GHOSTLULZ HACKS

Hack the planet

Blog

If you want to find vulnerabilities and make a money bug bounty hunting you may want to get a copy of my book. BUY NOW!

Github OSINT

Slack Group

Before we get started I have started a slack group dedicated to hacking. We welcome everyone from beginner to advanced to join. I will be on everyday answer questions, doing CTFs, and talking about cool hacks. If you enjoy hacking and are looking for like minded people join below:

NEW Hacking Group Slack Channel

Introduction

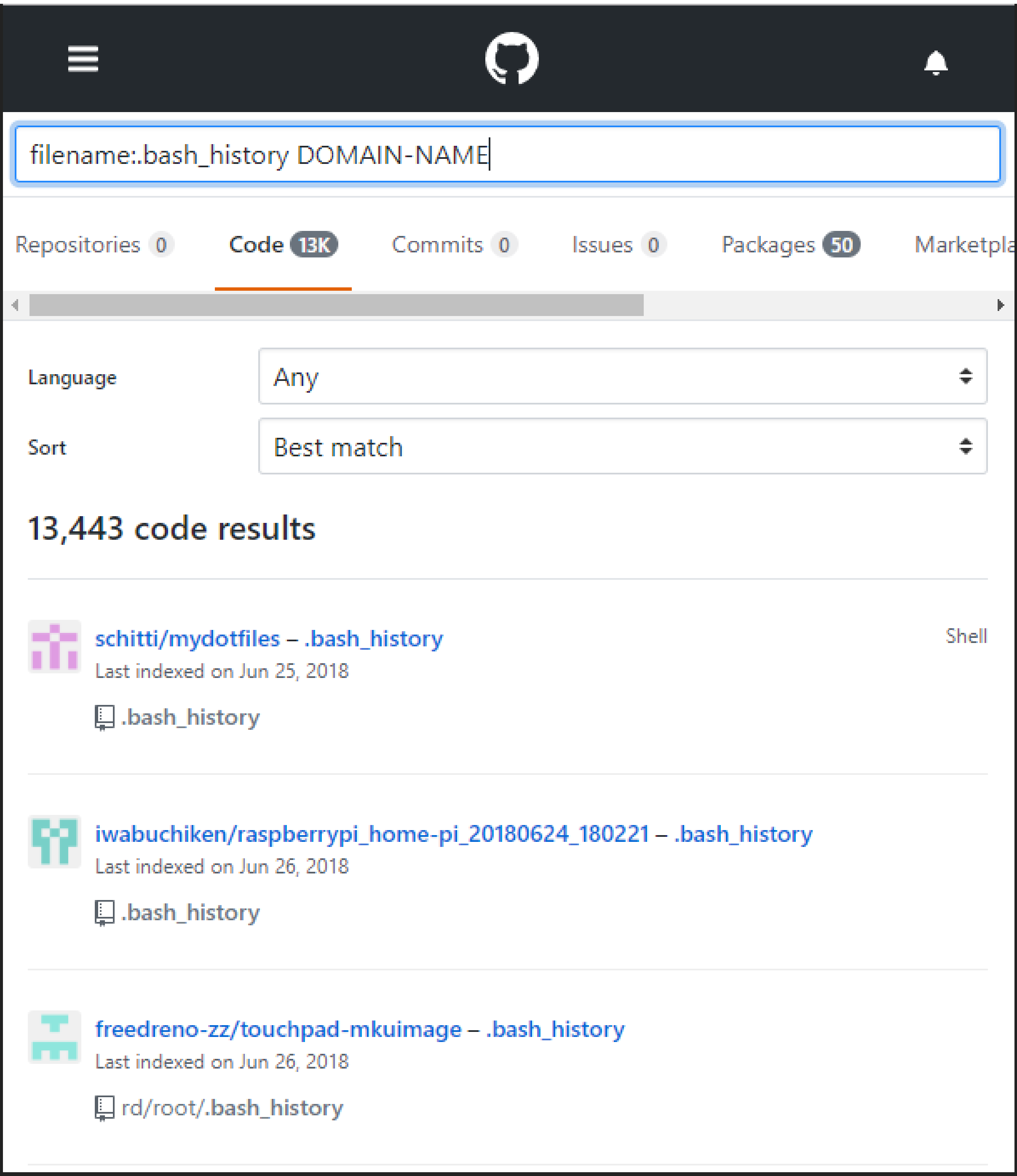
When performing your initial recon on an organization dont forget about Github. Github is used by developers to maintain and share their code, most of the time they end up sharing much more though. Most of the organizations I come across have a public Github which can contain a tun of use full information. I have personally popped boxes using only information gained from a github account. Depending on the size of the company you can literally spend a weeks just looking for exposures on Github.

Github Dorks

You probably know what google dorks are but what are Github dorks. Github dorks are basically the same thing as google dorks. A dork is used to find specific information in a sea of information. It helps us narrow down the search to exactly what we want. We can match on file extensions , file names, or a specific set or words. This can be very handy when searching for sensitive files, API keys, passwords, and a lot more.

We can use dorks to find sensitive files that developers might have accidentally uploaded. For instance one time I was performing an external pentest against company and I was able to use github dorks to find an exposed bash_history file which had ssh passwords. This was easily done by submitting the following dork:

filename:.bash_history DOMAIN-NAME



filename:.bash_history DOMAIN-NAME

Language: Any

Sort: Best match

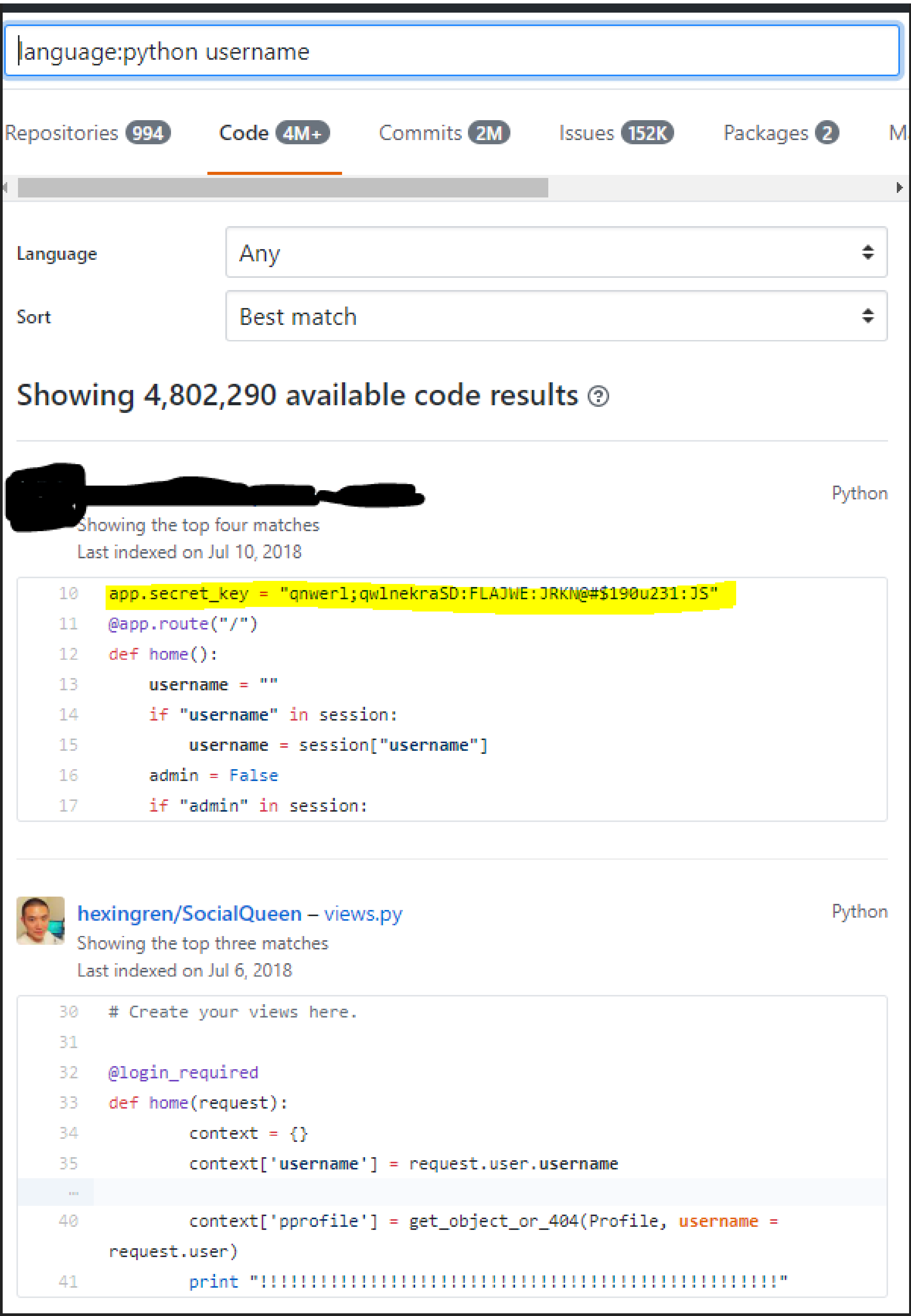
13,443 code results

schitti/mydotfiles – .bash_history — Shell
Last indexed on Jun 25, 2018
.bash_history

iwabuchiken/raspberrypi_home-pi_20180624_180221 – .bash_history
Last indexed on Jun 26, 2018
.bash_history

freedreno-zz/touchpad-mkuimage – .bash_history
Last indexed on Jun 26, 2018
rd/root/.bash_history

People are always uploading sensitive files to github, its a gold mine. Its also a good idea to look for exposed passwords, tokens, and api keys,usernames. Often I will search for these words followed by the company name as show below:



language:python username

Language: Any

Sort: Best match

Showing 4,802,290 available code results

[redacted]

Python

Showing the top four matches

Last indexed on Jul 10, 2018

```
app.secret_key = "qnwerl;qwlnekraSD:FLAJWE:JRKN@#$190u231:JS"
@app.route("/")
def home():
    username = ""
    if "username" in session:
        username = session["username"]
    admin = False
    if "admin" in session:
```

hexingren/SocialQueen – views.py

Python

Showing the top three matches

Last indexed on Jul 6, 2018

```
# Create your views here.

@login_required
def home(request):
        context = {}
        context['username'] = request.user.username
…
        context['pprofile'] = get_object_or_404(Profile, username =
request.user)
        print "!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!"
```

Usernames are often associated with passwords and api keys. As shown above someone is leaking their secrete key. If this was an engagement I would use that key to login to their application.

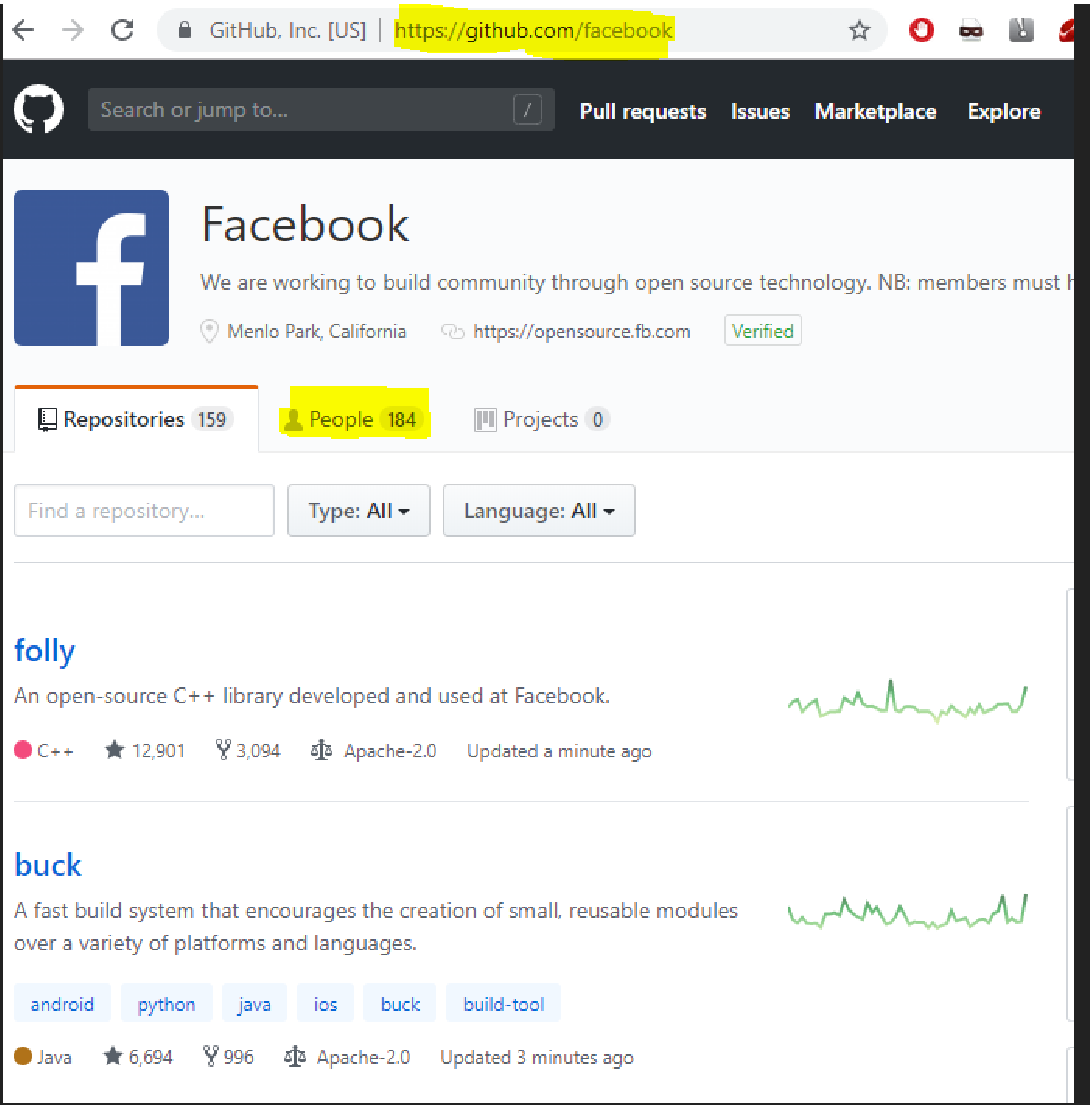
A good list of these dorks can be found below:**techgaun/github-dorks**

*Collection of github dorks and helper tool to automate the process of checking dorks – techgaun/github-dorks*github.com

Company Github

Instead of using Github dorks to find exposures you might want to go directly to the source. To do this you must find the companies Github page and from there you can locate all their developers and monitor their accounts.

Not all companies have a public github page but you can do a google search to find out.



Facebook

We are working to build community through open source technology. NB: members must h

Menlo Park, California https://opensource.fb.com Verified

folly

An open-source C++ library developed and used at Facebook.

● C++ ★ 12,901 3,094 Apache-2.0 Updated a minute ago

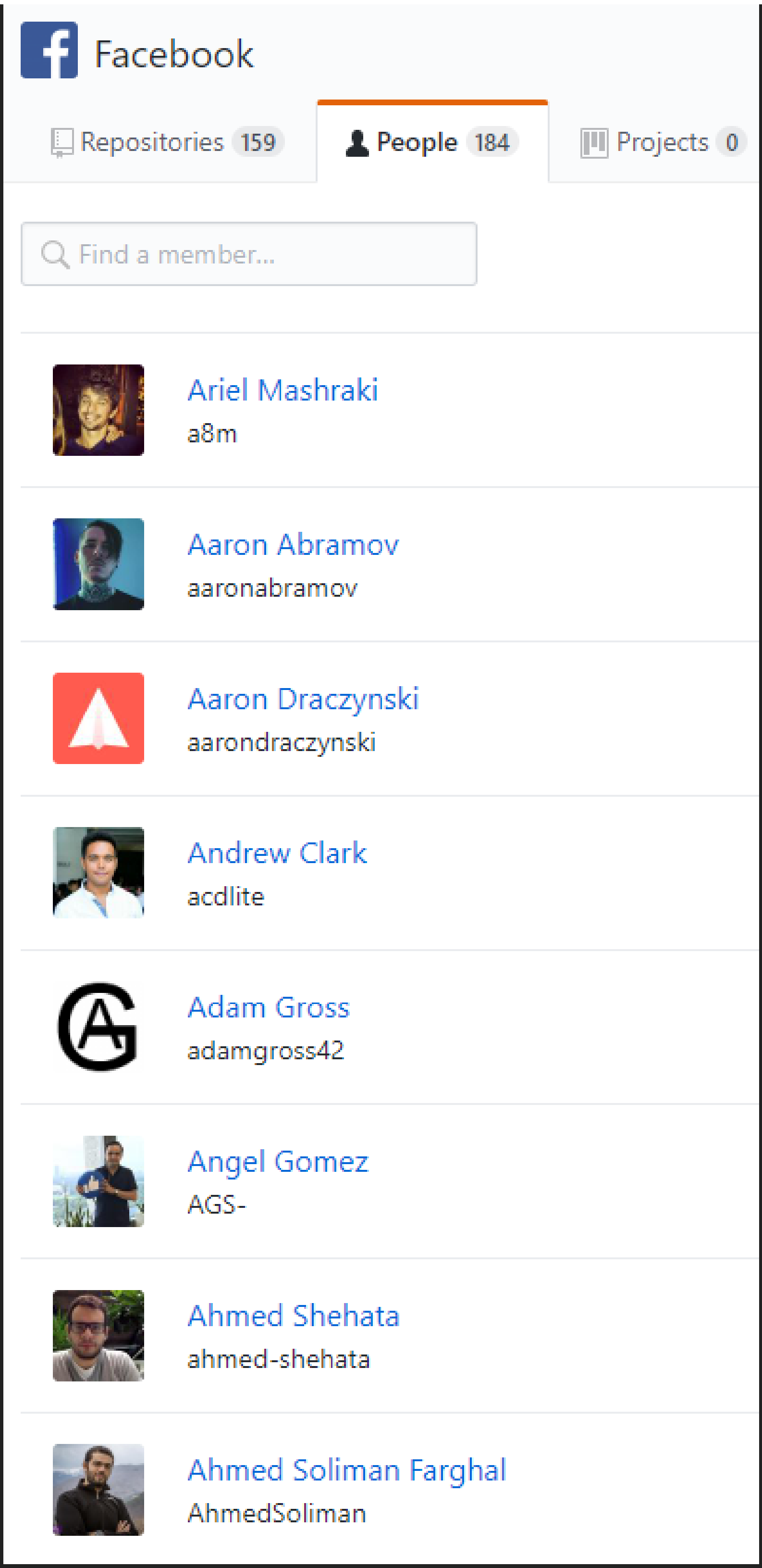
buck

A fast build system that encourages the creation of small, reusable modules over a variety of platforms and languages.

android python java ios buck build-tool

● Java ★ 6,694 996 Apache-2.0 Updated 3 minutes ago

Once you find a companies page you want to get a list of people that are associated with the company. This can be done by clicking on the “people” tab.



Facebook

Repositories 159 | People 184 | Projects 0

Find a member...

Ariel Mashraki
a8m

Aaron Abramov
aaronabramov

Aaron Draczynski
aarondraczynski

Andrew Clark
acdlite

Adam Gross
adamgross42

Angel Gomez
AGS-

Ahmed Shehata
ahmed-shehata

Ahmed Soliman Farghal
AhmedSoliman

Now you will need to manually go through each one and look for exposures. Thats why this process can take so long. Facebook has 184 people and looking through each one can be boring and take along time. However, if there are a lot of people then there is a greater chance someone uploaded something they shouldnt have. You should be looking for urls, api keys, usernames, passwords, vulnerabilities, and anything else that could provide value.

Conclusion

Github is a great source of information. The vast majority of companies now a days have a Github page. If you find this page you can monitor all of their employees for sensitive exposures. You can also use Github dorks to do a broad search across all of github. You should be looking for passwords, tokens, api keys, usernames, hidden urls, or any thing else that provides value. Github is a gold mine and you should be taking advantage of it during your recon phase. OSINT for the win!

← Vulnerable Javascript Files

Malware-Basic Windows Key logger

Your email address will not be published. Required fields are marked *

□

Post Comment

TWITTER

SLACK CHANNEL

GITHUB

Copyright © 2019 Ghostlulz Hacks — Velux WordPress theme by GoDaddy