reqpi

Release 0+untagged.2.g7c23d71.dirty

December 16, 2015

Contents

CHAPTER 1

Introduction

Usually, Python projects are installed with `pip install -r requirements.txt`, with a frozen `requirements.txt` file. However, alternative build systems (such as Pants, Pex or hand-coded Dockerfiles) sometimes specify "floaters": packages that allow more than one version number (for example, "any greater than 1.2"). In addition, if `requirements.txt` is missing a requirement, most of these tools will recover gracefully by getting the highest compatible version.

While these are features sometimes, they undercut the concept of a "deterministic build" or "hermetic build": a build whose output depend only on the inputs, and not on the state of the world, such as what packages have been uploaded to PyPI.

ReqPI is a PyPI-compatible server which will generate ad-hoc end-points where "pre-commitment" is made to which packages will be requested. It will reject requests for any other packages, and will only offer the versions specified in a `requirements.txt` file. All Python package-fetching systems allow specifying an alternate URL for package source.

CHAPTER 2

Running

2.1 Server

The server is a twisted plugin. After installing `reqpi`, `twistd reqpi` should just work. Refer to `twistd` documentation for details on how to use it.

```
$ twistd reqpi [--http PORT] [--url URL]
```

The port is the port that `reqpi` will listen on. While it will try to make a good guess as to what is the URL through which it should be accesses, enough layers of reverse proxies, with interesting enough configuration, can confuse it. In that case, `--baseurl` should be passed to tell it where it is accessed from.

2.2 Client

```
$ PYPI=$(python -m reqpi gethash --url URL REQUIREMENTS_FILE)
```

This command will initialize PYPI with a URL that points to a PyPI-compatible server, but only allowing the packages in the requirements file. For example, this can be used with pip as follows:

Note that the requirements file only supports the `PACKAGE==VERSION` syntax. This is intentional: this is the only syntax which is properly hermetic (it is also what `pip freeze` will output).

```
$ pip install --index-url $PYPI Twisted[tls]
```