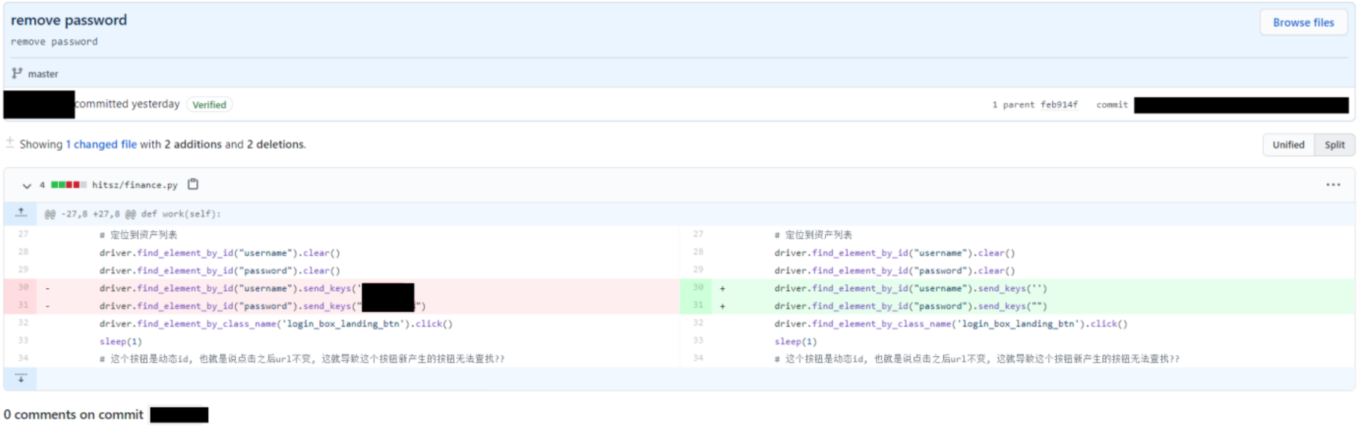
32

Now that you've moved onto a new site by crossing the forest trust boundary your team needs to perform initial reconnaissance again this time the osint and passive recon is up to you. Go through Throwback Hacks Security online presence and see what information you can gather about the company to move on to gaining access to the rest of their network.

Github, The Goldmine

Github often has tons of juicy information that is up for grabs at any given time. Sensitive data such as API Keys or valid Credentials are left in previous commits, which can be viewed by just about anyone. The example photo below was found at the time of writing by searching for "Removed Password" in Github and filtering by commits.



remove password

remove password

master

[redacted] committed yesterday Verified

1 parent feb914f commit [redacted]

Showing 1 changed file with 2 additions and 2 deletions.

4 hitsz/finance.py

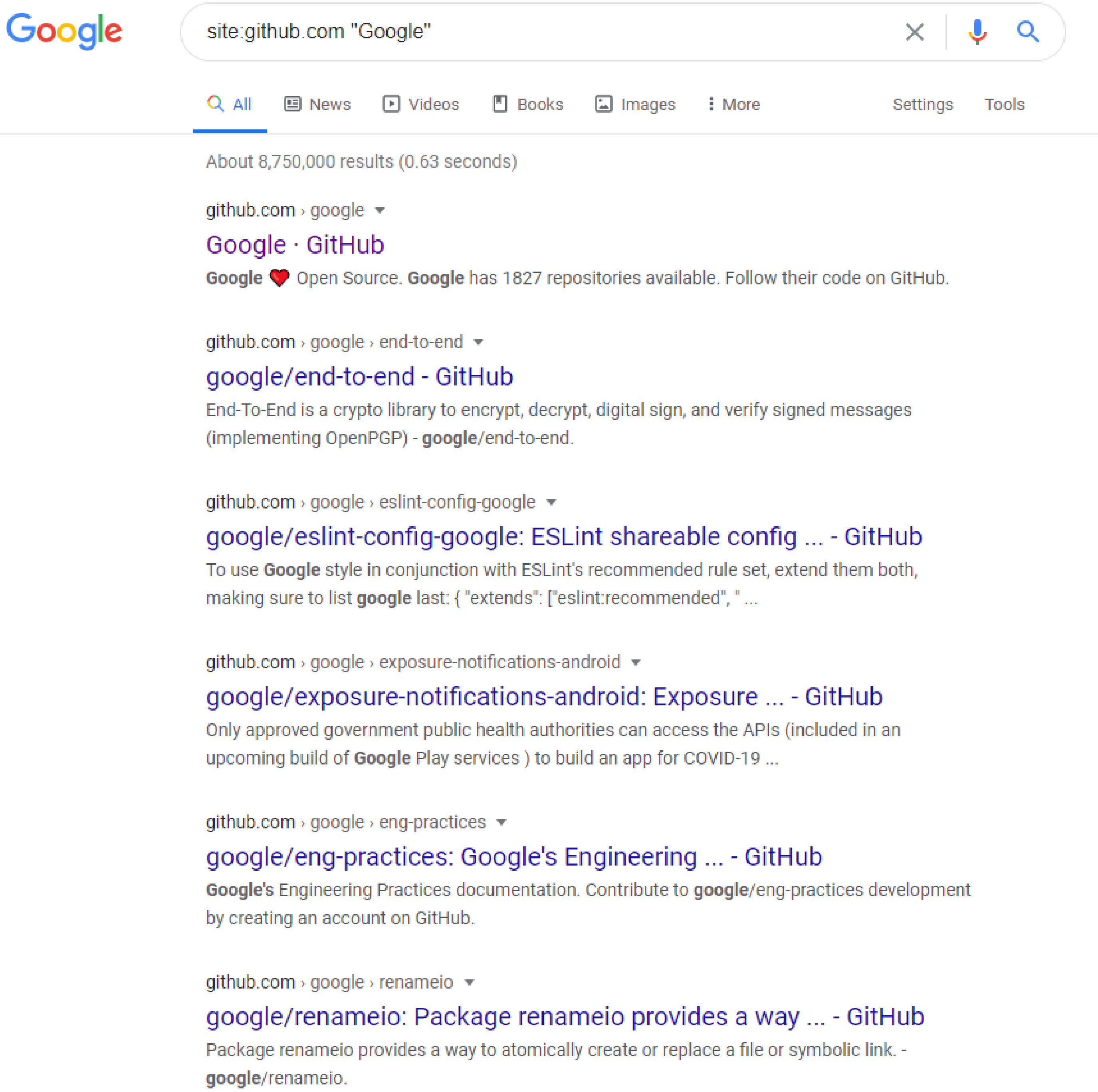
```
@@ -27,8 +27,8 @@ def work(self):
        # 定位到资产列表
        driver.find_element_by_id("username").clear()
        driver.find_element_by_id("password").clear()
-       driver.find_element_by_id("username").send_keys('[redacted]
-       driver.find_element_by_id("password").send_keys("")
        driver.find_element_by_class_name('login_box_landing_btn').click()
        sleep(1)
        # 这个按钮是动态id，也就是说点击之后url不变，这就导致这个按钮新产生的按钮无法查找??
```

```
        # 定位到资产列表
        driver.find_element_by_id("username").clear()
        driver.find_element_by_id("password").clear()
+       driver.find_element_by_id("username").send_keys('')
+       driver.find_element_by_id("password").send_keys("")
        driver.find_element_by_class_name('login_box_landing_btn').click()
        sleep(1)
        # 这个按钮是动态id，也就是说点击之后url不变，这就导致这个按钮新产生的按钮无法查找??
```

0 comments on commit [redacted]

A password recently removed during a new commit

Google Dorking can often lead to some great results that you may be able to use to find company Github repositories, employees or much more.


site:github.com "Google"

About 8,750,000 results (0.63 seconds)

github.com › google

Google · GitHub

Google ❤ Open Source. **Google** has 1827 repositories available. Follow their code on GitHub.

github.com › google › end-to-end

google/end-to-end - GitHub

End-To-End is a crypto library to encrypt, decrypt, digital sign, and verify signed messages (implementing OpenPGP) - **google**/end-to-end.

github.com › google › eslint-config-google

google/eslint-config-google: ESLint shareable config ... - GitHub

To use **Google** style in conjunction with ESLint's recommended rule set, extend them both, making sure to list **google** last: { "extends": ["eslint:recommended", " ...

github.com › google › exposure-notifications-android

google/exposure-notifications-android: Exposure ... - GitHub

Only approved government public health authorities can access the APIs (included in an upcoming build of **Google** Play services) to build an app for COVID-19 ...

github.com › google › eng-practices

google/eng-practices: Google's Engineering ... - GitHub

Google's Engineering Practices documentation. Contribute to **google**/eng-practices development by creating an account on GitHub.

github.com › google › renameio

google/renameio: Package renameio provides a way ... - GitHub

Package renameio provides a way to atomically create or replace a file or symbolic link. - **google**/renameio.

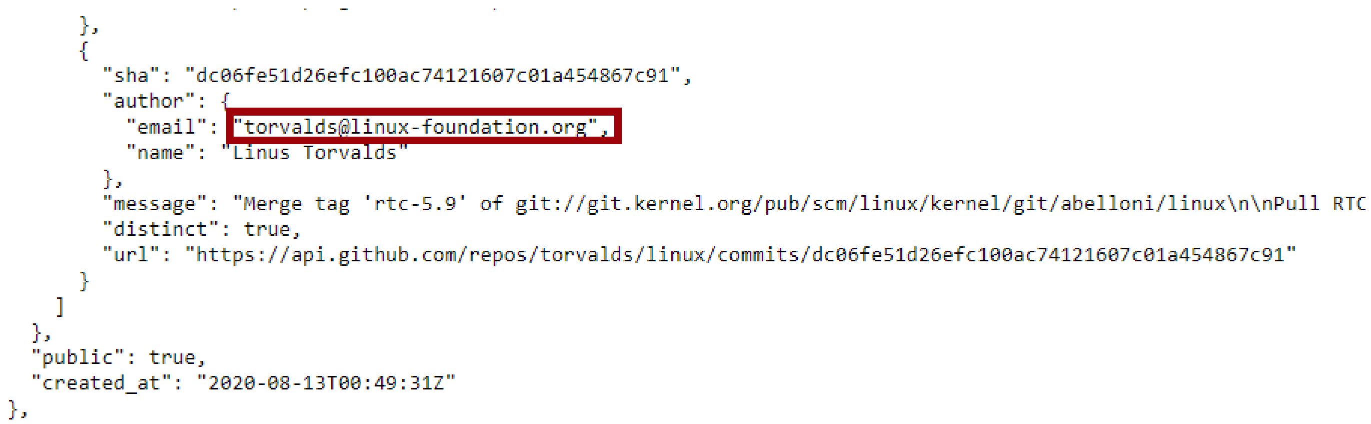
Google Dorking for Google's Github

API's and you!

Once you find the user you want to target, you may also want to investigate the Github API to see if you can't find any other sensitive information such as a company email address. You can check a users public events history by visiting the following URL.

https://api.github.com/users/USERGOESHERE/events/public

Below is a sample result of Linus Torvalds Github, where his email and name can be found. For OpSec purposes, having your email exposed on Github is less than ideal, and could directly lead to a phishing attack!



```
      },
      {
        "sha": "dc06fe51d26efc100ac74121607c01a454867c91",
        "author": {
          "email": "torvalds@linux-foundation.org",
          "name": "Linus Torvalds"
        },
        "message": "Merge tag 'rtc-5.9' of git://git.kernel.org/pub/scm/linux/kernel/git/abelloni/linux\n\nPull RTC
        "distinct": true,
        "url": "https://api.github.com/repos/torvalds/linux/commits/dc06fe51d26efc100ac74121607c01a454867c91"
      }
    ]
  },
  "public": true,
  "created_at": "2020-08-13T00:49:31Z"
},
```

Linux Torvald's email exposed by the Github API

Now that you know the fundamentals of gathering information from github utilize your new found resource to find data leaks from Throwback Hacks

Answer the questions below

What User has a Github Account?

Submit

What was the user found in github?

Submit

What password was found in github?

Submit

What machine can you access with the credentials?

Submit