keybar Documentation

Release 0.1.0

keybar

March 26, 2016

Warning: Keybar is under heavy development. Please don’t use it.

Keybar is a framework, service and client for secure password storage and exchange.

This project aims to implement a safe, open and easy to use password store. Basically it’ll be a simple web-application that exposes it’s functionality via a simple REST-Api.

It’ll be extensible and easily deployable. With that in mind it’ll be easy to not just host it almost everywhere a certain Python/Django environment is supported but more importantly to easily host it yourself on your own personal computer or server.

CHAPTER 1

Features

1.1 Good security features

- Open Source - everyone is invited to review the code!
- TLS 1.2 only with a very limited set of good ciphers
- Client certification verification built-in
- JSON Web Token authentication with RSA public/private keys
- We don't do crypto ourselfs but utilize battle-tested libraries and algorithms
- Data is encrypted with Fernet (symmetric authenticated cryptography)
- Data can be encrypted and stored on the client, encryption keys are always generated by the client to ensure trust.
- Encryption keys are not directly derived from a password, this way both the password an encryption-keys can easily be reset in case of a security-breach
- Planned support for all sorts of keys (fingerprint, yubikey and others)

See *keybar.utils.crypto* for more crypto-related configuration details.

If you find any security related issue please write an email to cg@webshox.org.

CHAPTER 2

Why yet another password storage?

The main idea is to create a open-source system to manage those passwords, with many new features like sharing, teams and organization management that others don't have.

A migration or partially-support for other systems like Keepass 1Password, LastPass is planned.

With that in mind, I generally wanted to implement one specific feature on top of LastPass (I use currently), and that was "change all passwords on a regular basis". With more than 200 sites registered with unique passwords it takes way too long to change all relevant passwords on a regular basis.

Since LastPass in particular does not provide any good API and in general is sort of a blackbox (we know they are using PBKDF2 and AES encryption but don't see any code or specifics) the only way was to step up and do it myself. To host the storage system in an environment I trust.

Also, I don't like the idea of unlocking all my passwords with just one "key" - usually some kind of a password. There has to be other ways…

2.1 Installation

Note: Keybar is being developed and tested on ArchLinux, Ubuntu and MacOSX. I doubt it'll work on Windows yet.

```
$ Create your virtualenv (recommended, use virtualenvwrapper)
$ mkvirtualenv keybar

$ # Clone repository
$ git clone git@github.com:keybar/keybar.git

$ # Activate Environment and install
$ workon keybar
$ make develop

$ # run tests
$ make test
```

2.2 Edit settings

Create a new file `src/keybar/settings.py` with the following content:

```
from keybar.conf.development import *
```

Edit and adapt this file to your specific environment.

2.3 Setup the database

Note: Please note that Keybar was developed with PostgreSQL in mind. It uses PostgreSQL-specific features and thus doesn’t support anything else.

Create an empty new PostgreSQL database (any other supported by Django works too).

```
$ createdb keybar_dev
```

Note: You might need to apply a postgresql user (`createdb -U youruser`) e.g `postgres` for proper permissions.

```
$ python manage.py migrate
```

2.4 Superuser

```
$ # Create a new super user
$ python manage.py createsuperuser
```

2.5 Run the server, celery and other services

Other services being used:

- Celery, is being used to run [regular] tasks, e.g for mail output.

To start all of them (including the tls-server):

```
$ honcho start
```

Note: You can find the SSL version on port 8443

Note: Our celery configuration requires redis to be installed and running. Please make sure it’s up!

2.6 Run the test-suite

Note: The test-suite requires to have access to the `local.keybar.io` domain. You might need to add it to your `/etc/hosts` or use a DNS server like `dnsmasq`.

```
$ make test
```

2.7 Resources

- Documentation
- Bug Tracker
- Code

CHAPTER 3

Keybar ChangeLog

3.1 Version 0.1

Not yet released, codename to be decided.

First preview release.

3.2 More documentation

CHAPTER 4

Indices and tables

- genindex
- modindex
- search