pickle-secure

Stephanos Kuma

Mar 07, 2023

CONTENTS

pickle-secure is a wrapper around pickle that creates encrypted pickles.

CHAPTER

ONE

IN A NUTSHELL

1.1 Installation

The easiest way is to use poetry to manage your dependencies and add *pickle-secure* to them.

```
[tool.poetry.dependencies]
pickle-secure = "^0.9.0"
```

1.2 Usage

`pickle-secure` offers a similar API as the built-in pickle.

CHAPTER

TWO

LINKS

- Documentation
- Changelog

2.1 Installation

The easiest way is to use poetry to manage your dependencies and add *pickle-secure* to them.

```
[tool.poetry.dependencies]
pickle-secure = "^0.9.0"
```

2.2 Usage

`pickle_secure` implements a secure way to *pickle* and *unpickle* a python object. It offers the same interface as a pickle, but a key is also required, which encrypts and decrypts the pickle.

Everything is placed in the `pickle_secure` module.

Three constants are provided:

`pickle_secure.`**`API_VERSION: str`**

The python version of the pickle that pickle_secure targets

`pickle_secure.`**`HIGHEST_PROTOCOL: int`**

The same as the original HIGHEST_PROTOCOL from the *pickle* module

`pickle_secure.`**`DEFAULT_PROTOCOL: int`**

The same as the original DEFAULT_PROTOCOL from the *pickle* module

There are also three exceptions provided, all of them are just the same as the ones in the original pickle

`exception` `pickle_secure.`**`PickleError`**

The same as the original PickleError from the *pickle* module

`exception` `pickle_secure.`**`PicklingError`**

The same as the original PicklingError from the *pickle* module

`exception` `pickle_secure.`**`UnpicklingError`**

The same as the original UnpicklingError from the *pickle* module

Also, the dumping and loading functions present in the original module are present:

`def dumps(obj, protocol=None, *, fix_imports=True, key):`

Dump the object to a bytes object.

Parameters

- **obj** – The object to be pickled
- **protocol** (*int*) – The pickle protocol to be used, or None to use the default protocol
- **fix_imports** (*bool*) – If the protocol is < 2, it will try to fix the imports to be readable by python2
- **key** (*str*) – The encryption key

Returns

the encrypted pickle of the object

Return type

bytes

`def dump(obj, file, protocol=None, *, fix_imports=True, key):`

Dump the obj in the file object named `file`.

Parameters

- **obj** – The object to be pickled
- **file** – The file to use to write the pickle
- **protocol** (*int*) – The pickle protocol to be used, or None to use the default protocol
- **fix_imports** (*bool*) – If the protocol is < 2, it will try to fix the imports to be readable by python2
- **key** (*str*) – The encryption key

`def loads(bytes_object, *, fix_imports=True, encoding="ASCII", errors="strict", key):`

Retrieve the original object from a bytes object

Parameters

- **bytes_obj** (*bytes*) – The encrypted bytes object to be unpickled
- **fix_imports** (*bool*) – If the protocol is < 2, it will try to fix the imports to be readable by python2
- **encoding** (*str*) – It is present for compatibility reasons with python2
- **errors** (*str*) – It is present for compatibility reasons with python2
- **key** (*str*) – The encryption key

Returns

The object that was originally pickled

`def load(file, key, *, fix_imports=True, encoding="ASCII", errors="strict"):`

Retrieve the original object from a file

Parameters

- **file** – The file containing the encrypted pickle
- **fix_imports** (*bool*) – If the protocol is < 2, it will try to fix the imports to be readable by python2
- **encoding** (*str*) – It is present for compatibility reasons with python2

- **errors** (*str*) – It is present for compatibility reasons with python2
- **key** (*str*) – The encryption key

Returns

The object that was originally pickled

2.3 Changelog

All notable changes to this project will be documented in this file.

The format is based on Keep a Changelog, and this project adheres to Semantic Versioning.

2.3.1 Unreleased

2.3.2 0.99.9 - 2023-03-07

Added

- Added type hints

Removed

- Dropped python 3.7 support
- Dropped support for cryptography <= 39.0.0

Removed

- Removed changelog from the published wheel

2.3.3 0.9.99 - 2022-01-05

Added

- Added python310 support
- Added a changelog

Removed

- Dropped python36 support

2.3.4 0.9.9 - 2020-02-26

Changed

- Fully implemented the python 3.6 pickle API

2.3.5 0.2.0 - 2018-10-06

Changed

- Changed crypto backend from pycrypto to cryptography

2.3.6 0.1.3 - 2018-10-06

Changed

- Changed licence to MIT

2.3.7 0.1.2 - 2018-10-06

Removed

- Dropped support for python less than 3.6

2.3.8 0.1.1 - 2018-03-03

Removed

- Dropped support for python 3.2

2.3.9 0.1.0 - 2018-03-03

Added

- Initial release

2.3.10 0.0.1a1 - 2016-09-27

Added

- Added the following constants:
  - HIGHEST_PROTOCOL
  - DEFAULT_PROTOCOL
- Added the following methods:
  - load

  - loads
  - dump
  - dumps
- Added the following exceptions:
  - PickleError
  - PicklingError
  - UnpicklingError
- Added the following classes:
  - Pickler
  - Unpickler

PYTHON MODULE INDEX

INDEX