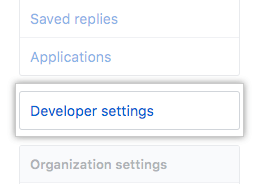
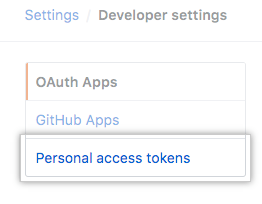
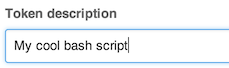
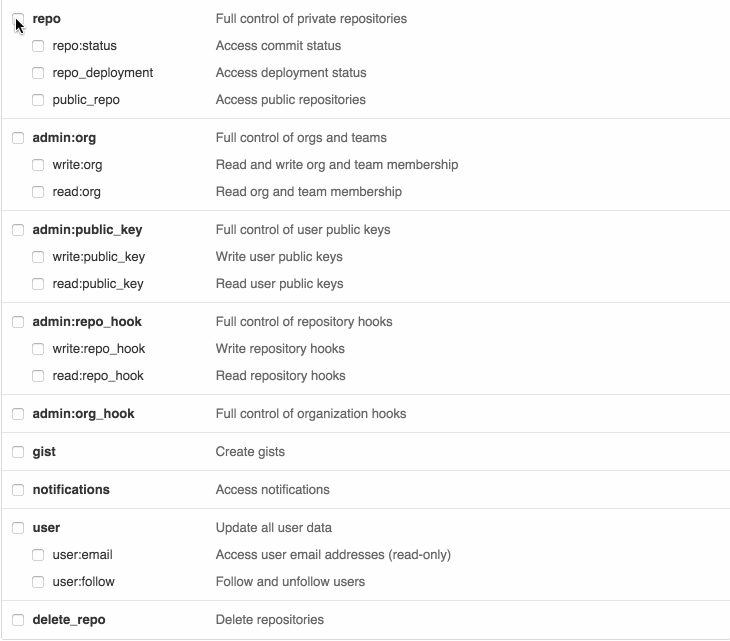
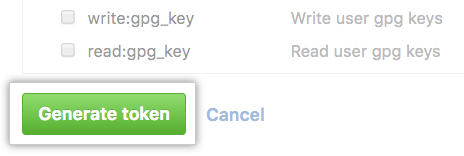
**Github Audit application:**

Please note this script was originally made by [kencochrane](http://docker.atlassian.net/wiki/pages/resumedraft.action?draftId=476808126&draftShareId=e92efd38-f92d-4d68-823e-ce106c2d0bfc), if you have any questions or trouble running the script please reach out to [Olivier Gambier](http://docker.atlassian.net/wiki/display/~dmp42).

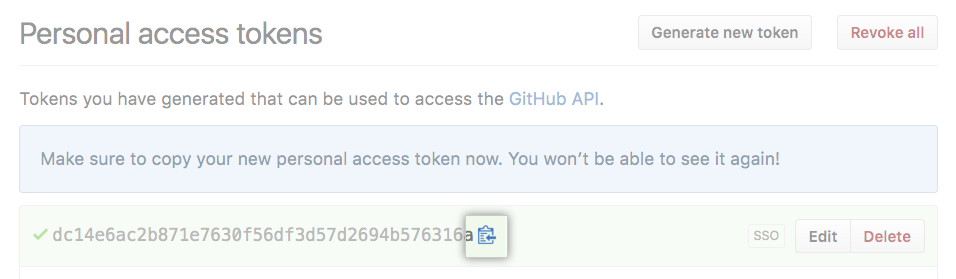
**GitHub token:**

1. In the upper-right corner of any page, click your profile photo, then click **Settings**.
2. In the left sidebar, click **Developer settings**.
   * 
3. In the left sidebar, click **Personal access tokens**.
   * 
4. Click **Generate new token**.
   * 
5. Give your token a descriptive name.
   * 
6. Select the scopes, or permissions, you'd like to grant this token. To use your token to access repositories from the command line, select **repo**.
   * 
7. Click **Generate token**.
   * 

|  |
| --- |
| When creating your github token, you need the following scopes   * + - repo (full control of private repos)     - repo:public\_repo (access public repos)     - read:org (Read org and team membership)     - user:email (Access user email addresses (read-only)) |

1. Click  to copy the token to your clipboard. For security reasons, after you navigate off the page, you will not be able to see the token again.

**Warning:** Treat your tokens like passwords and keep them secret. When working with the API, use tokens as environment variables instead of hardcoding them into your programs.

* + 

1. To use your token to authenticate to an organization that uses SAML SSO, [authorize the token for use with a SAML single-sign-on organization](https://help.github.com/articles/authorizing-a-personal-access-token-for-use-with-a-saml-single-sign-on-organization).

**Downloading the script:**

* [Python Audit script](http://docker.atlassian.net/wiki/download/attachments/476808126/audit.py?version=1&modificationDate=1534970232628&cacheVersion=1&api=v2)
  + This script is the main python script, this is the only script your need to run in command after you've finished running the requirements file.
  + It holds the api url for github and connects your github token to website then displays the information within command line.
* [Requirements pip download](http://docker.atlassian.net/wiki/download/attachments/476808126/requirements.txt?version=1&modificationDate=1534970233218&cacheVersion=1&api=v2)
  + This Script will download all the packages from python needed to run the audit script.
  + You will only need to use this once.
* [Python Utils script](http://docker.atlassian.net/wiki/download/attachments/476808126/utils.py?version=1&modificationDate=1534970233776&cacheVersion=1&api=v2)
  + This Script is used to set Bots to be skipped from the being checked for 2fa and name, as well as configure your Github Token to access the Github and pull in the data.

**Using command line:**

1. Open Terminal
2. $ cd Downloads
3. Type in GITHUB\_TOKEN=<your github token> ./audit.py <script commands>
4. To see all the script commands enter [options] as the <script commands>

**Running from source:**

1. You will need to download [python 2.7.15](https://www.python.org/downloads/release/python-2715/)
   * Preferably the [macOS 64-bit installer](https://www.python.org/ftp/python/2.7.15/python-2.7.15-macosx10.9.pkg) version
2. Make sure you have an ENV variable called GITHUB\_TOKEN with your github API token.
3. $ cd Downloads
4. $ pip install -r requirements.txt
5. $ GITHUB\_TOKEN=<your github token> ./audit.py audit
6. Lookup owners for the docker org
7. $ GITHUB\_TOKEN=<your github token> ./audit.py owners
8. Lookup the collaborators for a given repo under dockers org
9. $ GITHUB\_TOKEN=<your github token> ./audit.py repo\_collaborators --reponame docker
10. Lookup who doesn't have 2factor auth enabled.
11. $ GITHUB\_TOKEN=<your github token> ./audit.py twofactorauth
12. Lookup the members within Github
13. GITHUB\_TOKEN=<your github token> ./audit.py members