

# Git-Recon



# WHO I AM ?

Indian

Bugcrowd Top 100

Bug bounty hunter & trainer



# Your target & mind workflow

- Understanding codes and repo
- Checking view and laziness
- Date , Person, Authentication
- Luck



# On point !!!

## Basic Dorks

"site.com" password

"site.com" key=

"site.com" access token

"site.com" secret key

"site.com" st no

"site.com" uri=

--branch=

--username=

-Dmaven.javadoc.skip=

OGITHUB\_TOKEN=

--username=

FIREBASE\_KEY=

ENV\_KEY=

END\_USER\_USERNAME=

END\_USER\_Password=



**Wait !!! Need to verify it ?**

## ■ -What to check ?

- Who posted data
  - Guy from org
  - Interns & Dev

## ■ -Keys, Password, Data etc ?

- Not every key is issue
- Use curl for keys, Search API docs
- Password ! Access it bro...

# Example <3

The screenshot shows the Zomato API documentation page for the 'cities' endpoint. The page is titled 'Example <3' at the top. The left sidebar contains links for 'Introduction', 'API Credentials', and 'Documentations'. The main content area is divided into several sections:

- city\_ids**: A text input field containing '1'. To its right, a table specifies the parameter: 'comma separated city\_id values', 'query', 'string'.
- count**: A text input field containing '1'. To its right, a table specifies the parameter: 'number of max results to display', 'query', 'integer'.
- Response Messages**: A table with columns 'HTTP Status Code', 'Reason', 'Response Model', and 'Headers'. It shows a single row with '400' and 'Invalid input'.
- Try It Out!**: A green button next to a 'Hide Response' link.
- Curl**: A text area containing a curl command: `curl -X GET --header "Accept: application/json" --header "user-key: asfdsgdhsthjfgssjsyfjfsghfdgd" "https://developers.zomato.com/api/v2.1/ci`
- Request URL**: A text area containing the URL: `https://developers.zomato.com/api/v2.1/cities?q=1&lat=1&lon=1&city_ids=1&count=1`
- Response Body**: A text area containing a JSON response: 

```
{  "code": 403,  "status": "Forbidden",  "message": "Invalid API Key"}
```
- Response Code**: A section at the bottom of the main content area.

The bottom of the browser window shows the taskbar with the Windows logo, a search bar, and several application icons. The system tray on the right shows the date and time as '7:10 AM 9/25/2020' and the language as 'ENG IN'.



# GOOGLE

Search on google for main org  
repo of github

"ea" github

High chance  
to get valid in  
main

← → ↻ [github.com/search?q=org%3Aelectronicarts+DB\\_PW+%3D&type=code](https://github.com/search?q=org%3Aelectronicarts+DB_PW+%3D&type=code)

 org:electronicarts DB\_PW =  [Pull requests](#) [Issues](#) [Marketplace](#) [Explore](#)

Repositories 0

Code 2

Commits 0

Issues 0

Discussions 0 Beta

Packages 0

Marketplace 0

Topics 0

Wikis 0


Users 0

Languages

Python 2

[Advanced search](#) [Cheat sheet](#)


2 code results or view [all results on GitHub](#)

 electronicarts/ava-capture

[website-backend/ava/ava/dev\\_secure\\_settings.py](#)

```
2 # This is the sample secure file for DEV, for a PROD environment, this is replaced with
  file secure_settings.py
3
4 DB_PW = '3navet' # your DB password
5 SECRET_KEY = 's(=+g!q6lt+tuq4t@f_l+ha#z%h+)@3e%+n862h^1c1*_qhwrq' # DEV only, change for
```

Python Showing the top match Last indexed on May 2, 2019

 electronicarts/ava-capture

[website-backend/ava/ava/settings.py](#)

```
22 import dev_secure_settings as secure_settings
23
24 ''' secure_settings.py is not in source control. It contains:
25
26 DB_PW = 'databasepassword'
...
136 'USER': 'django',
137 'PASSWORD': secure_settings.DB_PW,
138 'HOST': 'localhost', # Or an IP Address that your DB is hosted on
```

Python Showing the top two matches Last indexed on May 2, 2019

# Happy ?? Wait wait wait !!

- Got information ,Reported
- Happy xD, Don't post tips instantly
  - You may disclose bug
  - People are here to ask
    - You cant ignore
- Verify, Craft report, Send them, Wait for patch





# Need of program ?

- Remote access
- Employee information
  - DB access
- No data related to customer
  - Intranet access
- Default URL of projects





# Bounty Rules

-Don't expect anything

If you did it in passion,  
you'll get dollars

-Constant Recon impotent

-Recon guy's are hero

## **VERIFY DATA**

Some data are intended, No bug here

## **REPORTED > INVALID**

Don't get angry, You may lose good bonds with program

## **YES THEY DO ACCEPT THIRD PARTY**

Your crafting and exploits are gold. Make it high as you can

## **BE HUMBLE WITH PROGRAM**

Money going no where. Don't message constant to team

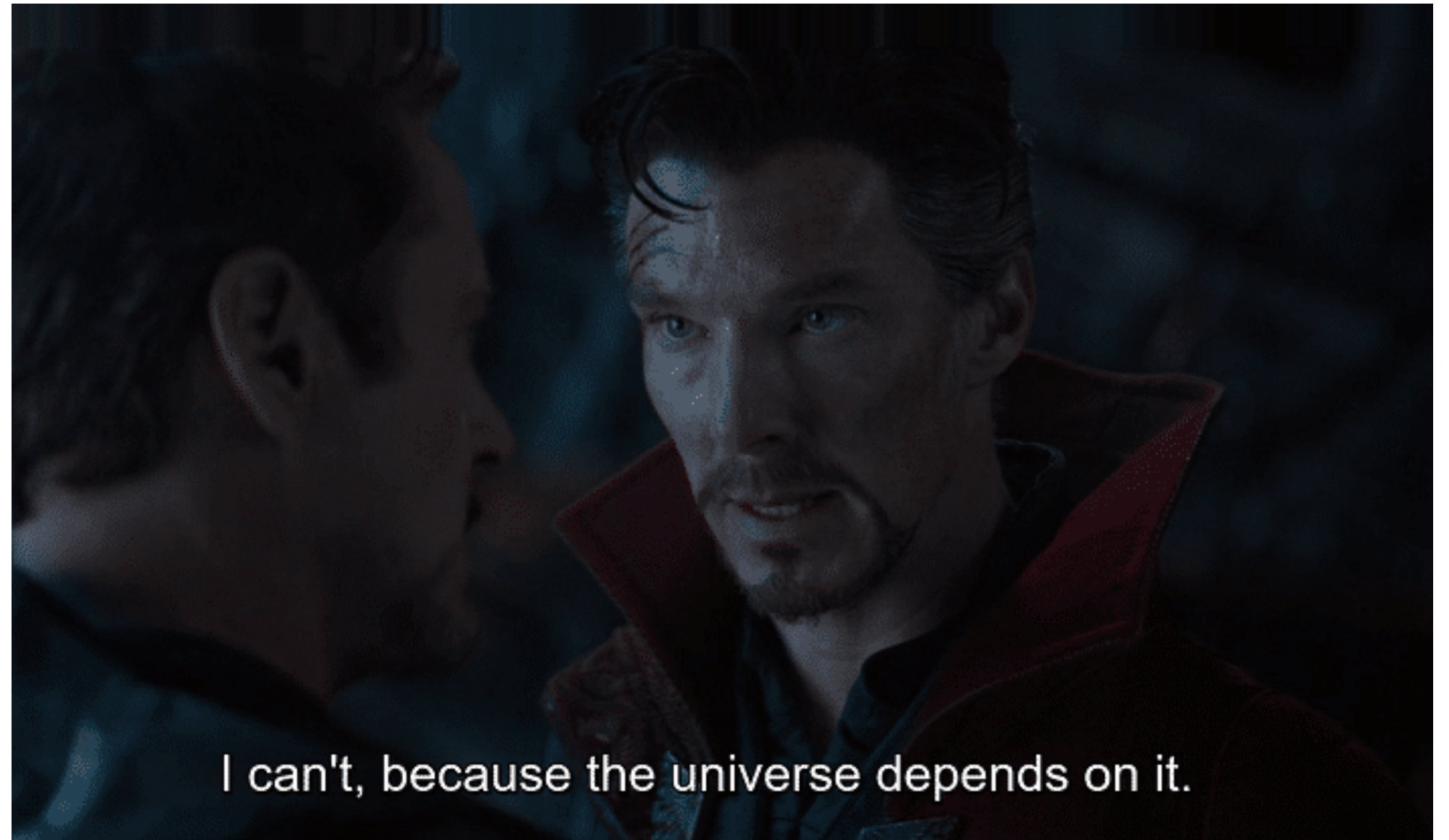
## **Final tips**





# Tools ???

- Gitrob
- GitHound
- Your mind



Note: I don't use tools, My all git recon is manual

**Thank  
you**

**WANTS TO  
FOLLOW ME ?**

**DORK IT  
BRUH...**

