BREAKING INTO GOOGLE'S ADMIN PANEL & TWITTER'S DM/NOTIFICATIONS

DEF CON

DC 0471 TRIVANDRUM

Vishnu Prasad PG
MashupStack

29th September, 2018

#About Me

$ **Vishnu Prasad P G**

$ Student Developer at **MashupStack** & Final year engineering student at **PRS College of Engineering.**

$ Listed as the Global Top VRP Researcher in 2017 by Google & Ranked in the 1st Page of Hall of Fame of Google Bug Bounty Hunters.

$ Python tools developer, Open source lover and contributor.

LET'S GET INTO MY TOPIC

This explains the recon I performed to find the way to Google admin panel.

which allowed me access to different varieties of administrative controls of various google products including YouTube TV, YouTube Broadcasting satellite, PCSC admin panel, Router management, etc.

Google acknowledged the bug as P0 (Extremely critical) multiple times and I was awarded with $13337.

Similarly, in Twitter, a critical security flaw allowed me to read DM's and notifications of any user even after the user logs out of the system via browser notifications. This bug was acknowledged and fixed by Twitter thereby adding me to their Hall of Fame.

Let’s start with Google

Recon Recon Recon……..

One day, while searching for new bugs in Google ⍰ , I got some of Google’s IP addresses from some disclosure of their internal issues. (I had no idea what to do with these IP addresses ⍰)

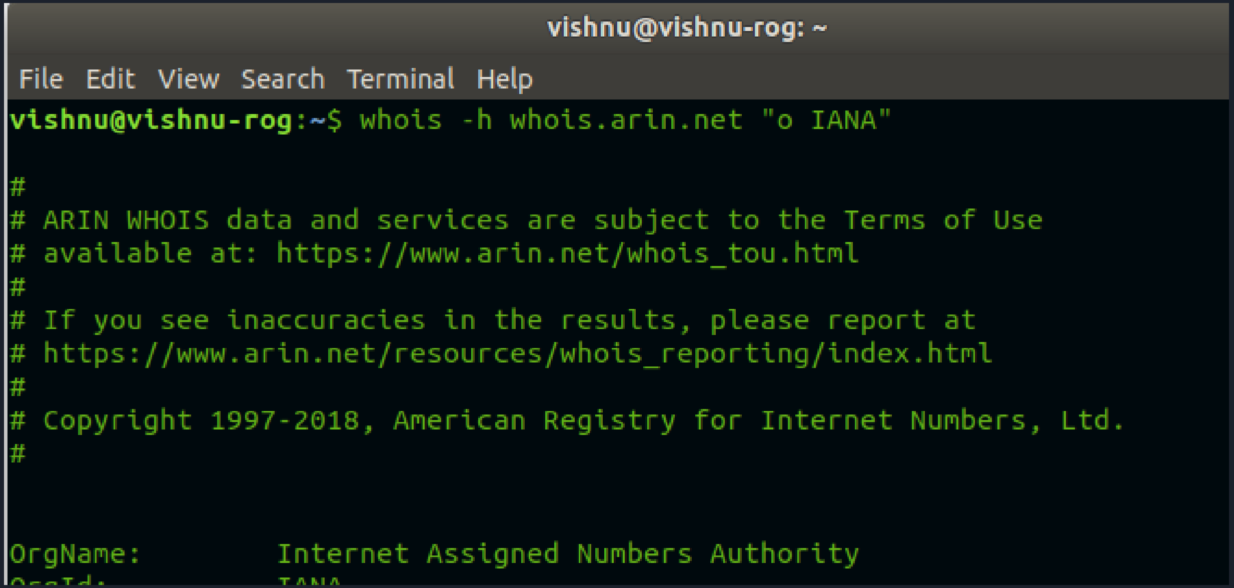
My idea was to find more like this using ASN via ARIN

What is ARIN ?

The American Registry for Internet Numbers is the Regional Internet Registry for Canada, the United States, and many Caribbean and North Atlantic islands. ARIN manages the distribution of Internet number resources, including IPv4 and IPv6 address space and AS numbers.

It’s simple .. Powerful...Robust □

I just searched for organisation ASN via ARIN and its intresting...



```
vishnu@vishnu-rog:~$ whois -h whois.arin.net "o IANA"

#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/whois_tou.html
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/whois_reporting/index.html
#
# Copyright 1997-2018, American Registry for Internet Numbers, Ltd.
#


OrgName:        Internet Assigned Numbers Authority
OrgId:          IANA
```

Sort -> Scan -> Repeat

- My idea was to sort these IP's using the details from ARIN.
- So I just made a **bash script** and sort out IP's that belongs only to a particular Organization.
- And finally I sorted out .. (It's feels like a 100 year passed)
- Next is to check for all IP's (Made a bash script and it's opens all it to browsers)

Nothing worked…. Tired..!

Now what to do !!!

Sort -> Scan -> Repeat

So i tried from **mobile**.. . NO LUCK!

Because Sreeram already reported it and Google fixed it.

So stuck again ! Now What !!!

The alternate way

Then I read about a recent Google CTF blog

EUREKAAA!!!

Maybe….. There is an option.

So if i can get into any Google server whitelisted server, maybe i can get in…

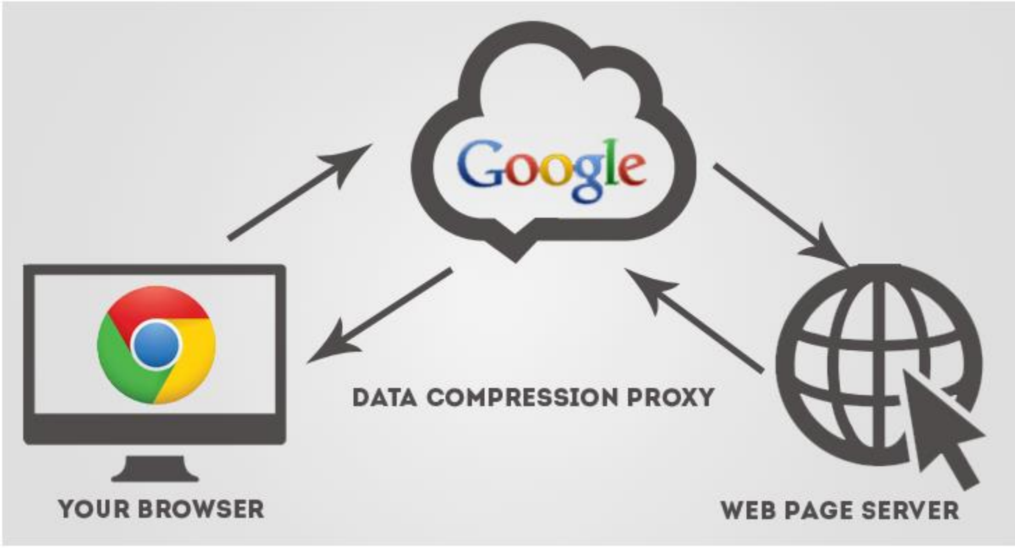
So if i can get into any such proxy, maybe i can get in…

So if i can install a Google data server addon, it through Google whitelisted server.

Maybe i can get in. and YES !!!! BINGO ! I was able to get in !!

The grand mystery had been decoded !

It was Google's Data saver that helped me to access their internal IP's. It was turned on in my Chrome mobile browser.



What is data compression proxy ?

The core optimizations that allow us to reduce overall data usage are performed by Google servers. When Data Saver is enabled, Chrome opens a connection between your phone and one of the optimization servers running in Google's datacenters and relays all non-encrypted HTTP requests over this connection.

How as a access proxy ?

Unfortunately, They allow all connections from google datacenters and the compression proxy is also making connections via Google’s datacenters.

And Finally...

- I used same method to access some of their other panel too..
- Including YouTube TV, YouTube Broadcasting satellite, PCSC admin panel, Router management, etc.

And I was able to login to the ADMIN PANEL !

You won’t believe me !
They had the DEFAULT PASSWORD!!!

And some DIDN’T HAVE A PASSWORD!!

That’s All For Google

The Fix

They made all the IP's separate from public connections

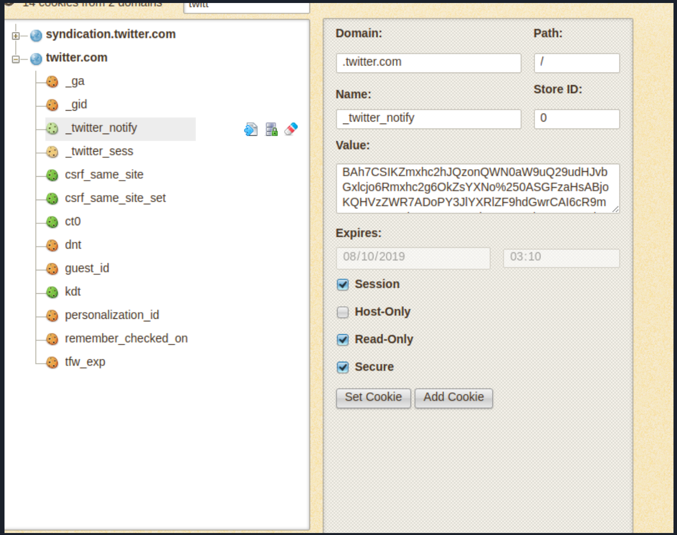
They make data saver as a separate proxy connection.

Now Let’s Move To Twitter

Read DM’s and notifications of any user even after the user logs out of the system via browser notifications.

Misconfiguration Everywhere..!

- ★ It was a simple misconfiguration issue where they used different authentication cookies for *.twitter.com and another for Browser Notifications.
- ★ When you turn ON browser notifications it's create a new cookie.
- ★ When you logout from the system the cookies for *.twitter.com is only expiring and other one is still active



14 cookies from 2 domains twitt

- syndication.twitter.com
- twitter.com
  - _ga
  - _gid
  - _twitter_notify
  - _twitter_sess
  - csrf_same_site
  - csrf_same_site_set
  - ct0
  - dnt
  - guest_id
  - kdt
  - personalization_id
  - remember_checked_on
  - tfw_exp

Domain: .twitter.com

Path: /

Name: _twitter_notify

Store ID: 0

Value: BAh7CSIKZmxhc2hJQzonQWN0aW9uQ29udHJvbGxlcjo6Rmxhc2g6OkZsYXNo%250ASGFzaHsABjoKQHVzZWR7ADoPY3JlYXRlZF9hdGwrCAI6cR9m

Expires: 08/10/2019 03:10

☑ Session

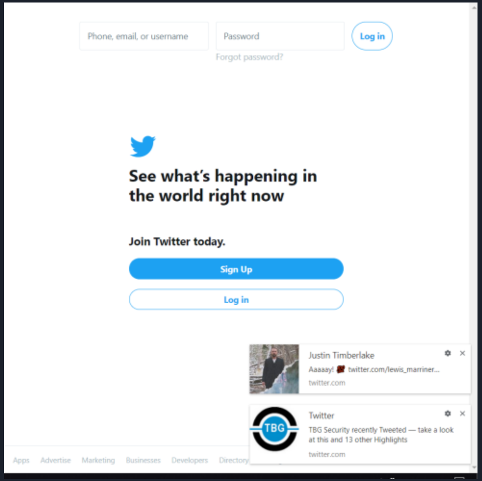
☐ Host-Only

☑ Read-Only

☑ Secure

How it's works ?

- *When you have a Message or Notification in Twitter , it will show up in browser even if you are not an authenticated user.*
- *It will show you all the messages and notifications in detail.*



Phone, email, or username

Password

Log in

Forgot password?

See what's happening in the world right now

Join Twitter today.

Sign Up

Log in

Justin Timberlake

Aaaaay! twitter.com/lewis_marriner...

twitter.com

Twitter

TBG Security recently Tweeted — take a look at this and 13 other Highlights

twitter.com

The Fix

- They merged the cookies for both twitter and browser notification and awarded a cool bounty :p
- Also they awarded me their Hall Of Fame.

Let's Stop here..

ThankYou!

Vishnu Prasad G
+91 - 8547838966
www.vishnuprasadpg.com
info@vishnuprasadpg.com