FIELD NOTE / PYTHON

Mengorek Secuil Informasi Sensitif dari Github

Petruknisme · 25 Oct, 2019 · 4 min to read

GitHub merupakan layanan web hosting untuk git repositori. Kalau saya biasa menyebutnya sebagai social coding. Karena didalamnya terdapat banyak sekali software-software yang terbuat atas bantuan dari para penggiat Open Source. Dari mulai project berbasis Web sampai project berbasis mesin ada.

Pada proses *commit* dan *push* code ke GitHub, kadang kita melakukan kecerobohan atau mungkin keteledoran. Apa itu? Ya, informasi sensitif yang kita tinggalkan. Informasi tersebut bisa berupa banyak hal, mungkin bisa berupa password, akun, atau kredensial informasi lainnya yang dimana bisa menjadikan abuse atau penyalahgunaan.

Pada pembahasan kali ini, kita akan memanfaatkan kecerobohan dan keteledoran yang dilakukan. Kita akan menggunakan **Gitrob**??sebagai alat untuk melakukan uji coba dan pencarian informasi sensitif yang berada pada repo publik. Sebelum memulai, saya perlu ingatkan bahwa apa yang akan dilakukan hanya untuk pelajaran dan Do with your own risk :p

Jadi apa itu Gitrob?

Gitrob merupakan sebuah CLI tool yang ditujukan kepada organisasi atau security professional untuk melakukan pencarian informasi sensitif yang terdapat pada berkas yang tersedia dalam publik repositori. Gitrob ini akan melakukan keseluruhan pencarian terhadap suatu repositori yang terdapat dalam organisasi ataupun repositori pada setiap member organisasi yang bersifat publik repositori dan melakukan pencocokan dengan pattern Gitrob yang sudah dikategorikan termasuk kedalam informasi sensitif.

Sebelum melakukan instalasi terhadap Gitrob, ada beberapa hal yang harus diperhatikan.

Requirements

- Ruby 1.9.3+
- RubyGems
- PostgreSQL
- GitHub Access Tokens

Install Ruby & Rubygems

Karena Gitrob ini ditulis dalam bahasa Ruby, pastikan kamu sudah memasang Ruby pada mesin yang akan dipakai. Kalau belum, lakukan pemasangan terlebih dahulu seperti yang ada pada halaman berikut https://www.ruby-lang.org/en/documentation/installation/ (https://www.ruby-lang.org/en/documentation/installation/) . Untuk memastikan versi Ruby mana yang sedang berjalan, lakukan _ruby –version??_untuk melakukan cek versi. Pastikan versi Ruby yang terpasang adalah 1.9.3 atau diatasnya.

Licensed under CC BY-SA 4.0

Gitrob pun dipaketkan sebagai Ruby gem untuk memudahkan proses pemasangan atau pembaruan. Kalau di ArchLinux ketika melakukan pemasangan ruby sudah disertakan juga rubygems. Tapi kalau kurang yakin, cek saja dengan menggunakan *gem -v*. Setelahnya, kita lakukan pembaruan terhadap paket ruby yang terpasang dengan melakukan perintah:

```
[me@Chernobyl ~]$ gem update --system
Updating rubygems-update
Fetching: rubygems-update-2.6.8.gem (100%)
Successfully installed rubygems-update-2.6.8
Parsing documentation for rubygems-update-2.6.8
Installing ri documentation for rubygems-update-2.6.8
Installing darkfish documentation for rubygems-update-2.6.8
Done installing documentation for rubygems-update after 28 seconds
Parsing documentation for rubygems-update-2.6.8
Done installing documentation for rubygems-update after 0 seconds
Installing RubyGems 2.6.8
RubyGems 2.6.8 installed
Parsing documentation for rubygems-2.6.8
Installing ri documentation for rubygems-2.6.8
```

Bila dua langkah diatas sudah selesai dan berjalan dengan lancar, maka kita lanjutkan ke langkah selanjutnya.

Mempersiapkan Database

Gitrob menggunakan PostgreSQL sebagai database untuk melakukan penyimpanan keseluruhan data yang sudah didapatkan. Berikut daftar panduan pemasangan PostgreSQL sesuai distro yang digunakan:

```
Arch Linux - https://wiki.archlinux.org/index.php/PostgreSQL#Installing_Po
Ubuntu - https://www.digitalocean.com/community/tutorials/how-to-install-a
Debian - https://www.digitalocean.com/community/tutorials/how-to-install-a
OpenSuse - https://www.howtoforge.com/tutorial/how-to-install-postgresql-a
Fedora - https://www.liquidweb.com/kb/how-to-install-and-connect-to-postgr
```

Gitrob juga membutuhkan dependensi PostgreSQL. Lakukan pemasangan untuk paket berikut juga:

Licensed under CC BY-SA 4.0

```
Ubuntu/Debian - libpq-dev
Arch Linux - postgresql-libs
Fedora - postgresql-libs
```

Setelah selesai pada tahap pemasangan database, pastikan bahwa service postgresql sudah berjalan. Selanjutnya kita perlu mengatur user dan database yang akan dipakai untuk Gitrob dengan perintah berikut:

```
sudo su postgres # Not necessary on Mac OS X
createuser -s gitrob --pwprompt
createdb -O gitrob gitrob
exit
```

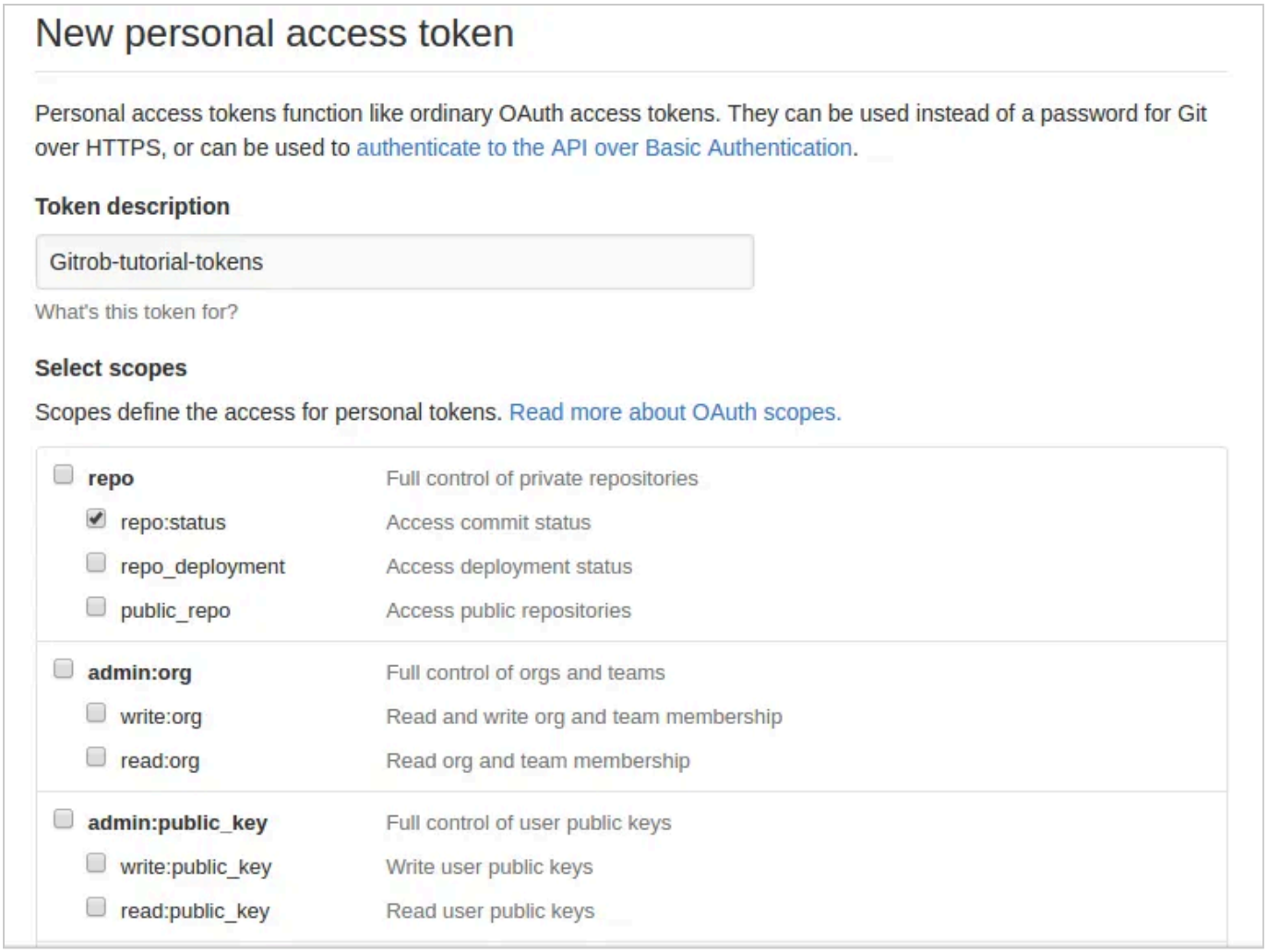
Nah, sekarang kita sudah memiliki database dengan nama *gitrob*??serta user *gitrob*??dan password sesuai dengan yang sudah kita masukkan sebelumnya. Kita pun sudah memberikan hak akses kepada user gitrob terhadap database gitrob.

Github Access Tokens

Gitrob ini bekerja dengan cara melakukan query terhadap Github API untuk mendapatkan data, jadi kita membutuhkan access token untuk menjalankan aplikasi ini agar terhindar dari rate limit saat melakukan query terhadap API. Untuk membuat token nya sangat mudah, cukup ke halaman https://github.com/settings/tokens (https://github.com/settings/tokens) dan klik Generate New Token, pastikan kamu sudah memiliki akun GitHub dan sedang dalam keadaan login.

Karena kita hanya akan melakukan scanning terhadap public repo, jadi kita tidak perlu memberikan akses apapun terhadap tokens yang akan kita buat ini. Disini saya akan menamai dengan seperti gambar berikut:

Licensed under CC BY-SA 4.0



Klik Generate Token, dan kita akan disuguhkan dengan peringatan *Make sure to copy your new personal access token now. You won't be able to see it again!*. Nah, simpan baik-baik token yang diberikan, karena itu yang akan kita gunakan nantinya. Maka akan muncul token baru seperti berikut :

```
1 | Gitrob-tutorial-tokens ??? public access
```

Ok, token sudah kita dapatkan. Lanjut ke langkah pemasangan Gitrob itu sendiri.

Pemasangan Gitrob

Setelah semua proses sebelumnya selesai. Sekarang saatnya kita melakukan pemasangan terhadap Gitrob.

```
1 | [me@Chernobyl ~]$ gem install gitrob
2 | Fetching: highline-1.7.8.gem (100%)
3 | Successfully installed highline-1.7.8
```

Licensed under CC BY-SA 4.0

```
Fetching: thread-0.2.2.gem (100%)
Successfully installed thread-0.2.2
Fetching: ruby-progressbar-1.8.1.gem (100%)
Successfully installed ruby-progressbar-1.8.1
Fetching: pg-0.19.0.gem (100%)
Building native extensions.  This could take a while...
Successfully installed pg-0.19.0
Fetching: sequel-4.40.0.gem (100%)
Successfully installed sequel-4.40.0
Fetching: github_api-0.14.5.gem (100%)
Successfully installed github_api-0.14.5
Fetching: sucker_punch-2.0.2.gem (100%)
Sucker Punch v2.0 introduces backwards-incompatible changes.
Please see https://github.com/brandonhilkert/sucker_punch/blob/master/CHAN
Successfully installed sucker_punch-2.0.2
Fetching: gitrob-1.1.0.gem (100%)
Successfully installed gitrob-1.1.0
Parsing documentation for highline-1.7.8
Installing ri documentation for highline-1.7.8
Parsing documentation for thread-0.2.2
Installing ri documentation for thread-0.2.2
Parsing documentation for ruby-progressbar-1.8.1
Installing ri documentation for ruby-progressbar-1.8.1
Parsing documentation for pg-0.19.0
Installing ri documentation for pg-0.19.0
Parsing documentation for sequel-4.40.0
Installing ri documentation for sequel-4.40.0
Parsing documentation for github_api-0.14.5
Installing ri documentation for github_api-0.14.5
Parsing documentation for sucker_punch-2.0.2
Installing ri documentation for sucker_punch-2.0.2
Parsing documentation for gitrob-1.1.0
Installing ri documentation for gitrob-1.1.0
Done installing documentation for highline, thread, ruby-progressbar, pg,
8 gems installed
```

Yey! kita sudah berhasil melakukan pemasangan Gitrob. Lakukan perintah *gitrob -h* untuk mengetahui apa saja help yang tersedia. Bagi yang menggunakan versi terbaru dari paket ***github_api-0.14.5*** dan mendapatkan pesan error seperti berikut saat menjalankan Gitrob:

Licensed under CC BY-SA 4.0

```
/home/me/.rvm/gems/ruby-2.3.1/gems/github_api-0.14.5/lib/github_api/api.rb
from /home/me/.rvm/gems/ruby-2.3.1/gems/github_api-0.14.5/lib/github_api/c
from /home/me/.rvm/gems/ruby-2.3.1/gems/github_api-0.14.5/lib/github_api/c
from /home/me/.rvm/gems/ruby-2.3.1/gems/github_api-0.14.5/lib/github_api/c
from /home/me/.rvm/rubies/ruby-2.3.1/lib/ruby/2.3.0/rubygems/core_ext/kern
from /home/me/.rvm/rubies/ruby-2.3.1/lib/ruby/2.3.0/rubygems/core_ext/kern
from /home/me/.rvm/gems/ruby-2.3.1/gems/github_api-0.14.5/lib/github_api.r
from /home/me/.rvm/gems/ruby-2.3.1/gems/github_api-0.14.5/lib/github_api.r
from /home/me/.rvm/gems/ruby-2.3.1/gems/github_api-0.14.5/lib/github_api.r
from /home/me/.rvm/gems/ruby-2.3.1/gems/github_api-0.14.5/lib/github_api.r
from /home/me/.rvm/gems/ruby-2.3.1/gems/github_api-0.14.5/lib/github_api.r
from /home/me/.rvm/rubies/ruby-2.3.1/lib/ruby/2.3.0/rubygems/core_ext/kern
from /home/me/.rvm/rubies/ruby-2.3.1/lib/ruby/2.3.0/rubygems/core_ext/kern
from /home/me/.rvm/gems/ruby-2.3.1/gems/gitrob-1.1.0/lib/gitrob.rb:9:in `<
from /home/me/.rvm/rubies/ruby-2.3.1/lib/ruby/2.3.0/rubygems/core_ext/kern
from /home/me/.rvm/rubies/ruby-2.3.1/lib/ruby/2.3.0/rubygems/core_ext/kern
from /home/me/.rvm/gems/ruby-2.3.1/gems/gitrob-1.1.0/exe/gitrob:3:in `<top
from /home/me/.rvm/gems/ruby-2.3.1/bin/gitrob:23:in `load'
from /home/me/.rvm/gems/ruby-2.3.1/bin/gitrob:23:in `<main>'
from /home/me/.rvm/gems/ruby-2.3.1/bin/ruby_executable_hooks:15:in `eval'
from /home/me/.rvm/gems/ruby-2.3.1/bin/ruby_executable_hooks:15:in `<main>
```

Maka cukup lakukan perubahan terhadap berkas *client.rb* yaitu dengan cara melakukan comment pada bagian ***namespace :say*** seperti berikut:

client.rb

```
[me@Chernobyl ~]$ cat ~/.rvm/gems/ruby-2.3.1/gems/github_api-0.14.5/lib/gi
# encoding: utf-8

module Github
  class Client < API
    require_all 'github_api/client',
                'activity',
                'authorizations',
                'emojis',
                'gists',
                'gitignore',
                'git_data',
                'issues',
```

Licensed under CC BY-SA 4.0

```
14                  'markdown',
15                  'meta',
16                  'orgs',
17                  'pull_requests',
18                  'repos',
19                  'say',
20                  'scopes',
21                  'search',
22                  'users'
23
24      # Serving up the 'social' in Social Coding, the Activity APIs
25      # provide access to notifications, subscriptions, and timelines.
26      namespace :activity
27
28      namespace :emojis
29
30      namespace :gists
31
32      namespace :gitignore
33      alias :git_ignore :gitignore
34
35      # The Git Database API gives you access to read and write raw Git obje
36      # to your Git database on GitHub and to list and update your reference
37      # (branch heads and tags).
38      namespace :git_data
39      alias :git :git_data
40
41      namespace :issues
42
43      namespace :markdown
44
45      namespace :meta
46
47      # An API for users to manage their own tokens. You can only access you
48      # tokens, and only through Basic Authentication.
49      namespace :authorizations
50      alias :oauth :authorizations
51      alias :auth :authorizations
52
53      namespace :orgs
54      alias :organizations :orgs
55
```

Licensed under CC BY-SA 4.0

```
56      namespace :pull_requests
57      alias :pulls :pull_requests
58
59      namespace :repos
60      alias :repositories :repos
61
62      #namespace :say
63      alias :octocat :say
64
65      namespace :scopes
66
67      namespace :search
68
69      # Many of the resources on the users API provide a shortcut for gettin
70      # information about the currently authenticated user.
71      namespace :users
72    end # Client
73  end # Github
```

Kalau sudah selesai, tahap selanjutnya adalah melakukan konfigurasi terhadap Gitrob itu sendiri:

```
1  gitrob configure
```


Informasi yang kita masukkan pada configuration wizard akan tersimpan di *~/.gitrobrc* . Ok, Gitrob sudah terpasang dan terkonfigurasi, saatnya kita jalankan Gitrob.

```
1  [me@Chernobyl ~]$ gitrob -h
2       _ _           _
3   ___|_| |_ ___ ___| |_
4  | . | |  _|  _| . | . |
5  |_  |_|_| |_| |___|___|
6  |___| By @michenriksen
7
```

Licensed under CC BY-SA 4.0

```
[*] Starting Gitrob version 1.1.0 at 2016-11-16 08:43 WIB
[*] Loading configuration... done
[*] Preparing database... done
Gitrob commands:
  gitrob analyze TARGETS  # Analyze one or more organizations or users
  gitrob configure        # Start configuration wizard
  gitrob help [COMMAND]   # Describe available commands or one specific co
  gitrob server           # Start web server

Options:
  [--bind-address=ADDRESS]   # Address to bind web server to
                             # Default: 127.0.0.1
  [--port=N]                 # Port to run web server on
                             # Default: 9393
  [--access-tokens=TOKENS]   # Comma-separated list of GitHub API tokens t
  [--color], [--no-color]    # Colorize or don't colorize output
                             # Default: true
  [--banner], [--no-banner]  # Show or don't show Gitrob banner
                             # Default: true
  [--debug], [--no-debug]    # Show or don't show debugging information
```

Kita dapat melakukan analyze terhadap single user GitHub ataupun Organization dengan perintah:

```
gitrob analyze username
```

Pada kasus ini, kita akan melakukan pencarian terhadap organisasi yang dimana saya sudah mendapatkan ijin untuk dijadikan sebagai target pada pembahasan kali ini.

```
[me@Chernobyl ~]$ gitrob analyze rndc
      _ _           _
 ___|_| |_ ___ ___| |_
| . | |  _|  _| . | . |
|_  |_|_| |_| |___|___|
|___| By @michenriksen

[*] Starting Gitrob version 1.1.0 at 2016-11-16 09:15 WIB
```

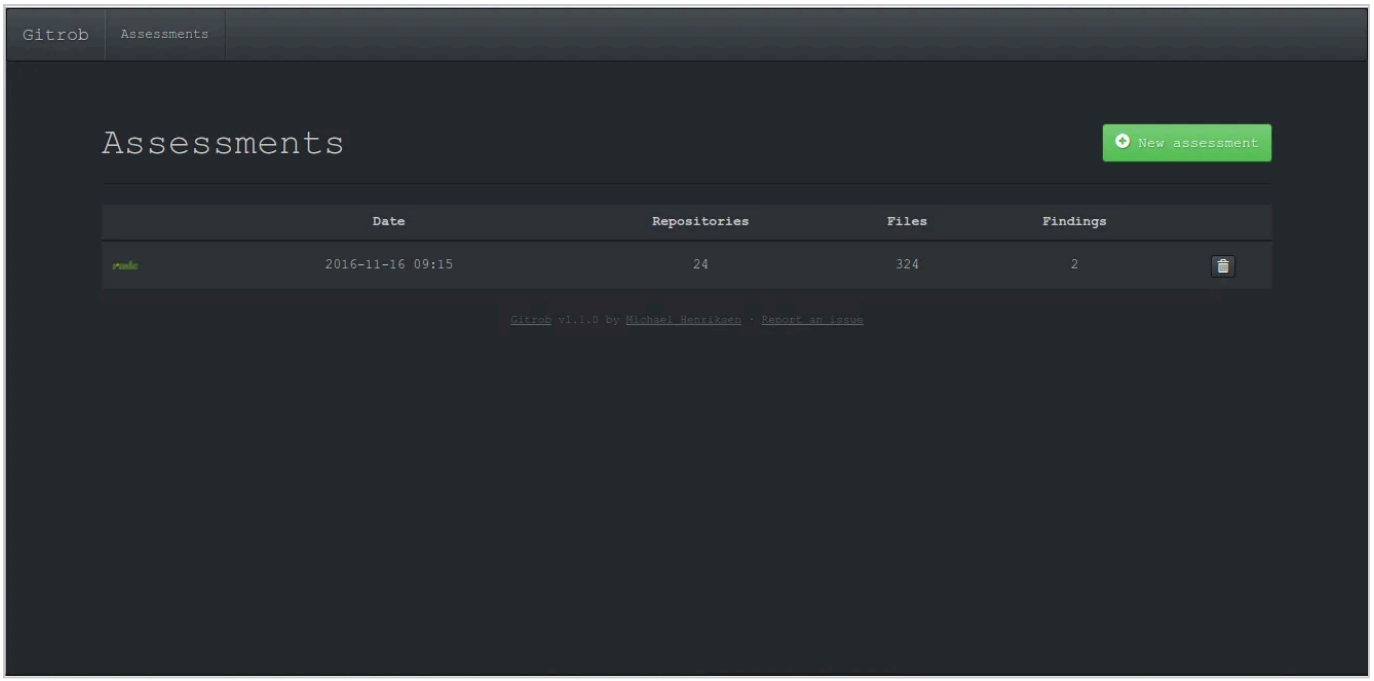
```
[*] Loading configuration... done
[*] Preparing database... done
[*] Loading signatures... done
[*] Loaded 79 signatures
[*] Gathering targets... done
[*] Gathering repositories from 1 targets...
[*] Progress 1/1 ||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||
[+] Gathered 24 repositories from rndc
[*] Gathered 24 repositories
[*] Analyzing repositories...
[+] Flagged 1 file in rndc/mfd
[+] Flagged 1 file in rndc/network-exercise
[*] Progress 24/24 ||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||
[*] Starting web application on port 9393...
[*] Browse to http://127.0.0.1:9393/ to see results!
== Sinatra (v1.4.7) has taken the stage on 9393 for production with backup
Thin web server (v1.6.4 codename Gob Bluth)
Maximum connections set to 1024
Listening on 127.0.0.1:9393, CTRL+C to stop
```

Secara default, saat melakukan analyze akan menjalankan pula web server, jadi kita tidak perlu menjalankan web server lagi. Dari hasil yang kita peroleh bahwa ada 2 berkas yang mengandung informasi sensitif dari 2 repositori.

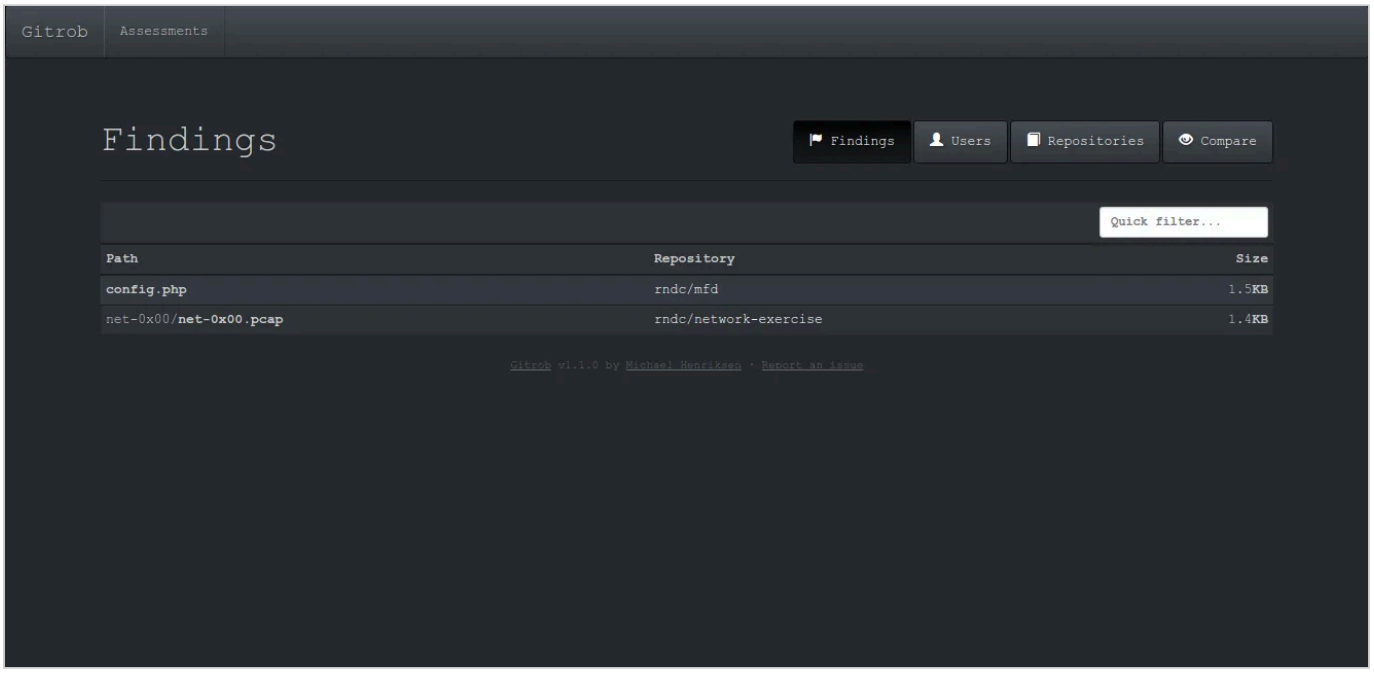
```
[+] Flagged 1 file in rndc/mfd
[+] Flagged 1 file in rndc/network-exercise
```

Buka laman **http://127.0.0.1:9393/** (http://127.0.0.1:9393/) untuk melihat hasil dari yang sudah kita dapatkan. Maka akan terlihat seperti berikut:

Licensed under CC BY-SA 4.0

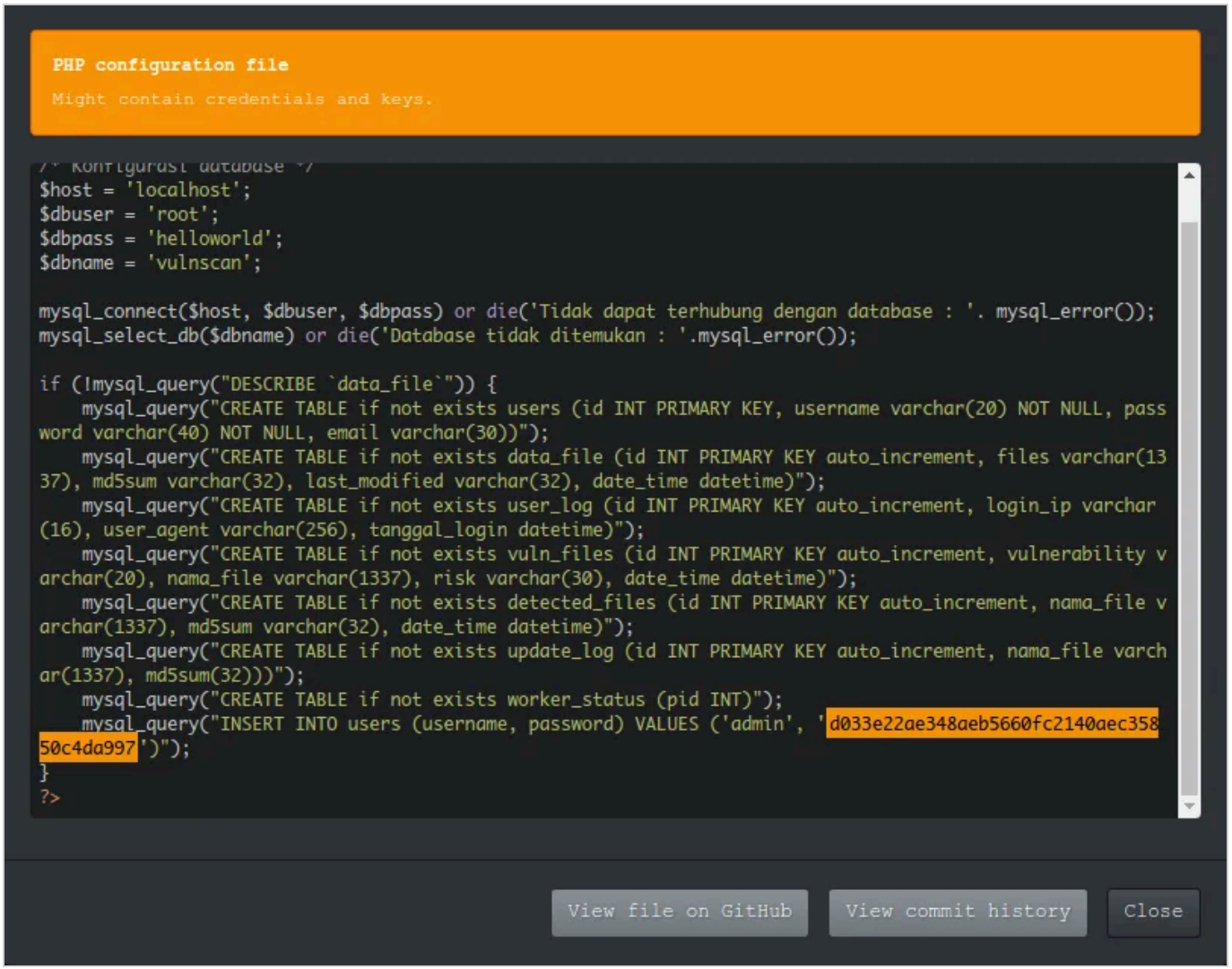


Klik pada Organization/User untuk melihat informasi lebih lengkap. Maka, akan muncul beberapa berkas dan repositori yang diidentifikasikan mengandung informasi sensitif.



Bila kita klik salah satu, maka akan menampilkan bagian mana yang dianggap sebagai informasi sensitif oleh Gitrob:

Licensed under CC BY-SA 4.0



Hore! kita sudah memasuki akhir dari pembahasan tentang Gitrob ini. Ingat, artikel ini tidak ditujukan untuk tujuan selain sebagai bahan pembelajaran. Baiknya bila kita menemukan informasi sensitif langsung dilaporkan ke pihak yang terkait. Semoga artikel ini bermanfaat.

Python # OSINT # Security # Tutorial

Licensed under CC BY-SA 4.0