OLD Times

462 Points **SOLVED**

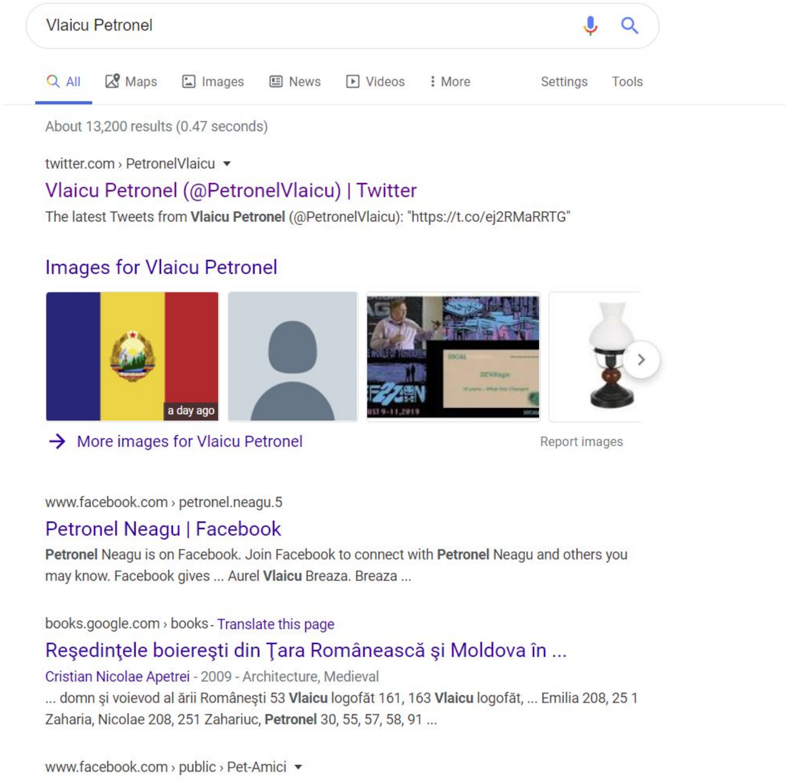
There are rumors that a group of people would like to overthrow the communist party. Therefore, an investigation was initiated under the leadership of Vlaicu Petronel. Be part of this ultra secret investigation, help the militia discover all secret locations and you will be rewarded.

Author: Legacy + FeDEX
Flag Format: HackTM{SECRET}

Author: Chaocipher
Date: 2/2/2020

Start

OK, so I start with a Google search for Vlaicu Petronel.



About 13,200 results (0.47 seconds)

twitter.com › PetronelVlaicu

Vlaicu Petronel (@PetronelVlaicu) | Twitter

The latest Tweets from **Vlaicu Petronel** (@PetronelVlaicu): "https://t.co/ej2RMaRRTG"

Images for Vlaicu Petronel

More images for Vlaicu Petronel

Report images

www.facebook.com › petronel.neagu.5

Petronel Neagu | Facebook

Petronel Neagu is on Facebook. Join Facebook to connect with **Petronel** Neagu and others you may know. Facebook gives ... Aurel **Vlaicu** Breaza. Breaza ...

books.google.com › books - Translate this page

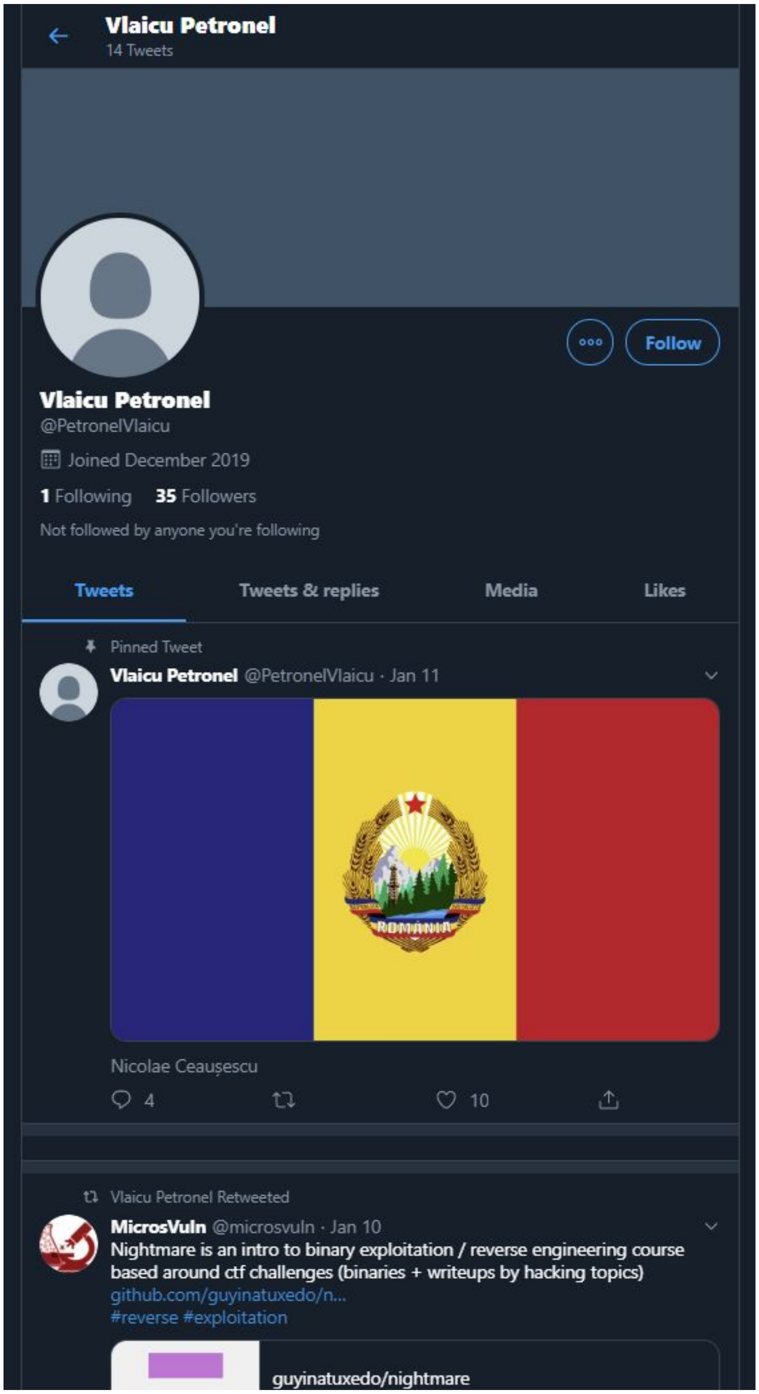
Reşedinţele boiereşti din Ţara Românească şi Moldova în ...

Cristian Nicolae Apetrei - 2009 - Architecture, Medieval

... domn şi voievod al ării Româneşti 53 **Vlaicu** logofăt 161, 163 **Vlaicu** logofăt, ... Emilia 208, 25 1 Zaharia, Nicolae 208, 251 Zahariuc, **Petronel** 30, 55, 57, 58, 91 ...

www.facebook.com › public › Pet-Amici

As you can see there isn’t much solid beyond the first hit for a Twitter account.



Vlaicu Petronel
14 Tweets

Vlaicu Petronel
@PetronelVlaicu
Joined December 2019
1 Following **35** Followers
Not followed by anyone you're following

Pinned Tweet
Vlaicu Petronel @PetronelVlaicu · Jan 11

Nicolae Ceaușescu
4 10

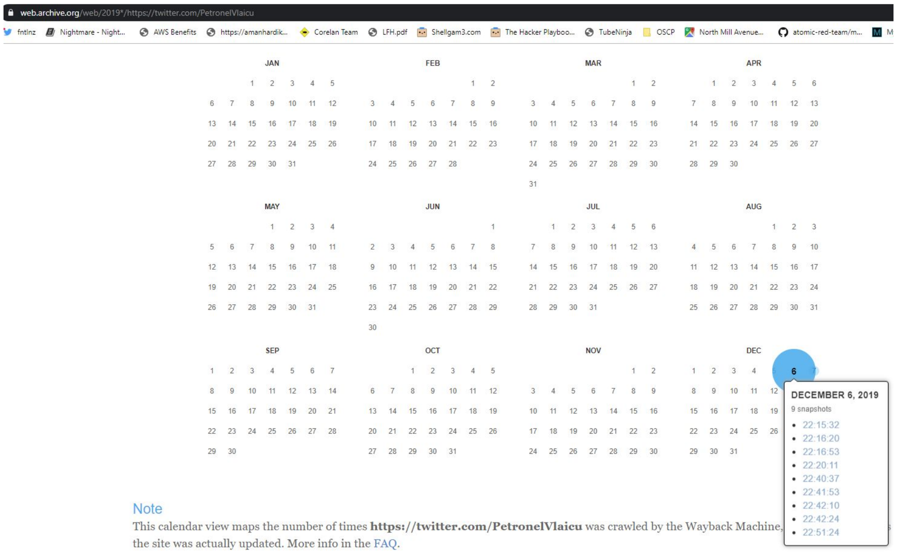
Vlaicu Petronel Retweeted
MicrosVuln @microsvuln · Jan 10
Nightmare is an intro to binary exploitation / reverse engineering course based around ctf challenges (binaries + writeups by hacking topics)
github.com/guyinatuxedo/n...
#reverse #exploitation

guyinatuxedo/nightmare

I spent a long time looking through all the social connections, followers, following, likes, chat threads. Wasted a ton of time doing that; many red herrings. The Nicolae Ceausescu person really cost me a lot of time, because he had been quoted many times with the words “old times” and people were talking about him as in, “bring back the old times”, etc. He also had some famous speeches that I poured over. I went through all the recent history of changes to all the wiki pages related to this guy and his militia.

Wayback Machine

I finally thought I might try the Wayback Machine. That's a normal OSINT thing to do, might as well give it a shot.



DECEMBER 6, 2019

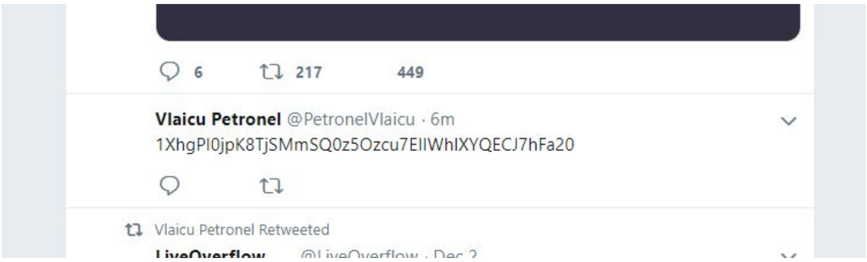
9 snapshots

- 22:15:32
- 22:16:20
- 22:16:53
- 22:20:11
- 22:40:37
- 22:41:53
- 22:42:10
- 22:42:24
- 22:51:24

Note

This calendar view maps the number of times **https://twitter.com/PetronelVlaicu** was crawled by the Wayback Machine, the site was actually updated. More info in the FAQ.

Holy crap! 9 snapshots on December 6th and 2 more on the 9th. So, that's pretty obvious where I need to be looking. That many snapshots in a short period is fishy. I'd practically memorized all his tweets and was sure that I'd know if something was new.



Vlaicu Petronel @PetronelVlaicu · 6m

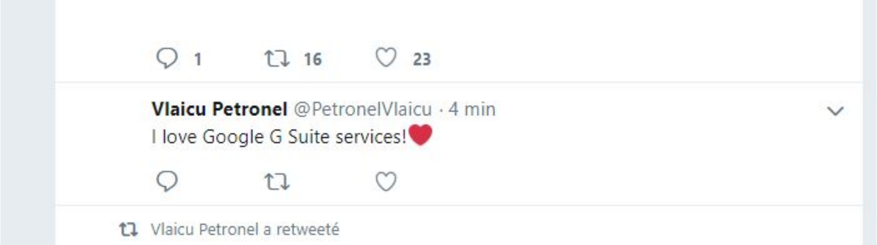
1XhgPI0jpK8TjSMmSQ0z5Ozcu7EIlWhlXYQECJ7hFa20

Vlaicu Petronel Retweeted

LiveOverflow @LiveOverflow · Dec 2

OK. This is something interesting. 1XhgPI0jpK8TjSMmSQ0z5Ozcu7EIIWhlXYQECJ7hFa20

So, what is this thing? I do an online hash checker and get no hits. It doesn't conform to any hash type. Base64 decode and no dice there. So, back to the Wayback machine I go.



1 16 23

Vlaicu Petronel @PetronelVlaicu · 4 min

I love Google G Suite services!❤️

Vlaicu Petronel a retweeté

Google drive

Got it. Should be a shared file sitting on Google drive.
https://docs.google.com/document/d/1XhgPI0jpK8TjSMmSQ0z5Ozcu7EIlWhlXYQECJ7hFa20/edit

Report - Week VII

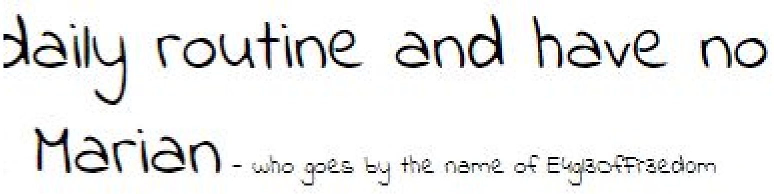
The local activity is under control. People seek their daily routine and have no doubts about the party, except for one man: Iovescu Marian - who goes by the name of DigitalFreedom

Profile:

Name: Iovescu Marian
Address: Romania, Timisoara, str. Mures, nr. 25
Activity: IT Programmer
Description: Lately, his activity has been suspicious. Therefore, I followed him closely for a week and found out that he was setting up an anti-communist uprising. He has been working for a while on a secret program that wants to mobilize the population to overthrow the communist system. The problem is that two days ago he realized that I was following him and deleted all the work that he published on a free and open platform.

Signed: Iovescu Marian

OK cool. Zoom in on this smaller section.

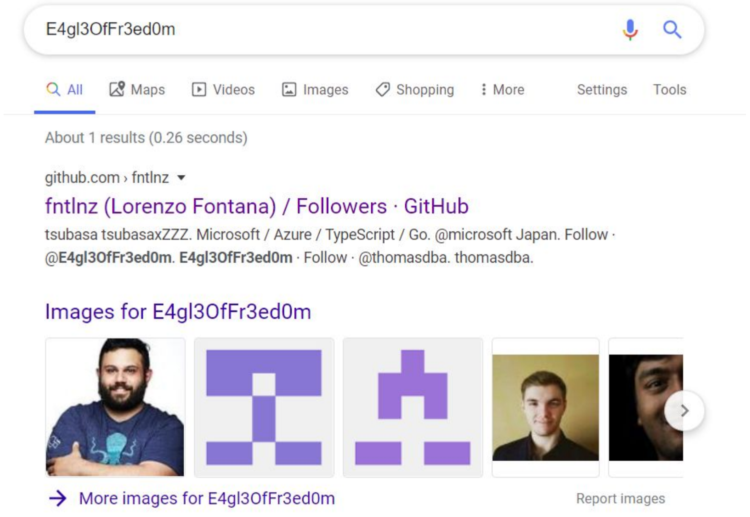


daily routine and have no

Marian - who goes by the name of E4gl3OfFr3edom

E4gl3OfFr3ed0m

OK, back to Google.



E4gl3OfFr3ed0m

About 1 results (0.26 seconds)

github.com › fntlnz

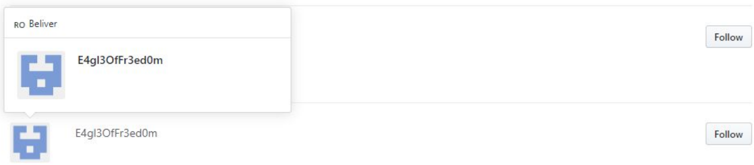
fntlnz (Lorenzo Fontana) / Followers · GitHub

tsubasa tsubasaxZZZ. Microsoft / Azure / TypeScript / Go. @microsoft Japan. Follow · @**E4gl3OfFr3ed0m**. **E4gl3OfFr3ed0m** · Follow · @thomasdba. thomasdba.

Images for E4gl3OfFr3ed0m

More images for E4gl3OfFr3ed0m

Pretty simple, one link. This is where I made a big mistake and got off track. I thought the picture in the dossier and the Github picture were the same guy. After looking much harder, later, I realized they weren't but it threw me off for a couple hours. I went through the Wayback Machine again looking through differences in his repos and I found one that had been deleted and so I poured over the info which led me to another person and went through all the commits for that repo, ugh! You get the point. If you look at the Google result carefully above; it's a follower of fntlnz not a connected handle.

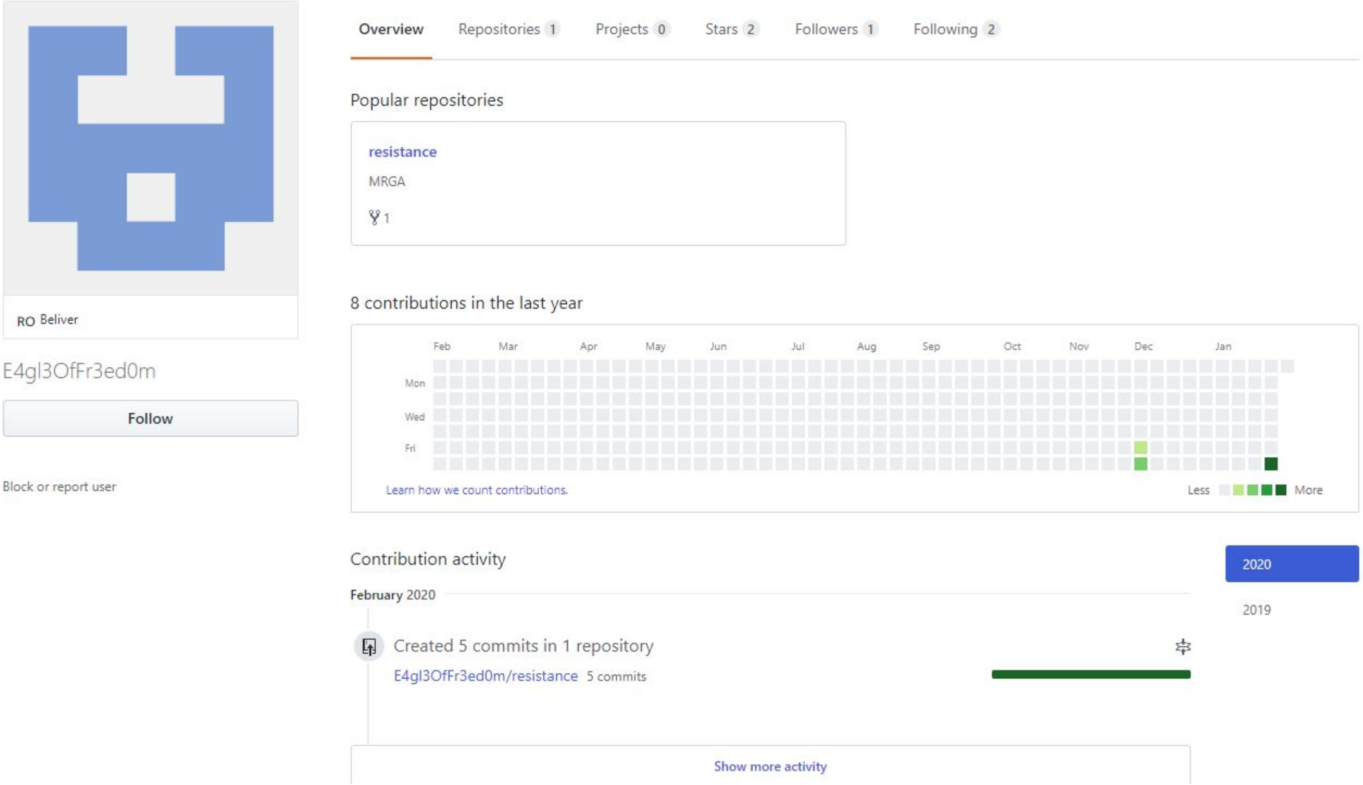


RO Beliver

E4gl3OfFr3ed0m

E4gl3OfFr3ed0m

Go to this page:



E4gl3OfFr3ed0m

Popular repositories

resistance
MRGA
1

8 contributions in the last year

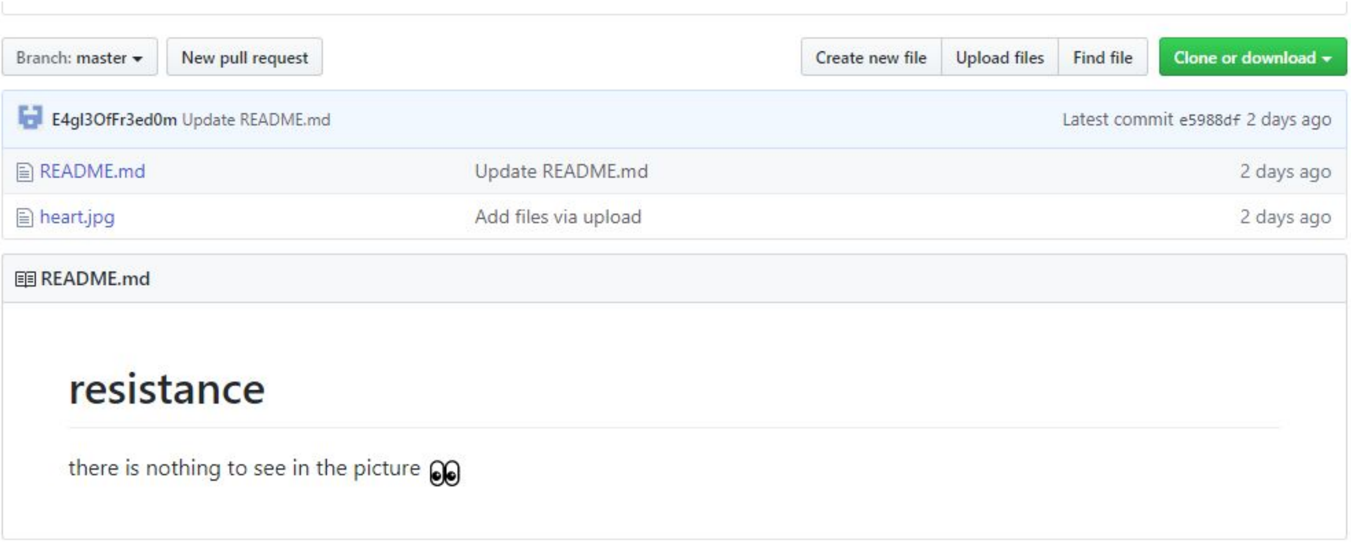
Contribution activity

February 2020

Created 5 commits in 1 repository

E4gl3OfFr3ed0m/resistance 5 commits

OK, now things are looking more like stuff within bounds for a CTF. The word resistance is a significant word. Let’s take a look.



E4gl3OfFr3ed0m Update README.md — Latest commit e5988df 2 days ago

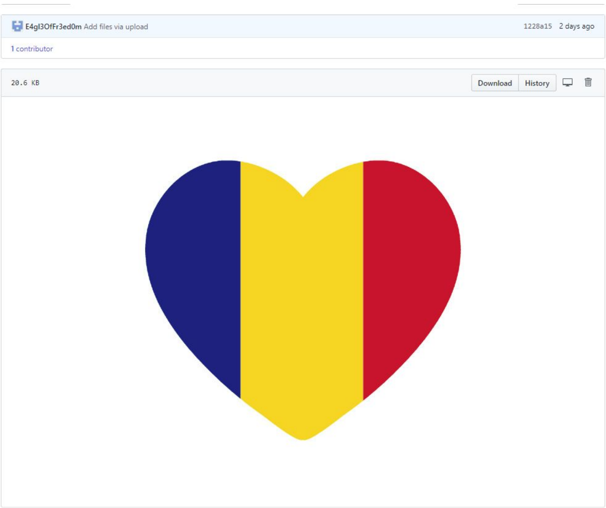
README.md	Update README.md	2 days ago
heart.jpg	Add files via upload	2 days ago

README.md

resistance

there is nothing to see in the picture 👀

Suspicious, OK. Let’s look at the pic file.

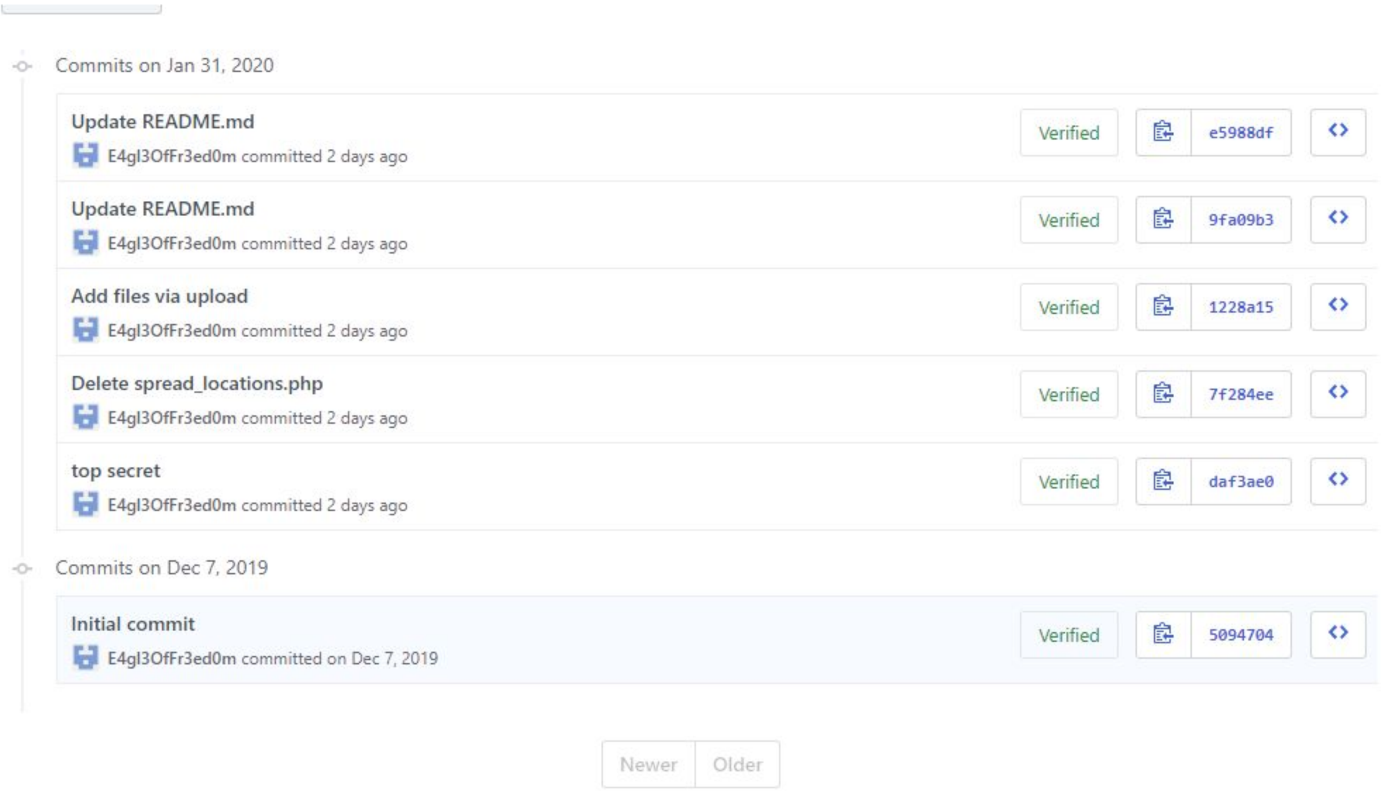


E4gl3OfFr3ed0m Add files via upload 1228a15 2 days ago

1 contributor

20.6 KB

It’s small and I ran some stego tools against it and didn’t see anything. So, I decided to look at the commits for the repo.



Commits on Jan 31, 2020

Update README.md
E4gl3OfFr3ed0m committed 2 days ago
Verified e5988df

Update README.md
E4gl3OfFr3ed0m committed 2 days ago
Verified 9fa09b3

Add files via upload
E4gl3OfFr3ed0m committed 2 days ago
Verified 1228a15

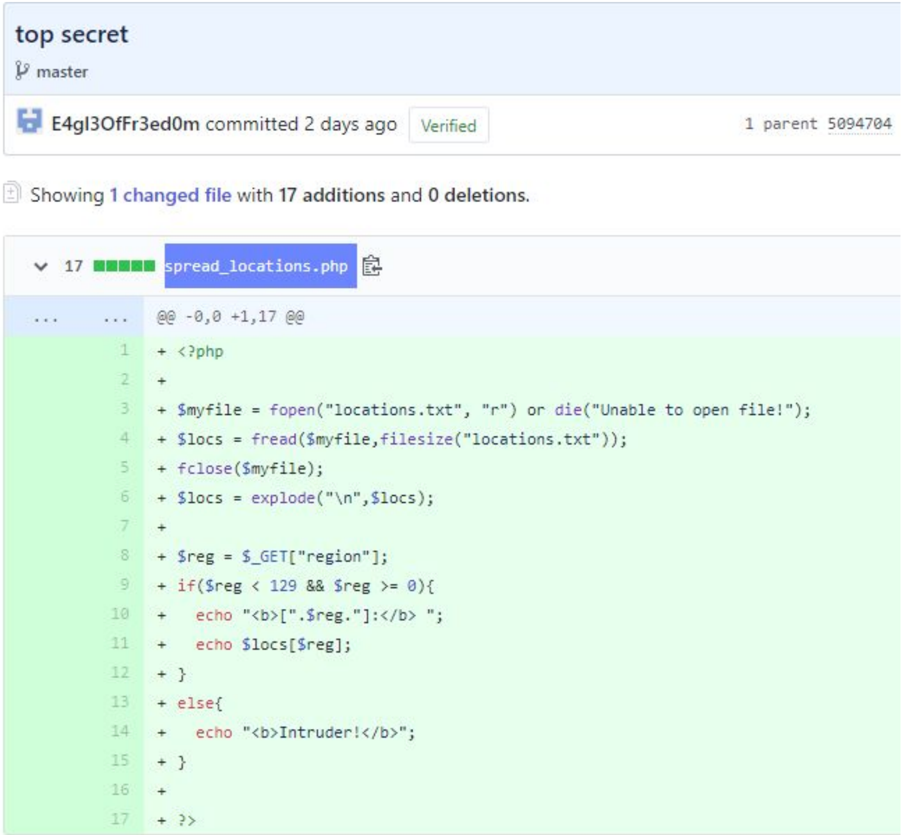
Delete spread_locations.php
E4gl3OfFr3ed0m committed 2 days ago
Verified 7f284ee

top secret
E4gl3OfFr3ed0m committed 2 days ago
Verified daf3ae0

Commits on Dec 7, 2019

Initial commit
E4gl3OfFr3ed0m committed on Dec 7, 2019
Verified 5094704

Interesting info here; “top secret”, “spread_locations”. Let’s dig into these a bit.



top secret

master

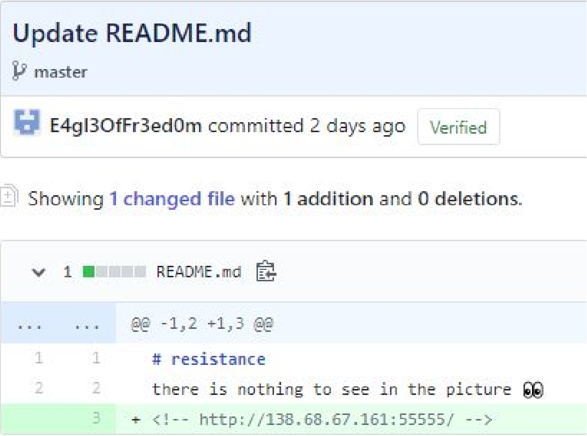
E4gl3OfFr3ed0m committed 2 days ago Verified 1 parent 5094704

Showing 1 changed file with 17 additions and 0 deletions.

17 spread_locations.php

```
... ...  @@ -0,0 +1,17 @@
  1  + <?php
  2  +
  3  + $myfile = fopen("locations.txt", "r") or die("Unable to open file!");
  4  + $locs = fread($myfile,filesize("locations.txt"));
  5  + fclose($myfile);
  6  + $locs = explode("\n",$locs);
  7  +
  8  + $reg = $_GET["region"];
  9  + if($reg < 129 && $reg >= 0){
 10  +   echo "<b>[".$reg."]:</b> ";
 11  +   echo $locs[$reg];
 12  + }
 13  + else{
 14  +   echo "<b>Intruder!</b>";
 15  + }
 16  +
 17  + ?>
```

So, if I can find the web server I can use spread_locations.php and inject a variable for the region(line 8) and as long as that number is under 129 and greater than or equal to 0 (line 9), that I should get info from the locations.txt file (line 11). But where is the webserver? Found it in the commit note for the last update to the README.md file.



Update README.md

master

E4gl3OfFr3ed0m committed 2 days ago Verified

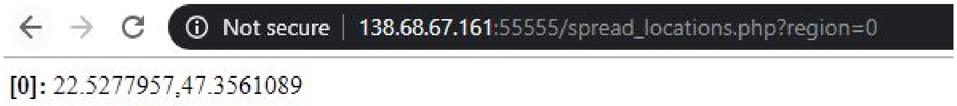
Showing 1 changed file with 1 addition and 0 deletions.

1 README.md

```
@@ -1,2 +1,3 @@
  # resistance
  there is nothing to see in the picture 👀
+ <!-- http://138.68.67.161:55555/ -->
```

spread_locations

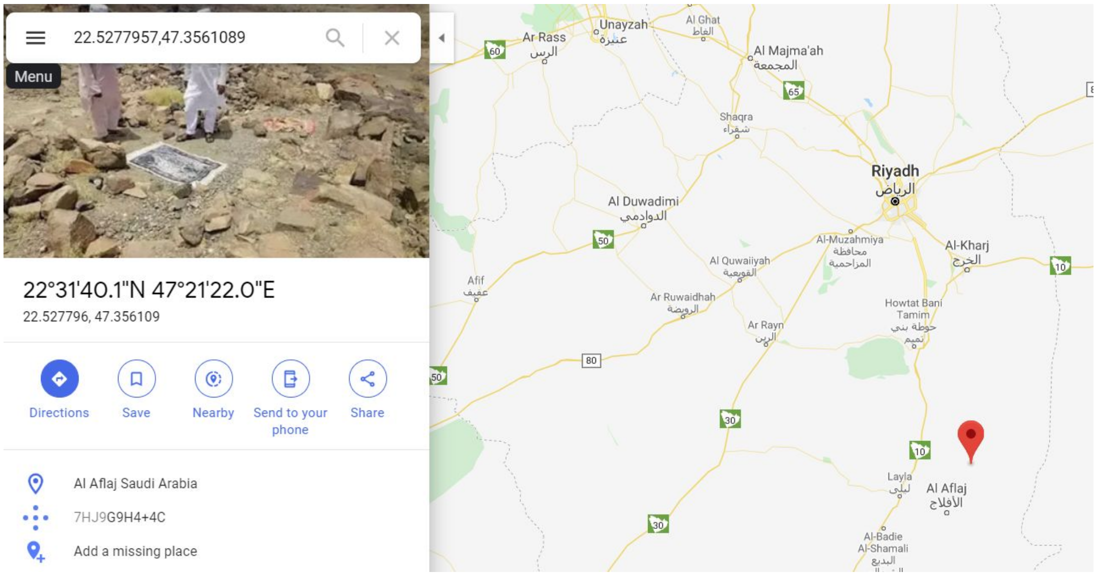
Let's give it a try:



138.68.67.161:55555/spread_locations.php?region=0

```
[0]: 22.5277957,47.3561089
```

Nice! Look like latitude and longitude coordinates. Let’s check that.

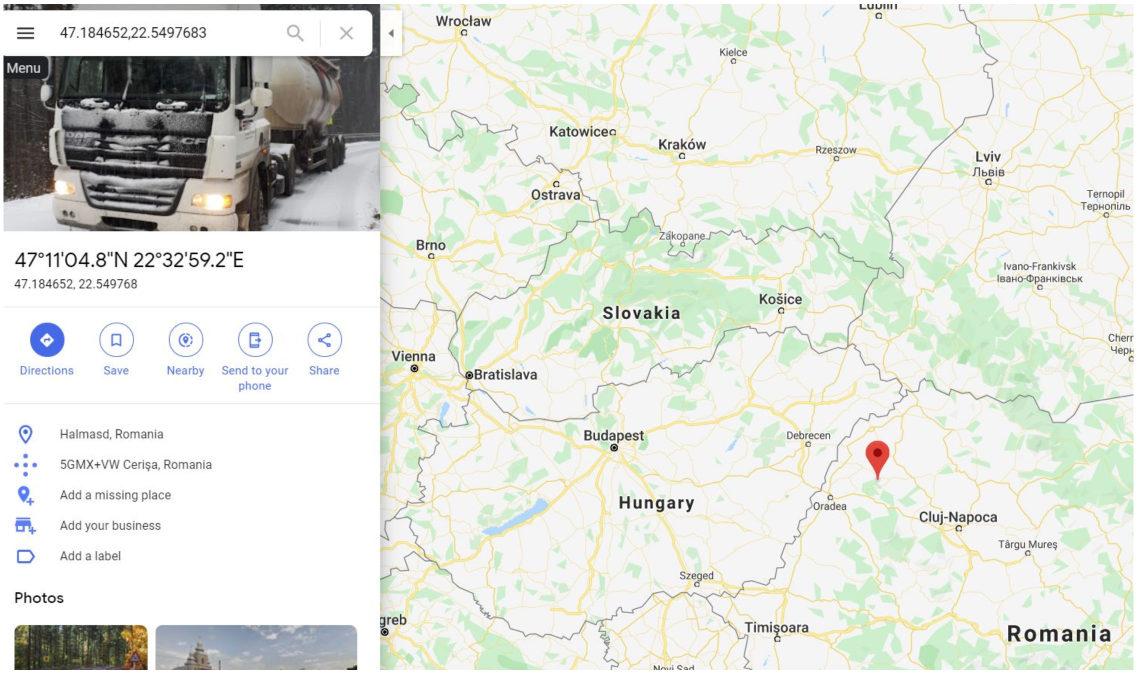


22.5277957,47.3561089

22°31'40.1"N 47°21'22.0"E
22.527796, 47.356109

Al Aflaj Saudi Arabia
7HJ9G9H4+4C
Add a missing place

Properly formed, but we get a spot in Saudi Arabia. Not really what I was expecting. Let’s try reversing the numbers.



47.184652,22.5497683

47°11'04.8"N 22°32'59.2"E
47.184652, 22.549768

Halmasd, Romania
5GMX+VW Cerişa, Romania
Add a missing place
Add your business
Add a label

Photos

Romania! That’s got to be it. So, let’s write some code to pull all the numbers out instead of doing this by hand.

Code

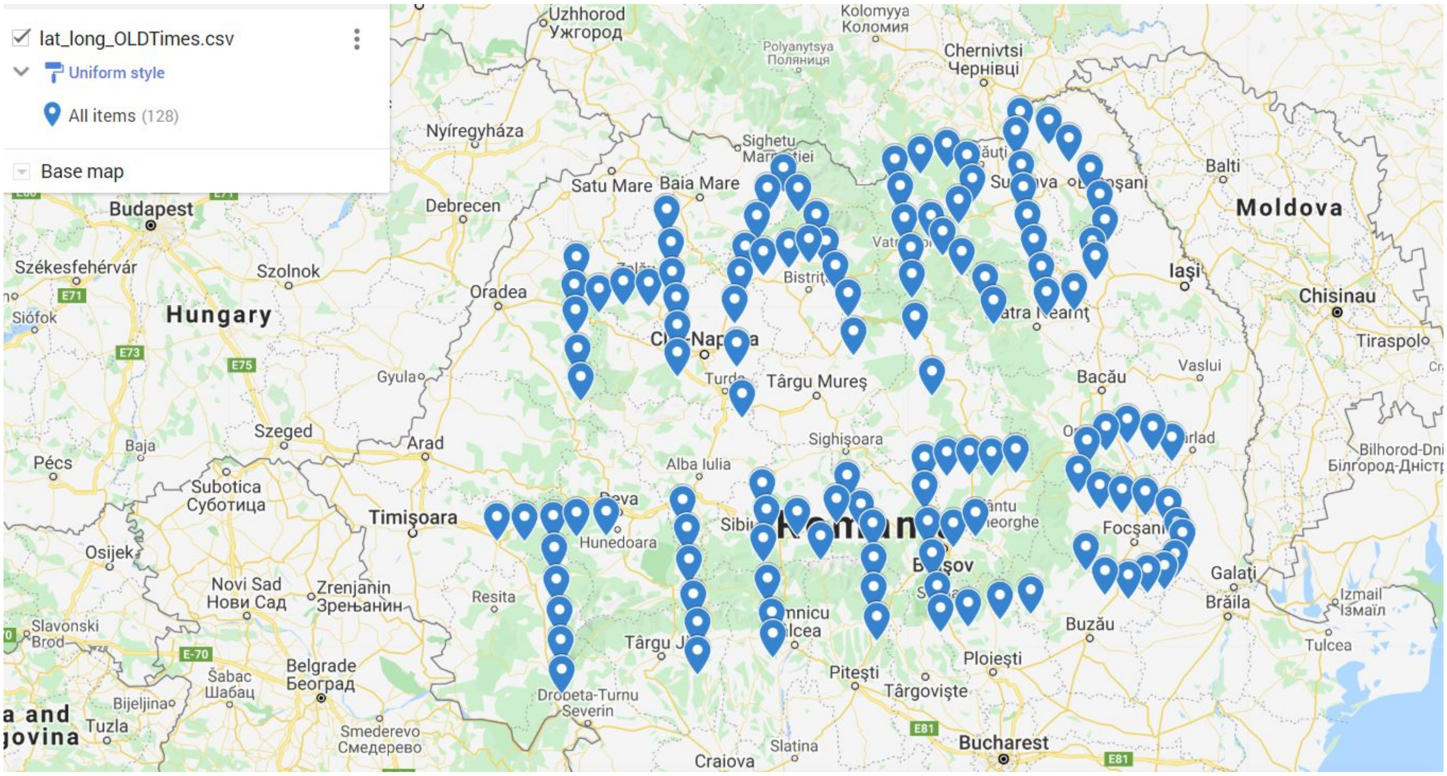
```
import requests

var_headers = {'content-type': 'application/x-www-form-urlencoded', 'user-agent': 'Python script'}
var_url_base_path = 'http://138.68.67.161:55555/spread_locations.php'
var_payload_base_string = '?region='


for var_seq_num in range(0, 129):

  var_payload_post = var_payload_base_string + str(var_seq_num)
  var_request1 = requests.get(var_url_base_path + var_payload_post)

  print("{}".format(var_request1.text))
```

OUTPUT (Sample - See Appendix for full output):

```
<b>[0]:</b> 22.5277957,47.3561089
<b>[1]:</b> 22.5497683,47.184652
<b>[2]:</b> 22.5277957,47.0276192
<b>[3]:</b> 22.538782,46.8851427
...
<b>[122]:</b> 27.4167117,45.4163615
<b>[123]:</b> 27.2738894,45.4009357
<b>[124]:</b> 27.1200808,45.3623528
<b>[125]:</b> 26.9223269,45.3855057
<b>[126]:</b> 26.7685183,45.5319208
<b>[127]:</b> 23.9230593,46.410005
<b>[128]:</b> 25.4941042,46.5386279
```

Google Maps

Save the trimmed output to a csv and upload to google maps.



Seems so easy after the fact.

Flag

HackTM{HARDTIMES}

Appendix:

```
Longitude,Latitude
22.5277957,47.3561089
22.5497683,47.184652
22.5277957,47.0276192
22.538782,46.8851427
22.5607546,46.6669469
22.5827273,46.508391
22.7365359,47.0051481
22.9342898,47.0500808
23.14303,47.0425947
23.2968386,47.4527737
23.3297976,47.2667225
23.3407839,47.1024545
23.3737429,46.9601776
23.3847292,46.8024828
23.3847292,46.6443244
23.879114,46.6970954
24.2636355,47.6825664
24.8459109,46.7648681
25.1864871,47.7343156
25.351282,46.8475858
24.1317996,47.5715023
24.0439089,47.4156159
23.945032,47.2443522
23.9010867,47.1024545
23.8571414,46.945179
24.3844851,47.5715023
24.5382937,47.4230496
24.615198,47.2741771
24.6921023,47.1398328
24.8019656,46.9826676
24.0988406,47.2145105
24.3075808,47.2592668
24.4723757,47.2890833
25.2304324,47.5863245
25.2633914,47.4081812
25.318323,47.2368934
25.3293093,47.0874959
25.4831179,47.4156159
25.3952273,47.7860133
25.6149539,47.8229089
25.7797488,47.756478
25.8236941,47.6233616
25.7138308,47.5047505
25.5819949,47.3263302
25.7358035,47.2145105
25.9335574,47.072533
25.9994753,46.9376782
26.2192019,47.9996428
26.1862429,47.8892548
26.2301882,47.7047509
26.2521609,47.5789139
26.2851199,47.4230496
26.3400515,47.2890833
26.4609011,47.9481577
26.625696,47.8524065
26.8014773,47.6825664
26.8783816,47.5344284
26.3949832,47.1323592
26.9223269,47.3933087
26.82345,47.2741771
26.4389285,46.9901622
26.6696414,47.0201299
26.8454226,47.1921182
21.8905886,45.7009791
22.1213015,45.7009791
22.3520144,45.7086515
22.5497683,45.723993
22.7914675,45.7316622
23.4286746,45.8006377
24.0878542,45.9001182
24.7909792,45.9383326
25.4281863,46.0451929
25.6149539,46.0756865
25.8017214,46.0833073
25.988489,46.0756865
26.1862429,46.090927
22.3630007,45.5242242
22.3849734,45.3391904
22.406946,45.161297
22.4179324,44.9828465
22.4289187,44.8116333
23.4616335,45.6395623
23.4836062,45.4549076
23.5165652,45.2541805
23.5495242,45.0915349
23.5495242,44.9206461
24.1208132,45.7469975
24.9008425,45.7776553
24.0988406,45.5780782
24.1317996,45.3469122
24.1647585,45.1458017
24.1757449,45.0216875
24.9997195,45.6626015
25.0107058,45.4703187
25.0107058,45.2928371
25.0326785,45.1225508
24.5712527,45.5934555
24.7030886,45.8082963
24.3734988,45.7316622
25.4281863,45.8848251
25.4611453,45.6779557
25.4941042,45.4934274
25.5380496,45.3005653
25.5600222,45.1690431
25.7907351,45.2000169
26.054407,45.246446
26.3070925,45.2773776
25.6698855,45.6626015
25.8566531,45.723993
27.4826296,46.1594571
27.3178347,46.2203012
27.1090945,46.2658901
26.9333132,46.2203012
26.7795046,46.1442356
26.7026003,45.9765207
26.8783816,45.8848251
27.0651492,45.8618775
27.2629031,45.8465739
27.4496707,45.7853172
27.526575,45.6702792
27.5705203,45.6088287
27.5046023,45.4857255
27.4167117,45.4163615
27.2738894,45.4009357
27.1200808,45.3623528
26.9223269,45.3855057
26.7685183,45.5319208
23.9230593,46.410005
25.4941042,46.5386279
```