BOUNTYCON

'19: SINGAPORE

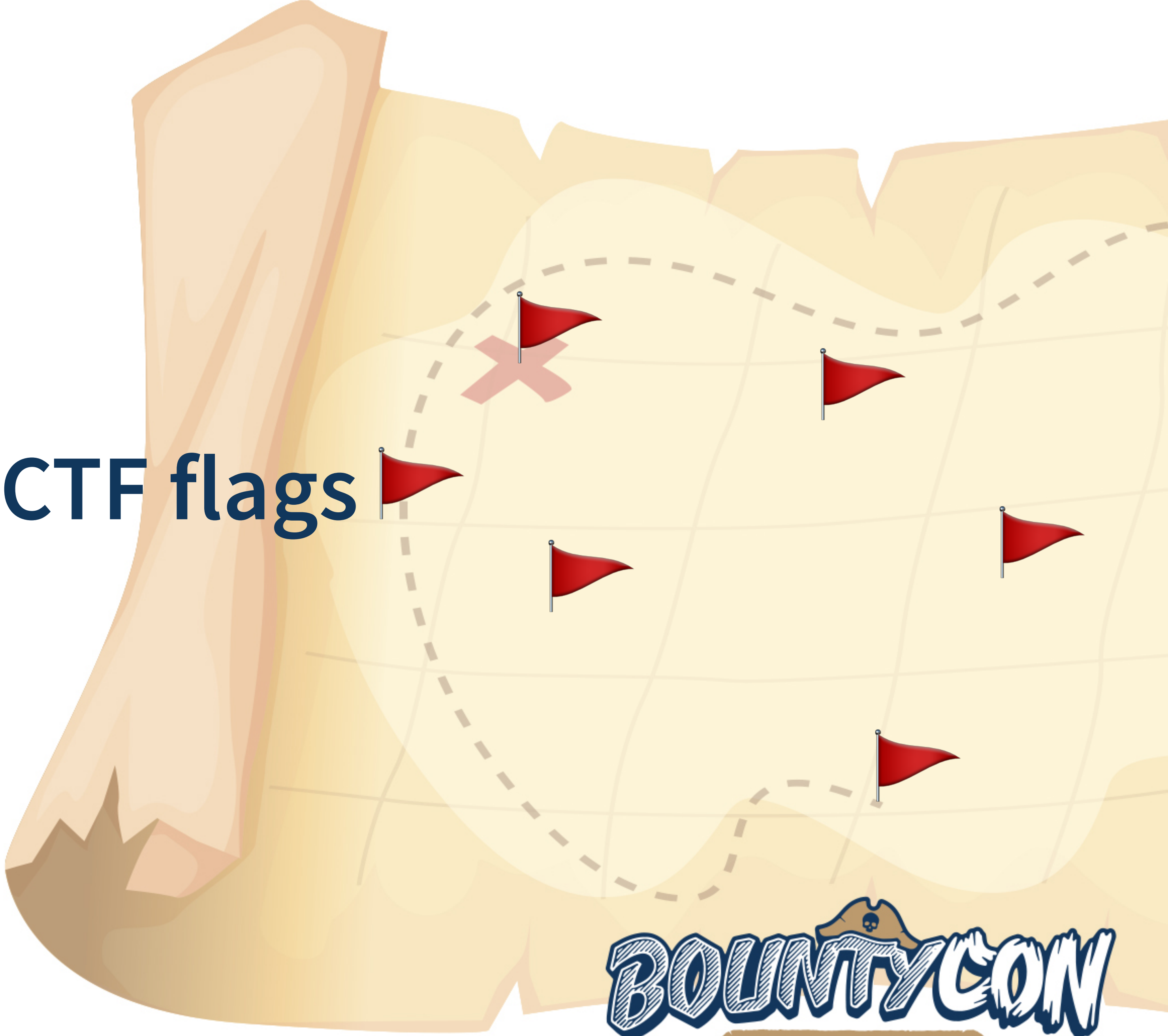
30th March 2019 • People Over Pixels

Hosted by

facebook Google

Finding BountyCon CTF flags

Kishan Bagaria



BOUNTYCON '19: SINGAPORE

$ whoami

# 👨🏻‍💻 indie software engineer by trade

# 🔐 security enthusiast

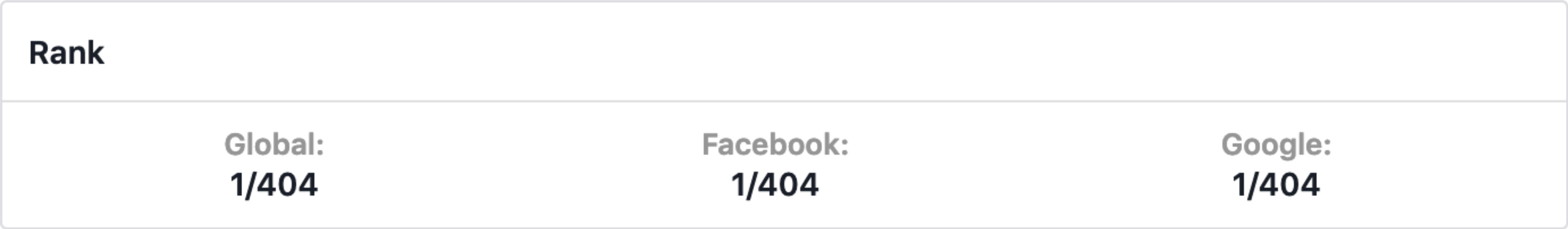
# 🥇 first hack: probably the time I bypassed the BIOS password 🔑

my father set when I was 6 👦🏻

$ whoami

# found 30 flags 🚩 (18 FB, 12 Google) in the BountyCon CTF between Jan 10th and 29th

# my rank:

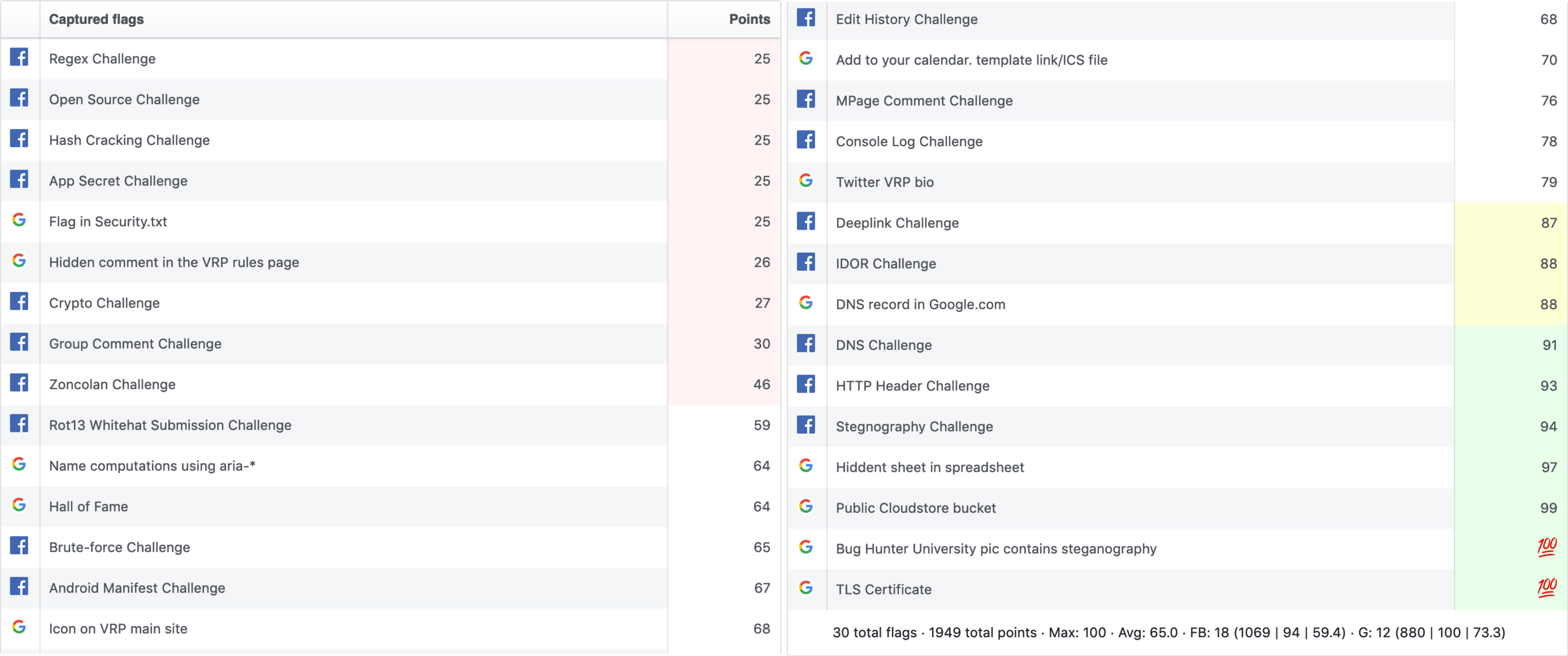


Rank

Global:	Facebook:	Google:
1/404	1/404	1/404

# that's not an error code. it's the total number of participants :)

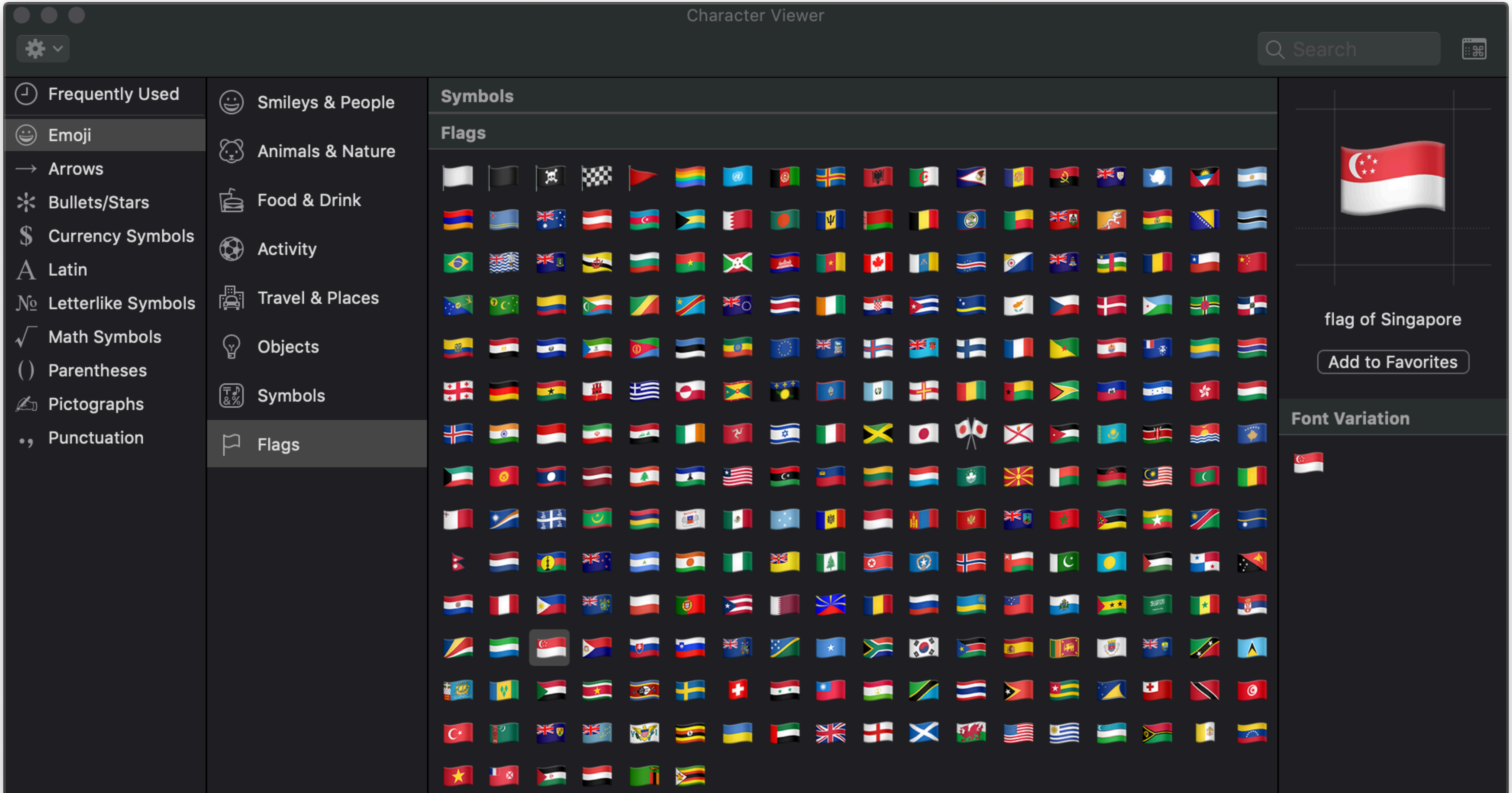
🚩🚩🚩🚩🚩🚩🚩🚩🚩🚩🚩🚩🚩🚩🚩🚩🚩🚩🚩🚩🚩🚩🚩🚩🚩🚩🚩🚩🚩🚩



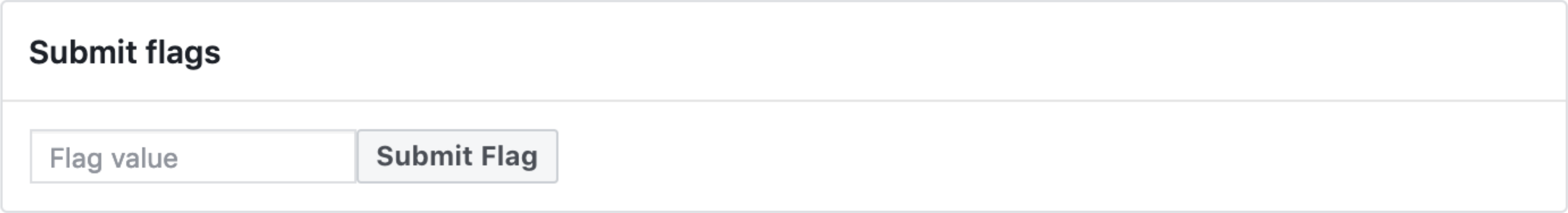
	Captured flags	Points
f	Regex Challenge	25
f	Open Source Challenge	25
f	Hash Cracking Challenge	25
f	App Secret Challenge	25
G	Flag in Security.txt	25
G	Hidden comment in the VRP rules page	26
f	Crypto Challenge	27
f	Group Comment Challenge	30
f	Zoncolan Challenge	46
f	Rot13 Whitehat Submission Challenge	59
G	Name computations using aria-*	64
G	Hall of Fame	64
f	Brute-force Challenge	65
f	Android Manifest Challenge	67
G	Icon on VRP main site	68
f	Edit History Challenge	68
G	Add to your calendar. template link/ICS file	70
f	MPage Comment Challenge	76
f	Console Log Challenge	78
G	Twitter VRP bio	79
f	Deeplink Challenge	87
f	IDOR Challenge	88
G	DNS record in Google.com	88
f	DNS Challenge	91
f	HTTP Header Challenge	93
f	Stegnography Challenge	94
G	Hiddent sheet in spreadsheet	97
G	Public Cloudstore bucket	99
G	Bug Hunter University pic contains steganography	💯
G	TLS Certificate	💯

30 total flags · 1949 total points · Max: 100 · Avg: 65.0 · FB: 18 (1069 | 94 | 59.4) · G: 12 (880 | 100 | 73.3)

also found these flags which weren't accepted 🤔



FB: [redacted] Challenge



Submit flags

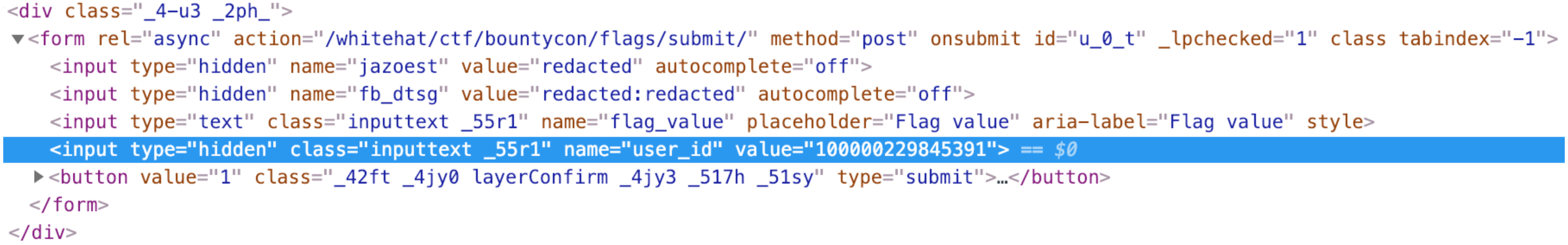
# flag present in submit flag endpoint

# initially didn't expect the form to have any vulnerabilities since it was crafted by security engineers

# after finding other flags in security/whitehat related pages, I realized this was a good place to hide a flag

FB: [redacted] Challenge

# let's inspect the form using developer tools



```
<div class="_4-u3 _2ph_">
▼<form rel="async" action="/whitehat/ctf/bountycon/flags/submit/" method="post" onsubmit id="u_0_t" _lpchecked="1" class tabindex="-1">
    <input type="hidden" name="jazoest" value="redacted" autocomplete="off">
    <input type="hidden" name="fb_dtsg" value="redacted:redacted" autocomplete="off">
    <input type="text" class="inputtext _55r1" name="flag_value" placeholder="Flag value" aria-label="Flag value" style>
    <input type="hidden" class="inputtext _55r1" name="user_id" value="100000229845391"> == $0
  ▶<button value="1" class="_42ft _4jy0 layerConfirm _4jy3 _517h _51sy" type="submit">…</button>
  </form>
</div>
```

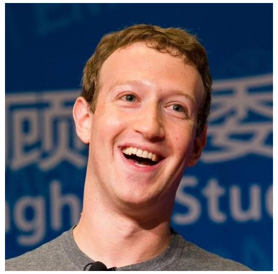
# unusual `user_id` param

# can you submit a flag for another user?

FB: IDOR Challenge

# set the `user_id` param to a valid user ID

# you can set it to 4 – the smallest valid user ID – belonging to this guy



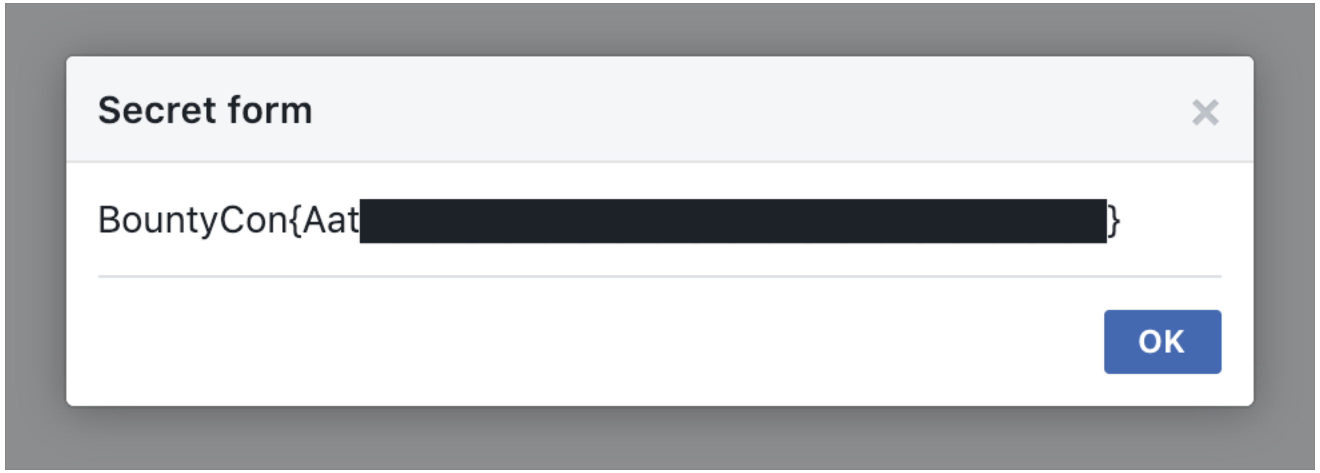
# pretty sure he wasn't playing in the CTF so even if there was a legit IDOR here, you wouldn't have increased his flags count meaningfully

# jk. don't test possible vulnerabilities with accounts that you don't control

FB: IDOR Challenge

# after changing the param, submit the form

# popup appears with the flag:



Secret form

BountyCon{Aat[redacted]}

FB: IDOR Challenge

88 points

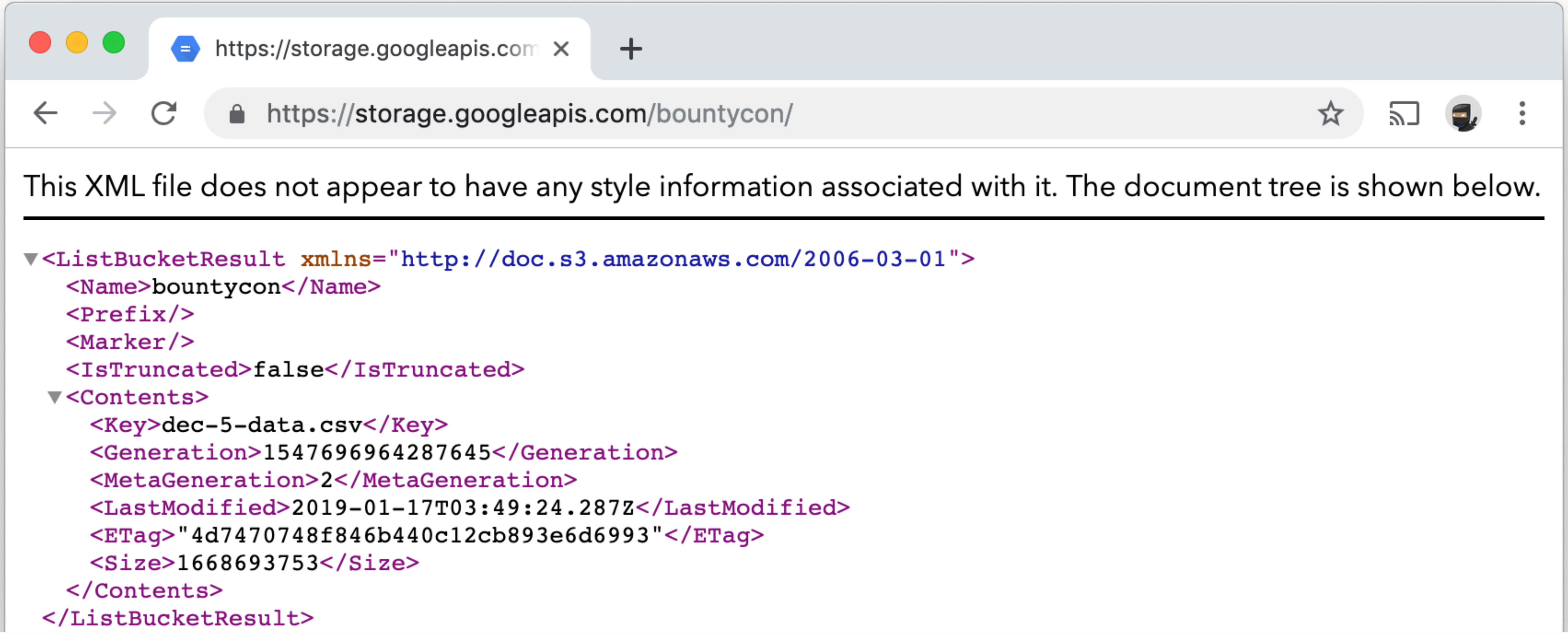
Google: [redacted] [redacted] [redacted]

# lots of storage buckets around the web have directory listing set to public causing data breaches

# what if there's a bucket named "bountycon"?

# let's open http://storage.googleapis.com/bountycon/ in a browser

Google: Public Cloudstore Bucket


https://storage.googleapis.com ×
+
https://storage.googleapis.com/bountycon/

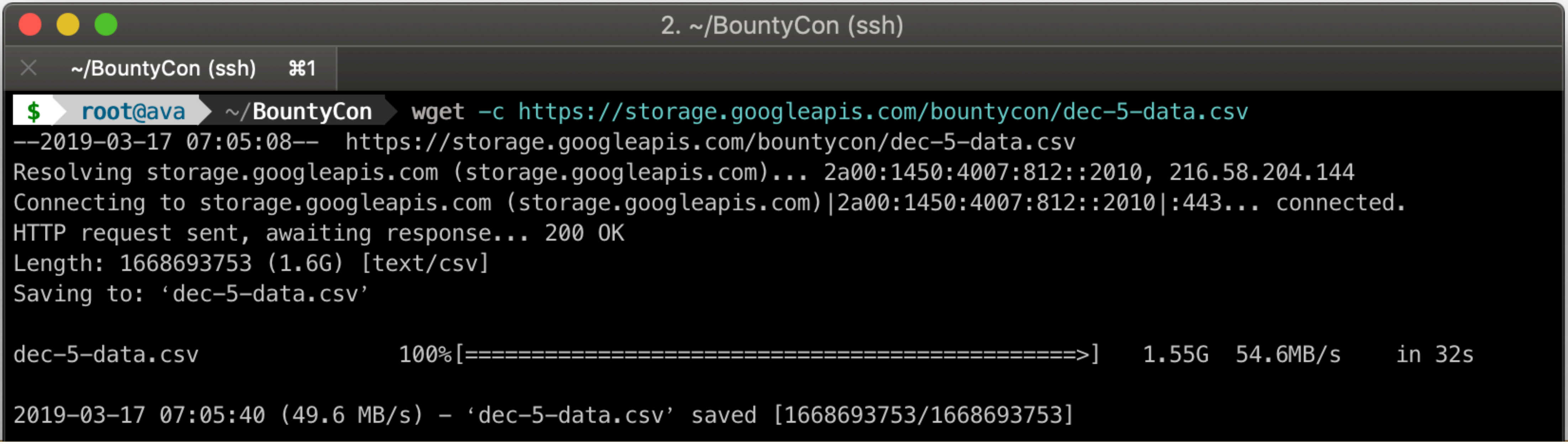
This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
▼<ListBucketResult xmlns="http://doc.s3.amazonaws.com/2006-03-01">
   <Name>bountycon</Name>
   <Prefix/>
   <Marker/>
   <IsTruncated>false</IsTruncated>
 ▼<Contents>
     <Key>dec-5-data.csv</Key>
     <Generation>1547696964287645</Generation>
     <MetaGeneration>2</MetaGeneration>
     <LastModified>2019-01-17T03:49:24.287Z</LastModified>
     <ETag>"4d7470748f846b440c12cb893e6d6993"</ETag>
     <Size>1668693753</Size>
   </Contents>
 </ListBucketResult>
```

Google: Public Cloudstore Bucket

file named `dec-5-data.csv` exists in the bucket and it's huge – 1.55GiB!

you have to download it to find the flag. use wget/curl and download on a server to download faster



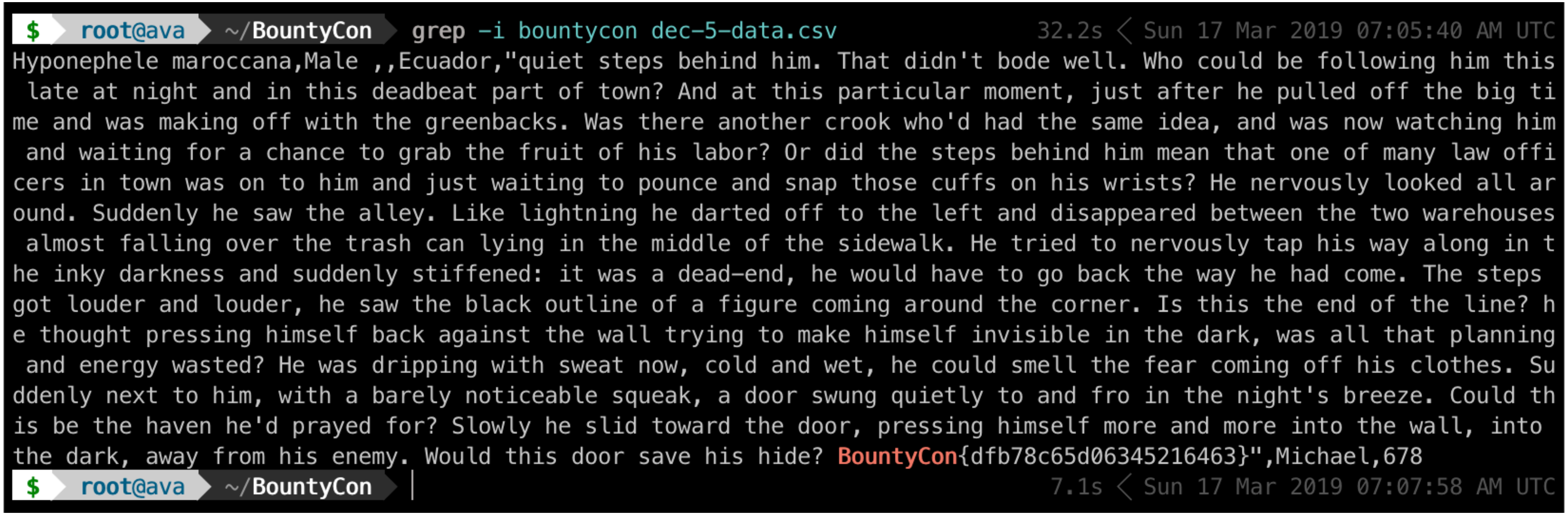
```
$  root@ava  ~/BountyCon  wget -c https://storage.googleapis.com/bountycon/dec-5-data.csv
--2019-03-17 07:05:08--  https://storage.googleapis.com/bountycon/dec-5-data.csv
Resolving storage.googleapis.com (storage.googleapis.com)... 2a00:1450:4007:812::2010, 216.58.204.144
Connecting to storage.googleapis.com (storage.googleapis.com)|2a00:1450:4007:812::2010|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1668693753 (1.6G) [text/csv]
Saving to: ‘dec-5-data.csv’

dec-5-data.csv              100%[==============================================>]   1.55G  54.6MB/s    in 32s

2019-03-17 07:05:40 (49.6 MB/s) - ‘dec-5-data.csv’ saved [1668693753/1668693753]
```

Google: Public Cloudstore Bucket

grep the file to find the flag:



```
$  root@ava  ~/BountyCon  grep -i bountycon dec-5-data.csv          32.2s < Sun 17 Mar 2019 07:05:40 AM UTC
Hyponephele maroccana,Male ,,Ecuador,"quiet steps behind him. That didn't bode well. Who could be following him this
 late at night and in this deadbeat part of town? And at this particular moment, just after he pulled off the big ti
me and was making off with the greenbacks. Was there another crook who'd had the same idea, and was now watching him
 and waiting for a chance to grab the fruit of his labor? Or did the steps behind him mean that one of many law offi
cers in town was on to him and just waiting to pounce and snap those cuffs on his wrists? He nervously looked all ar
ound. Suddenly he saw the alley. Like lightning he darted off to the left and disappeared between the two warehouses
 almost falling over the trash can lying in the middle of the sidewalk. He tried to nervously tap his way along in t
he inky darkness and suddenly stiffened: it was a dead-end, he would have to go back the way he had come. The steps
got louder and louder, he saw the black outline of a figure coming around the corner. Is this the end of the line? h
e thought pressing himself back against the wall trying to make himself invisible in the dark, was all that planning
 and energy wasted? He was dripping with sweat now, cold and wet, he could smell the fear coming off his clothes. Su
ddenly next to him, with a barely noticeable squeak, a door swung quietly to and fro in the night's breeze. Could th
is be the haven he'd prayed for? Slowly he slid toward the door, pressing himself more and more into the wall, into
the dark, away from his enemy. Would this door save his hide? BountyCon{dfb78c65d06345216463}",Michael,678
$  root@ava  ~/BountyCon  |                                                   7.1s < Sun 17 Mar 2019 07:07:58 AM UTC
```

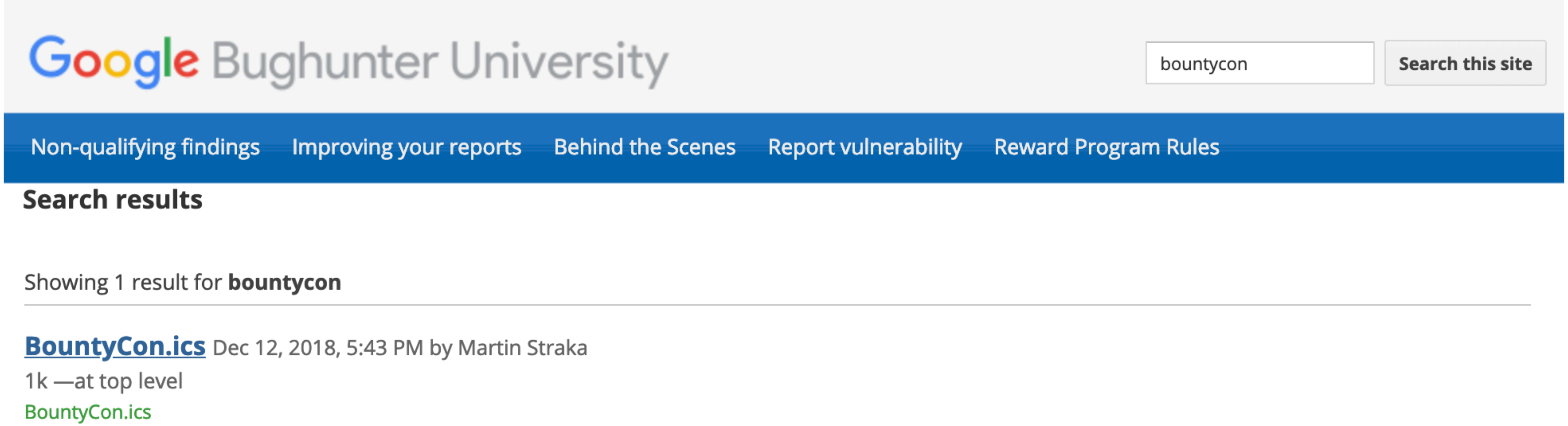
Google: Public Cloudstore Bucket

99 points

Google: Bug Hunter University Steganography

# most of the Google flags were in security related pages

# the Bug Hunter University site has a flag hidden in the "`BountyCon.ics`" file that you could find by searching for "BountyCon":



Search results

Showing 1 result for **bountycon**

BountyCon.ics Dec 12, 2018, 5:43 PM by Martin Straka
1k —at top level
BountyCon.ics

Google: Bug Hunter University Steganography

# after finding the ICS file, I tried to list all other files that might been added/updated on the site

# Google Sites exposes an endpoint for getting the RSS feed:

https://sites.google.com/feeds/content/site/bughunteruniversity

# the RSS feed gave away that:

# the home page was updated around the time (2018-12-11) the ICS file was added (2018-12-12)

# on 2018-12-06, `bug200_new.jpg` and `bug200_new (1).jpg` were uploaded

# only the latter image was linked on the home page, the other is simply a dud that nobody deleted

# `bug200_new (1).jpg` seemed like a suspicious file name because of "`_new`" and "`(1)`"

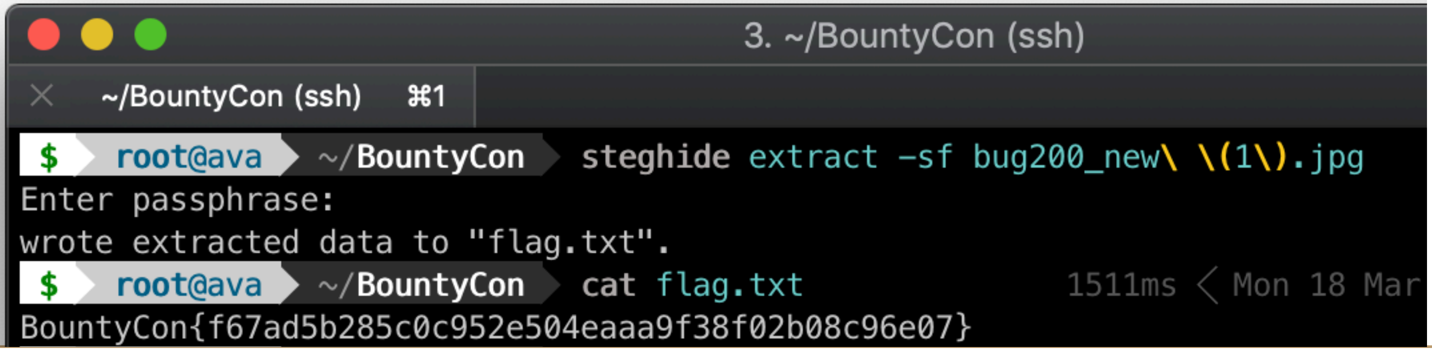
Google: Bug Hunter University Steganography

# if you're a CTF player and you see an interesting image, the first thing that will come to your mind is steganography

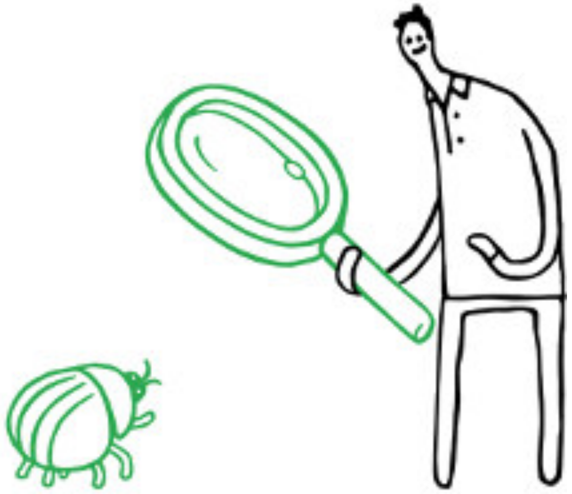
# lots of different steganography tools

# use steghide to extract data from the image

# a file named `flag.txt` will be extracted with the flag:



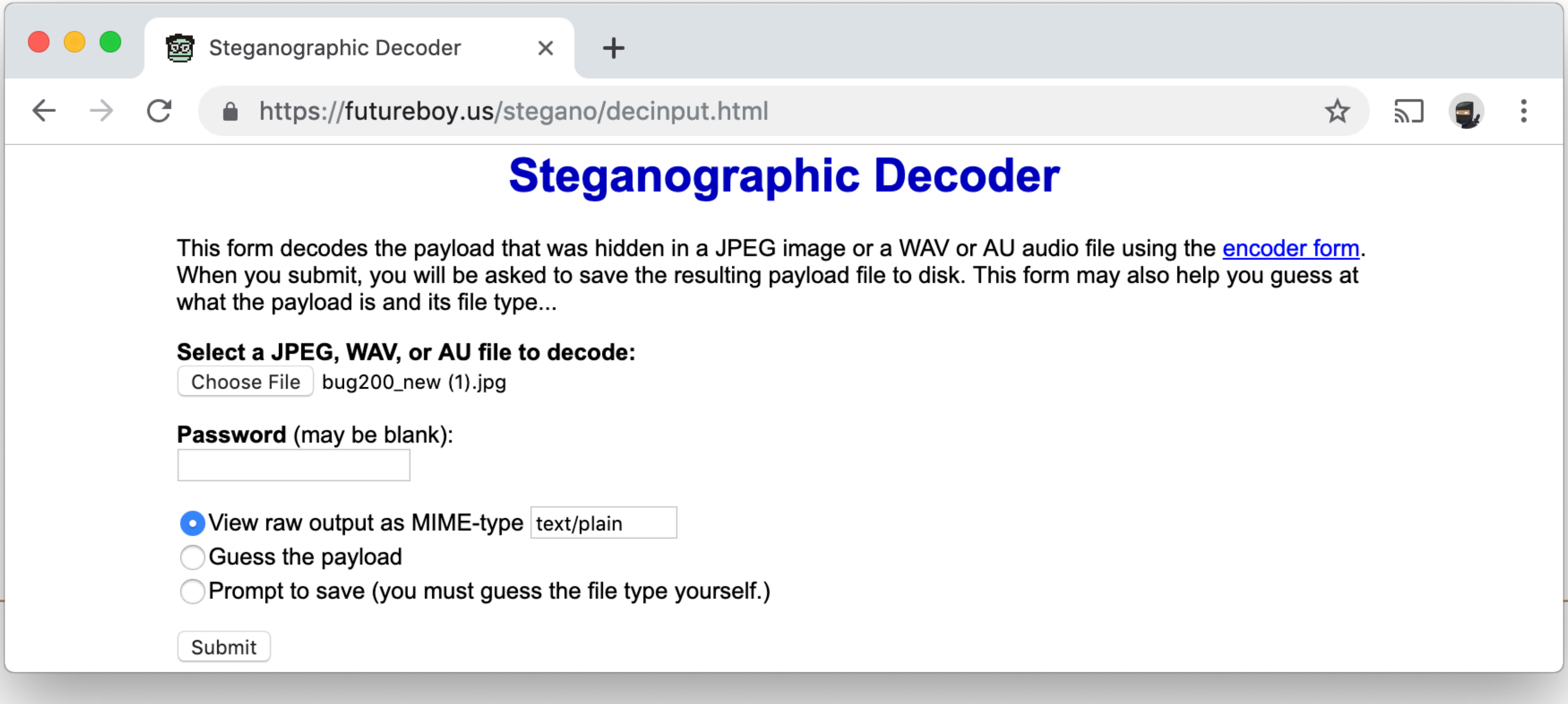
```
$  root@ava  ~/BountyCon  steghide extract -sf bug200_new\ \(1\).jpg
Enter passphrase:
wrote extracted data to "flag.txt".
$  root@ava  ~/BountyCon  cat flag.txt                  1511ms 〈 Mon 18 Mar
BountyCon{f67ad5b285c0c952e504eaaa9f38f02b08c96e07}
```



Google: Bug Hunter University Steganography

steghide not installed? you can instead use an online wrapper of steghide:

https://futureboy.us/stegano/decinput.html



Steganographic Decoder

This form decodes the payload that was hidden in a JPEG image or a WAV or AU audio file using the encoder form. When you submit, you will be asked to save the resulting payload file to disk. This form may also help you guess at what the payload is and its file type...

Select a JPEG, WAV, or AU file to decode:
Choose File bug200_new (1).jpg

Password (may be blank):

● View raw output as MIME-type text/plain
○ Guess the payload
○ Prompt to save (you must guess the file type yourself.)

Submit

Google: Bug Hunter University Steganography

100 points

Google: TLS Certificate

# what if there's a secret site where you can find more BountyCon challenges?

# you can make up a bunch of possible links and try accessing them:

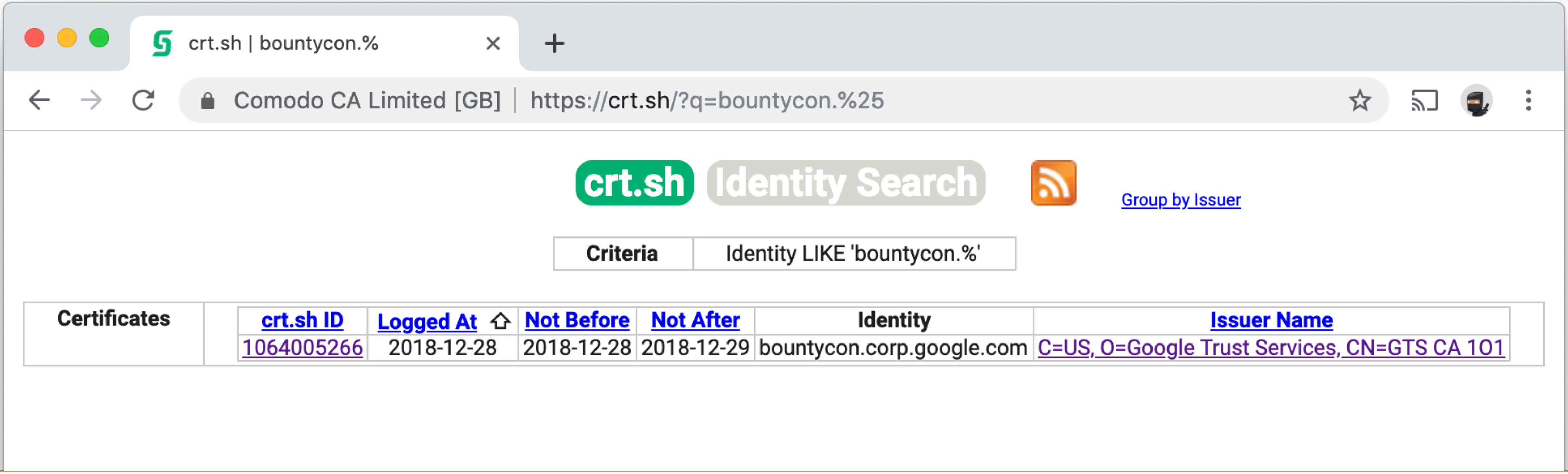
  # bountycon.google.com, bountycon.facebook.com, bountycon.fb.com

  # goo.gl/bountycon, fb.com/bountycon

# you can also search certificate transparency logs if any certificate was issued for a domain matching "bountycon"

Google: TLS Certificate

crt.sh is one of the sites you can use to search certificate transparency logs:



Criteria	Identity LIKE 'bountycon.%'

Certificates

crt.sh ID	Logged At ⇧	Not Before	Not After	Identity	Issuer Name
1064005266	2018-12-28	2018-12-28	2018-12-29	bountycon.corp.google.com	C=US, O=Google Trust Services, CN=GTS CA 1O1

Google: TLS Certificate

# there's a match: bountycon.corp.google.com

# *.corp.google.com addresses are only accessible over Google's internal networks

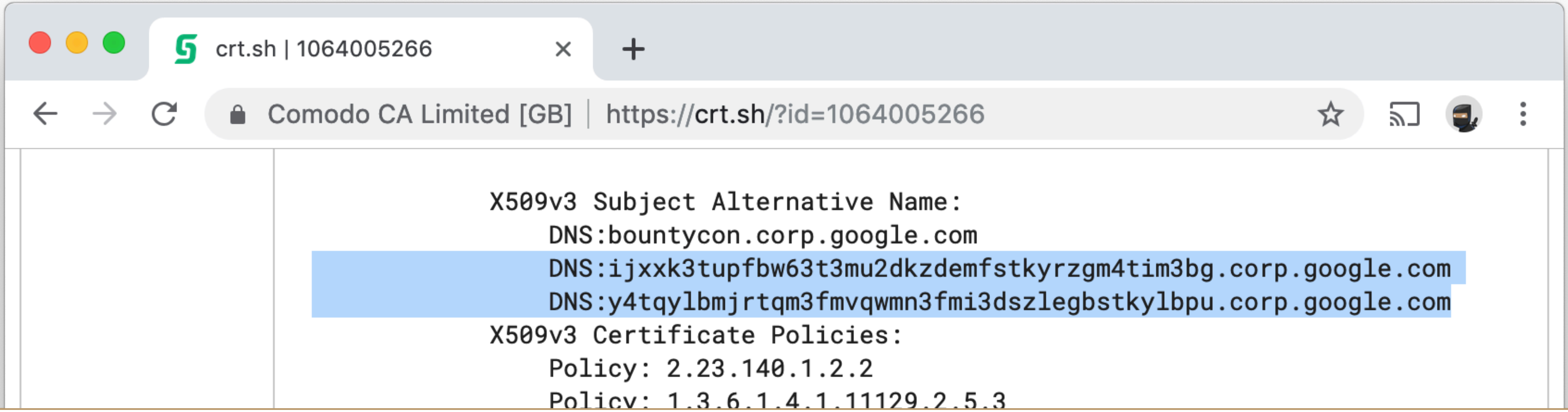
# there are no public DNS records for that domain

# it's entirely possible that the site is for Google employees to assist them with something BountyCon related

Google: TLS Certificate

# let's inspect the certificate

# you'll notice the cert has been issued for two extra domains with random seeming subdomains:



```
        X509v3 Subject Alternative Name:
            DNS:bountycon.corp.google.com
            DNS:ijxxk3tupfbw63t3mu2dkzdemfstkyrzgm4tim3bg.corp.google.com
            DNS:y4tqylbmjrtqm3fmvqwmn3fmi3dszlegbstkylbpu.corp.google.com
        X509v3 Certificate Policies:
            Policy: 2.23.140.1.2.2
            Policy: 1.3.6.1.4.1.11129.2.5.3
```

Google: TLS Certificate

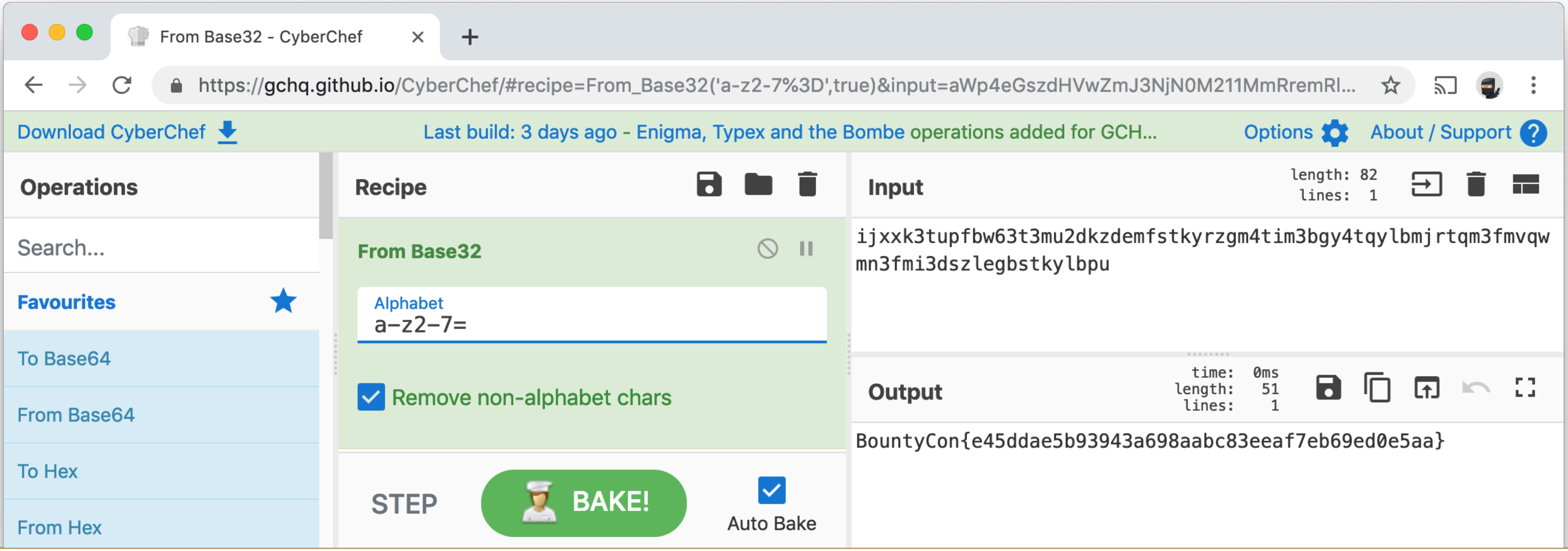
# `ijxxk3tupfbw63t3mu2dkzdemfstkyrzgm4tim3bg` and `y4tqylbmjrtqm3fmvqwmn3fmi3dszlegbstkylbpu` look like encoded strings or link fragments

# base64 obviously requires upper case characters and DNS names cannot have them

# so it must be in base32!

Google: TLS Certificate

base32 decode both subdomains together to get the flag:


From Base32 - CyberChef
https://gchq.github.io/CyberChef/#recipe=From_Base32('a-z2-7%3D',true)&input=aWp4eGszdHVwZmJ3NjN0M211MmRremRl...
Download CyberChef
Last build: 3 days ago - Enigma, Typex and the Bombe operations added for GCH...
Options
About / Support
Operations
Search...
Favourites
To Base64
From Base64
To Hex
From Hex
Recipe
STEP
BAKE!
☑ Auto Bake

From Base32

Alphabet: a-z2-7=

☑ Remove non-alphabet chars

Input (length: 82, lines: 1)

```
ijxxk3tupfbw63t3mu2dkzdemfstkyrzgm4tim3bgy4tqylbmjrtqm3fmvqwmn3fmi3dszlegbstkylbpu
```

Output (time: 0ms, length: 51, lines: 1)

```
BountyCon{e45ddae5b93943a698aabc83eeaf7eb69ed0e5aa}
```

Google: TLS Certificate

100 points

random tips

# ask yourself, "where would I hide a flag if I had to hide one?"

# note down good ideas of what you tried but didn't work, because it might in the future

# look for patterns

    # most of the BountyCon flags were in security/whitehat related pages

    # both Google and Facebook had a flag hidden in their respective vulnerability submission pages

# put your computer to use. use automated tools to notify you when a potential flag is found

    # like Burp Suite or any proxy that constantly searches network traffic for string matches

$ exit

full writeup of all 30 🚩 on KishanBagaria.com

$ exit

# 🙌 reach out on

# 🐦 twitter: @KishanBagaria

# ✉️ hi@kishan.info

# official BountyCon Slack

# IRL – I don't bite

$ exit

thanks for listening! 🙏