

```
root@kali:~/Desktop/Tools/Sublist3r# python sublist3r.py -d tesla.com
```

Sublist3r

Coded By Ahmed Aboul-Ela - @aboul3la

```
[*] Enumerating subdomains now for tesla.com
[*] Searching now in Baidu..
[*] Searching now in Yahoo..
[*] Searching now in Google..
[*] Searching now in Bing..
[*] Searching now in Ask..
[*] Searching now in Netcraft..
[*] Searching now in DNSdumpster..
[*] Searching now in Virusstat..
[*] Searching now in ThreatCrowd..
[*] Searching now in SSL Certificate..
[*] Searching now in PassiveDNS..
[!] Error: Google probably now is blocking our requests
[*] Finished now the Google Enumeration ...
[*] Total Unique Subdomains Found: 21
```

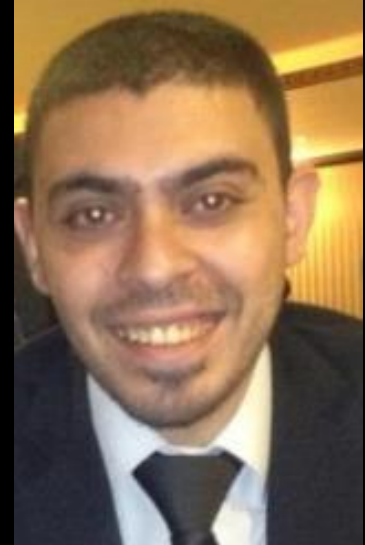
```
www.tesla.com
auth.tesla.com
autodiscover.tesla.com
blog.tesla.com
comparison.tesla.com
dev.tesla.com
eua-origin.tesla.com
forums.tesla.com
imap.tesla.com
ir.tesla.com
lyncdiscover.tesla.com
model3.tesla.com
my.tesla.com
naa-origin.tesla.com
nas-origin.tesla.com
new.tesla.com
new-dev.tesla.com
partners.tesla.com
pop.tesla.com
powerwall.tesla.com
resources.tesla.com
shop.tesla.com
```

GitHub Recon and Sensitive Data Exposure



Module Trainer

- Majd Aldeen Atiyat
 - [@th3g3nt3lman- Twitter](#)
 - [@th3g3nt3lman- Bugcrowd](#)
- Security Advisor, Penetration Tester
- Bugcrowd Ambassador



Module Outline

1. Introduction About Github
2. Github For Bug Bounty
3. Finding Sensitive Information Leaks
 - a. Manual Approach
 - b. Automation Approach
4. Resources and References



bugcrowd.com

Module Reading

★ Blogs:

- [A deep dive into ASW S3 access controls](#)

★ Video:

- <https://www.youtube.com/watch?v=x5VKuFjvrk>

★ Tools

- <https://github.com/koenrh/s3enum/>

```
root@kali:~/Desktop/Tools/Sublist3r# python sublist3r.py -d tesla.com
```

Sublist3r

Coded By Ahmed Aboul-Ela - @aboul3la

```
[*] Enumerating subdomains now for tesla.com
[*] Searching now in Baidu..
[*] Searching now in Yahoo..
[*] Searching now in Google..
[*] Searching now in Bing..
[*] Searching now in Ask..
[*] Searching now in Netcraft..
[*] Searching now in DNSdumpster..
[*] Searching now in Virustotal..
[*] Searching now in ThreatCrowd..
[*] Searching now in SSL Certificates..
[*] Searching now in PassiveDNS..
[!] Error: Google probably now is blocking the crawler
[*] Finished now the Google Enumeration ..
[*] Total Unique Subdomains Found: 36
```

```
www.tesla.com
auth.tesla.com
autodiscover.tesla.com
blog.tesla.com
comparison.tesla.com
dev.tesla.com
eua-origin.tesla.com
forums.tesla.com
imap.tesla.com
ir.tesla.com
lyncdiscover.tesla.com
model3.tesla.com
my.tesla.com
naa-origin.tesla.com
nas-origin.tesla.com
new.tesla.com
new-dev.tesla.com
partners.tesla.com
pop.tesla.com
powerwall.tesla.com
resources.tesla.com
shop.tesla.com
```

Introduction



Introduction to Github

- ★ **Git is a version control system, When developers create something (an app, for example), they make constant changes to the code.**
- ★ **Git is a command-line tool, but the center around which all things involving Git revolve is the [GitHub.com](https://github.com) where developers store their projects and network with like minded people**

Introduction to Github

- ★ **Developers store their projects in "A repository" which is a location where all the files for a particular project are stored. Each project has its own repo, and you can access it with a unique URL for user or organization, can be public or private.**

Introduction to Github

<https://github.com/bugcrowd>

Bugcrowd Organization page

31 Repositories

Each Repo has its own data/code

9 People (Employees)

The screenshot displays the GitHub profile for the organization Bugcrowd. At the top left is the Bugcrowd logo, an orange square with a white lowercase 'b'. To its right, the organization name 'Bugcrowd' is shown, followed by the tagline 'A radical cybersecurity advantage.', the location 'San Francisco', and the website 'https://www.bugcrowd.com'. Below this, navigation tabs for 'Repositories 31', 'Packages', and 'People 9' are visible. A search bar for repositories is present, along with filters for 'Type: All' and 'Language: All'. The first repository listed is 'vulnerability-rating-taxonomy', described as 'Bugcrowd's baseline priority ratings for common security vulnerabilities'. It includes tags for 'taxonomy', 'rating', 'vulnerabilities', 'vrt', and 'bugcrowd', and shows statistics for Python, Apache-2.0, 24 forks, 133 stars, 3 issues, and 0 pull requests, updated 2 days ago. The second repository is 'hedge', described as 'Percy GitHub integration', with statistics for Elixir, 0 forks, 4 stars, 1 issue, and 0 pull requests, updated 4 days ago.

Introduction to Github

Creating Your Own Repo

Create a new repository

A repository contains all project files, including the revision history. Already have a project repository elsewhere? [Import a repository](#).

Owner



th3g3nt3lman1 ▾



Repository name *

MyProject



Great repository names are short and memorable. Need inspiration? How about **improved-octo-couscous**?

Description (optional)



Public

Anyone can see this repository. You choose who can commit.



Private

You choose who can see and commit to this repository.

```
root@kali:~/Desktop/Tools/Sublist3r# python sublist3r.py -d tesla.com
```

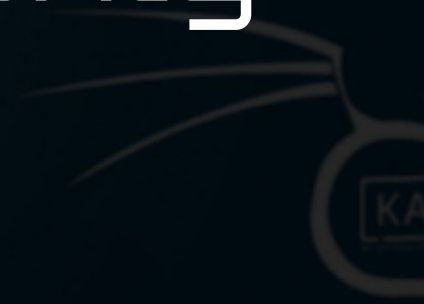
Sublist3r

Coded By Ahmed Aboul-Ela - @aboul3la

```
[*] Enumerating subdomains now for tesla.com
[*] Searching now in Baidu..
[*] Searching now in Yahoo..
[*] Searching now in Google..
[*] Searching now in Bing..
[*] Searching now in Ask..
[*] Searching now in Netcraft..
[*] Searching now in DNSdumpster..
[*] Searching now in Virustotal..
[*] Searching now in ThreatCrowd..
[*] Searching now in SSL Certificates..
[*] Searching now in PassiveDNS..
[!] Error: Google blocked requests
[*] Finished now the google enumeration.
[*] Total Unique Subdomains Found: 36
```

```
www.tesla.com
auth.tesla.com
autodiscover.tesla.com
blog.tesla.com
comparison.tesla.com
dev.tesla.com
eua-origin.tesla.com
forums.tesla.com
imap.tesla.com
ir.tesla.com
lyncdiscover.tesla.com
model3.tesla.com
my.tesla.com
naa-origin.tesla.com
nas-origin.tesla.com
new.tesla.com
new-dev.tesla.com
partners.tesla.com
pop.tesla.com
powerwall.tesla.com
resources.tesla.com
shop.tesla.com
```

GitHub For Bug Bounty



Github For Bug Bounty

- ★ **Github is a great resource for the bug bounty hunter to know more about the target, where you can search for a lot of stuff and get to know more information about the company infrastructure, products they use and internal details that can be used later on in your pentest process.**
- ★ **You can search for a company name or domain (company) or (company.com) in the github search area to see what projects and repos are pushed to github, and in most cases you will end up finding a thousands of results.**

Github For Bug Bounty

The screenshot shows a GitHub search interface. At the top, the search bar contains "bugcrowd.com". Navigation links include "Pull requests", "Issues", "Marketplace", and "Explore". On the left, a sidebar lists categories: Repositories (3), Code (2K), Commits (21), Issues (39), Packages (0), Marketplace (0), Topics (0), Wikis (19), and Users (3). Below this is a "Languages" section with a table:

Language	Count
Markdown	791
HTML	667
JSON	180
Text	163
CSV	79

The main content area displays "2,130 code results". The first result is from "alfredo1111/lb-192-30-252-153-iad.github.io" with the file "hosts.js". It shows the top six matches, with the first match being a JSON object:

```
1 {"api.bugcrowd.com": "104.20.61.51", "blog.bugcrowd.com": "104.20.5.239", "email.bugcrowd.com": "104.20.60.51"}
```

The second result is from the same repository with the file "hosts.txt", showing the top 12 matches. The first seven matches are IP addresses associated with various subdomains of bugcrowd.com:

```
1 api.bugcrowd.com, 104.20.61.51
2 blog.bugcrowd.com, 104.20.4.239
3 bounce.bugcrowd.com, 192.28.152.174
4 bugcrowd.com, 104.20.5.239
5 collateral.bugcrowd.com, 52.72.78.170
6 docs.bugcrowd.com, 104.20.5.239
7 email.bugcrowd.com, 104.20.60.51
```

The third result is from "hackers-terabit/ggitm" with the file "Bugcrowd.com.xml", showing the top four matches. The first match is a URL:

```
1 https://panopticclick.eff.org
```

Github For Bug Bounty

- ★ Creativity is required by looking for specific keywords in order to get the information you are looking for, you can look for services like (ssh, sftp, ftp, proxy, vpn, vsphere, internal, siem, firewall, etc.) and then again narrow down your search and check the code committed that might contains valuable information leads to vulnerabilities.
- ★ Search results are not all for the company or uploaded by company, it can be notes from random people, news, data gathering, recon tools, etc.

```
root@kali:~/Desktop/Tools/Sublist3r# python sublist3r.py -d tesla.com
```

Sublist3r

Coded By Ahmed Aboul-Ela - @aboul3la

```
[*] Enumerating subdomains now for tesla.com
```

```
[*] Searching now in Baidu..
```

```
[*] Searching now in Yahoo..
```

```
[*] Searching now in Google..
```

```
[*] Searching now in Bing..
```

```
[*] Searching now in Ask..
```

```
[*] Searching now in Netcraft..
```

```
[*] Searching now in DNSdumper..
```

```
[*] Searching now in Virustotal..
```

```
[*] Searching now in ThreatCloud..
```

```
[*] Searching now in SSL Certificate..
```

```
[*] Searching now in PassiveDNS..
```

```
[!] Error: Google probably now is blocking our requests
```

```
[*] Finished now the Google Enumeration ...
```

```
[*] Total Unique Subdomains:
```

```
www.tesla.com
```

```
auth.tesla.com
```

```
autodiscover.tesla.com
```

```
blog.tesla.com
```

```
comparison.tesla.com
```

```
dev.tesla.com
```

```
eua-origin.tesla.com
```

```
forums.tesla.com
```

```
imap.tesla.com
```

```
ir.tesla.com
```

```
lyncdiscover.tesla.com
```

```
model3.tesla.com
```

```
my.tesla.com
```

```
naa-origin.tesla.com
```

```
nas-origin.tesla.com
```

```
new.tesla.com
```

```
new-dev.tesla.com
```

```
partners.tesla.com
```

```
pop.tesla.com
```

```
powerwall.tesla.com
```

```
resources.tesla.com
```

```
shop.tesla.com
```

Finding Sensitive Information Leaks

Manual Approach

- ★ This can be simply done by searching for specific keywords in github search area , below basic examples :

"Company" password	"Company" key
"Company" secret	"Company" pass
"Company" credentials	"Company" login
"Company" token	"Company" ftp
"Company" config	"Company" pwd

Manual Approach

- ★ **With your creativity there is a lot of stuff to look for, below some examples i usually use :**

Search term	Results expected
"Company" security_credentials	LDAP (active directory)
"Company" connectionstring	Database Credentials
"Company" JDBC	Database Credentials
"Company" ssh2_auth_password	Unauthorized Access to Servers
"Company" send_keys or send,keys	If other keywords related to passwords failed

<https://github.com/random-robbie/keywords/blob/master/keywords.txt>

Manual Approach

```
1 env.put(javax.naming.Context.PROVIDER_URL, "ldap://172.16.0.197/cn=pdm.admin,ou=admin user,ou=DG tpe,DC=test,DC=com");
2 env.put(javax.naming.Context.SECURITY_AUTHENTICATION, "Simple");
3 //env.put(javax.naming.Context.SECURITY_PRINCIPAL, "cn=piduser,ou=DGUsers,ou=DG,DC=cn,DC=test,DC=com");
4 env.put(javax.naming.Context.SECURITY_PRINCIPAL, "cn=test,OU=PLM,OU=CA,OU=CIT,OU=TPV TPE,DC=test,DC=com");
5 //env.put(javax.naming.Context.SECURITY_CREDENTIALS , "piduser" );
6 env.put(javax.naming.Context.SECURITY_CREDENTIALS , "cscxx112129" );
7 //env.put(javax.naming.Context.SECURITY_CREDENTIALS , "Pdm@d20$0421" );
```

```
1         'bundles',
2         r'',
3         )
4 ftp_th3g3nt31 = ftp('ftp.th3g3nt31man.com',
5         'ASbd5FD',
6         'AB$1B#6mAk1HH',
7         info('->Start to upload to th3g3nt31.ftp<-')
8 ftpcli = ftp(ftp_th3g3nt31)
```

```
1 import pypyodbc as pyodbc # you could alias
2 db_host = 'mspitsql15.test.th3g3nt31.org'
3 db_name = 'BISE'
4 db_user = 'empDS'
5 db_password = 'Seattle@98121'
```

```
1 {
2     "ConnectionStrings": {
3         "Default": "Server=10.0.75.1; Database=PhoneBookDb; User=sa; Password=123qwe;"
```

Manual Approach

Unauthorized Access to k8s Dashboards secrets

secrets

🔒 (Private) (Private) · Updated 6 months ago

P1 Resolved

\$2,500
40 points

Comments 2

Critical: Unauthorized Access to Account on enterprise ARMS

· Updated 3 days ago

P1 Resolved

\$2,000
40 points

Comments 8

Internal Password Leaked for " " " "

· Updated a month ago

P2 Resolved

\$4,000
20 points

Comments 6

Manual Approach

New Sensitive Credentials, secrets and tokens Leaked
(vspher,aws,jenkins) / Github

🔒 (Private) · Updated 6 months ago

P1 Resolved

\$1,000
40 points

Comments 3

Information Disclosure / Jira Accses / Internal Issues Leaked

· Updated 2 months ago

P1 Resolved

\$5,000
40 points

Comments 4

Sensitive information disclosure For configurations ,usernames,
passwords

🔒 (Closed) · Updated a year ago

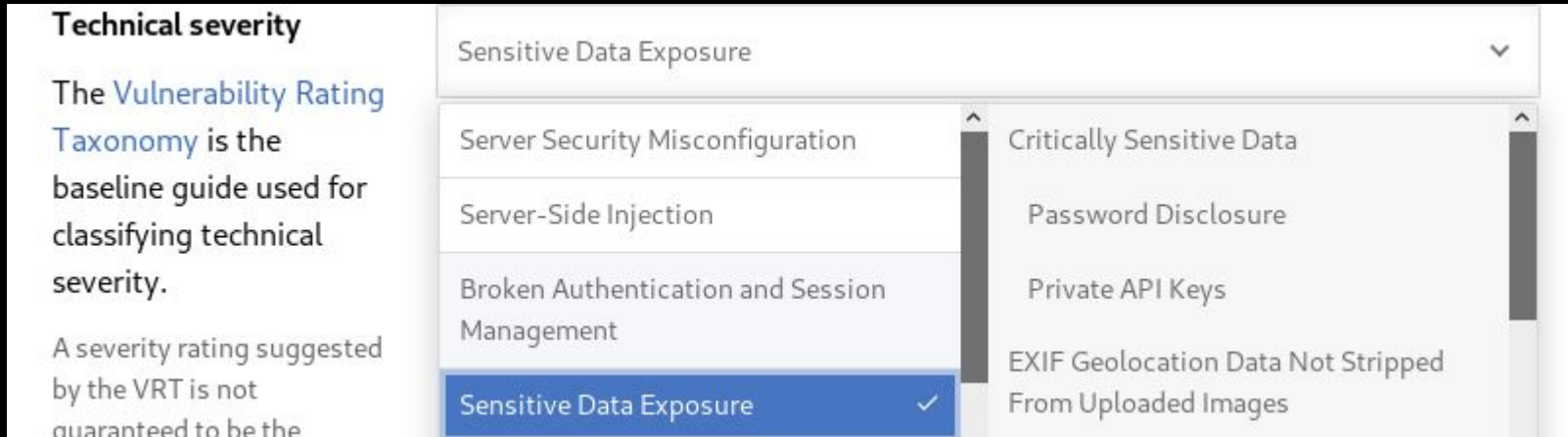
P1 Unresolved

\$5,000
40 points

Comments 9

Manual Approach

- ★ In Bugcrowd VRT this is considered as a P1 when reporting, however its subject to change based on the programs assessment for the risk and the access those leaks gave access to.



Technical severity

The [Vulnerability Rating Taxonomy](#) is the baseline guide used for classifying technical severity.

A severity rating suggested by the VRT is not guaranteed to be the

Sensitive Data Exposure	
Server Security Misconfiguration	Critically Sensitive Data
Server-Side Injection	Password Disclosure
Broken Authentication and Session Management	Private API Keys
Sensitive Data Exposure ✓	EXIF Geolocation Data Not Stripped From Uploaded Images

Manual Approach

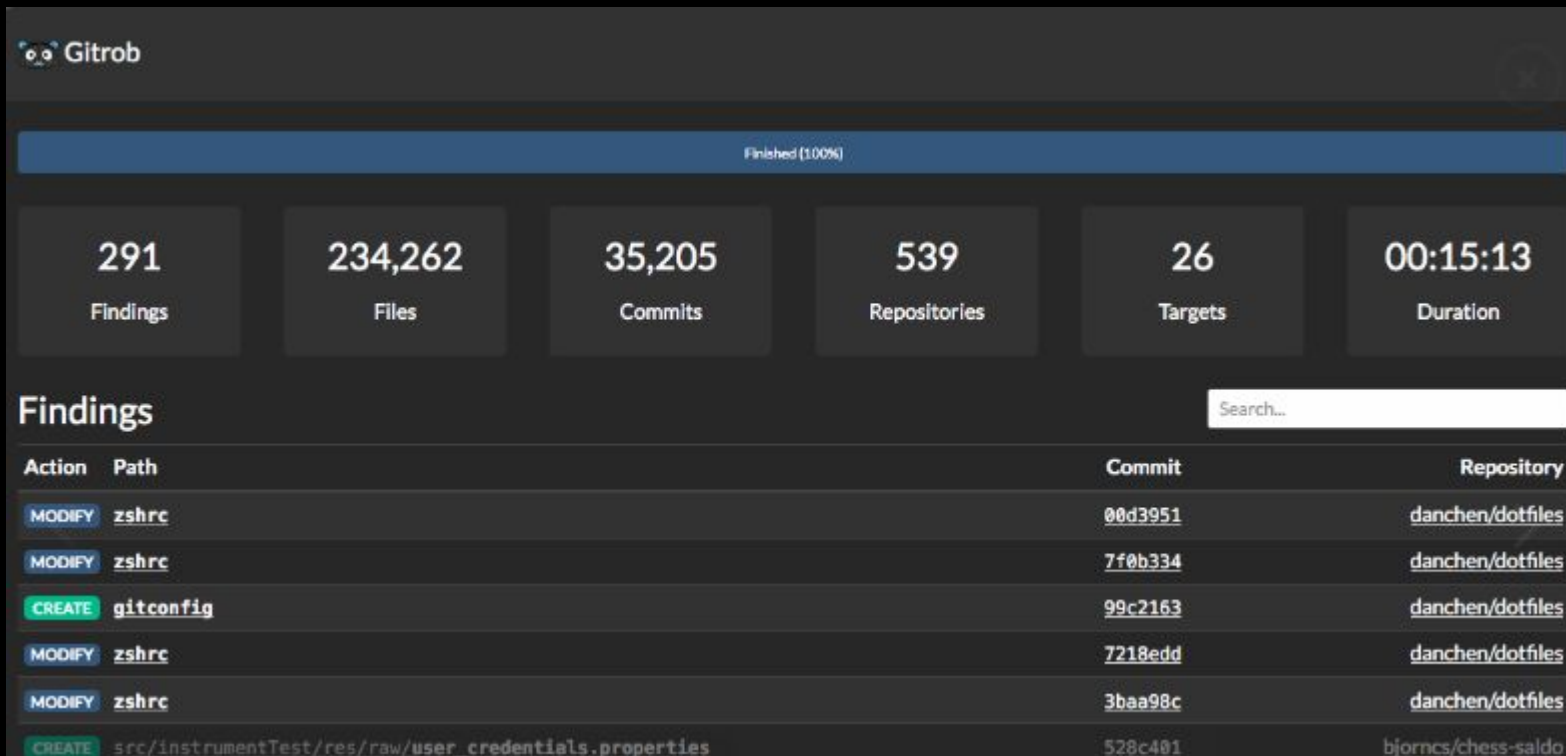
- ★ The valid submission must contain a proper written report explaining the leaked data impact on the company business and must be within scope.
- ★ When testing the leaked credentials stop after confirmation and don't try to dig more.
- ★ If the credentials are for internal & unreachable host where you can't provide an exploitation POC you can report it but its upto company to accept/reject submission based on their assessment.
- ★ Avoid sending old keys, old data, dummy/test password , in github you can sort results to the most updated ones.

Automation Approach

- ★ There is a lot of tools that automates searching in github , one of the most popular ones is "Gitrob", Gitrob is a tool to help find potentially sensitive files pushed to public repositories on Github. Gitrob will clone repositories belonging to a user or organization down to a configurable depth and iterate through the commit history and flag files that match signatures for potentially sensitive files. The findings will be presented through a web interface for easy browsing and analysis, for installation refer to the below link:

<https://github.com/michenriksen/gitrob>

Automation Approach



Automation Approach

- ★ While automation saves efforts and time, still a lot of employees repos gets missed in case they are not available in the organization people tab, while in manual you have the flexibility to search for everything.
- ★ Automation give a generic group of results based on sensitivity and you have to go through them all to find what sensitive and what's not, in manual you look for specific keyword and the results are easier to manage.
- ★ Reviewing the code manually can give you a nice information even though your keyword results are not good, you might find new subdomain, new endpoint, Ip address for a Dev/Staging/Prod system that you can target.


```
root@kali:~/Desktop/Tools/Sublist3r# python sublist3r.py -d tesla.com
```

Sublist3r

Coded By Ahmed Aboul-Ela - @aboul3la

```
[*] Enumerating subdomains now for tesla.com
[*] Searching now in Baidu..
[*] Searching now in Yahoo..
[*] Searching now in Google..
[*] Searching now in Bing..
[*] Searching now in Ask..
[*] Searching now in Netcraft..
[*] Searching now in DNSdumpster..
[*] Searching now in Virustotal..
[*] Searching now in ThreatCrowd..
[*] Searching now in SSL Certificate..
[*] Searching now in PassiveDNS..
[!] Error: Google probably now is blocking our requests
[*] Finished now the Google Enumeration ...
[*] Total Unique Subdomains Found: 36
```

```
www.tesla.com
auth.tesla.com
autodiscover.tesla.com
blog.tesla.com
comparison.tesla.com
dev.tesla.com
eua-origin.tesla.com
forums.tesla.com
imap.tesla.com
ir.tesla.com
lyncdiscover.tesla.com
model3.tesla.com
my.tesla.com
naa-origin.tesla.com
nas-origin.tesla.com
new.tesla.com
new-dev.tesla.com
partners.tesla.com
pop.tesla.com
powerwall.tesla.com
resources.tesla.com
shop.tesla.com
```

Resources and References

Resources and References

GITHUB DORKS	https://securitytrails.com/blog/github-dorks
GITROB	https://michenriksen.com/blog/gitrob-now-in-go/
NEWS	https://nakedsecurity.sophos.com/2019/03/25/thousands-of-coders-are-leaving-their-crown-jewels-exposed-on-github/
GITHUB BUG BOUNTY HUNTING	https://gist.github.com/EdOverflow/922549f610b258f459b219a32f92d10b
ASSETNOTE	https://blog.assetnote.io/bug-bounty/2019/04/23/getting-access-zendesk-gcp/