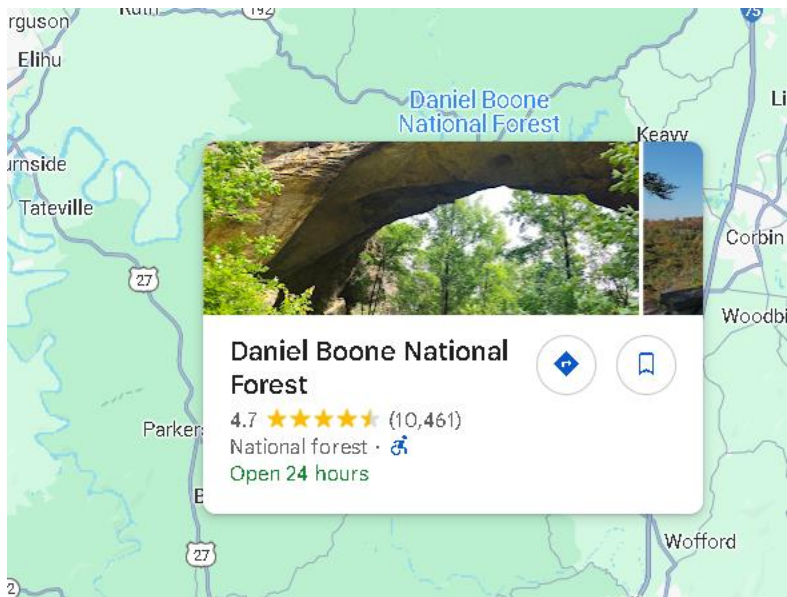
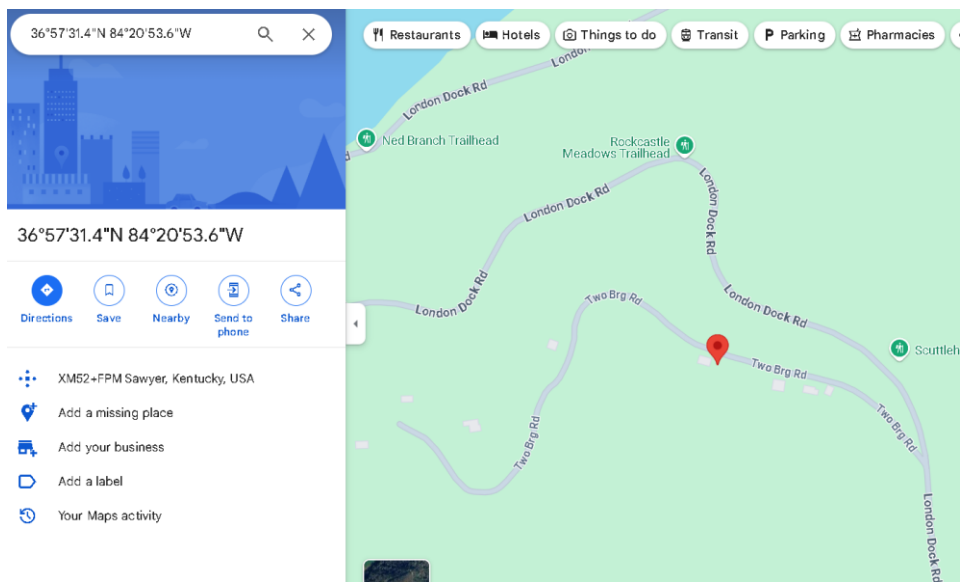
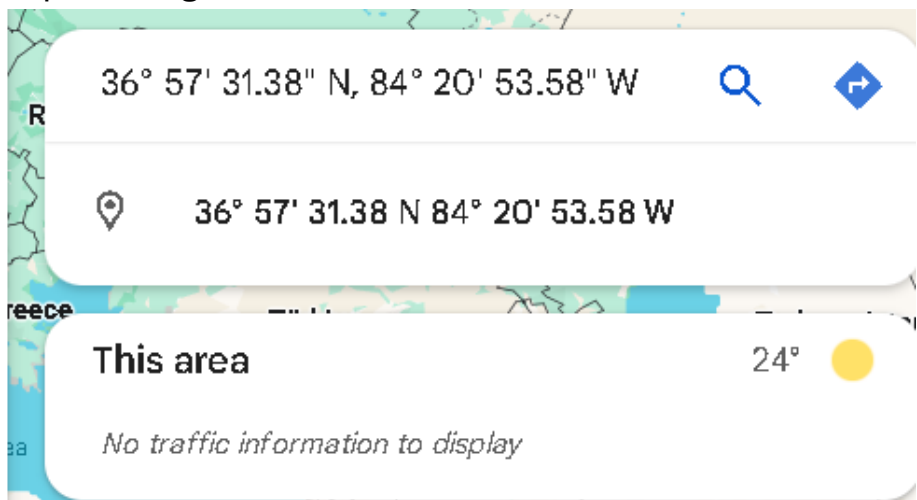
Here we can see the exposed GPS position of the location

36 deg 57' 31.38" N, 84 deg 20' 53.58" W

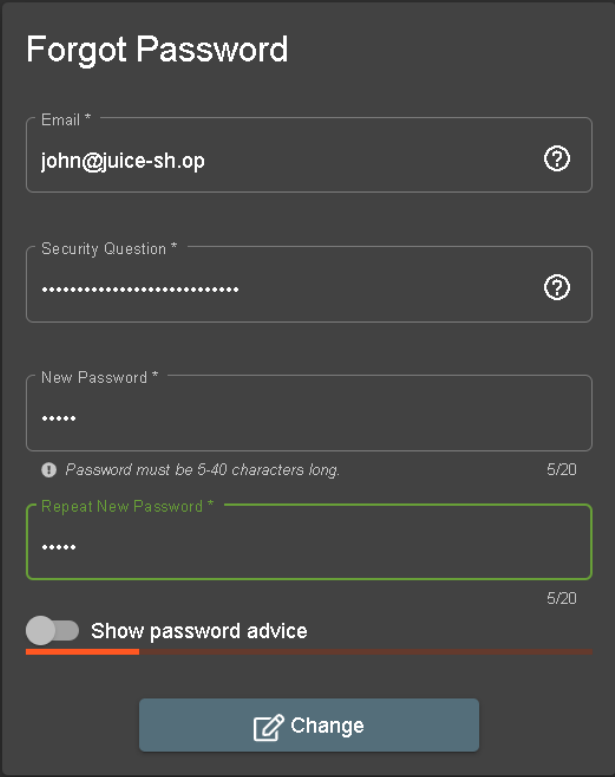
using google maps to see the location



Replace deg with °



Now trying to change his password



The image shows a 'Forgot Password' form with the following fields and elements:

- Email ***: A text input field containing 'john@juice-sh.op' with a question mark icon on the right.
- Security Question ***: A text input field with masked dots and a question mark icon on the right.
- New Password ***: A text input field with masked dots. Below it is a hint: 'Password must be 5-40 characters long.' and a character count '5/20'.
- Repeat New Password ***: A text input field with masked dots and a character count '5/20'.
- Show password advice**: A toggle switch that is currently turned off.
- Change**: A button with a pencil icon and the text 'Change'.

Security question's answer as Daniel Boone National Forest

And setting pass as 54321

Done

