



The **dangerous** Flask

Let's talk about itsdangerous



About Me

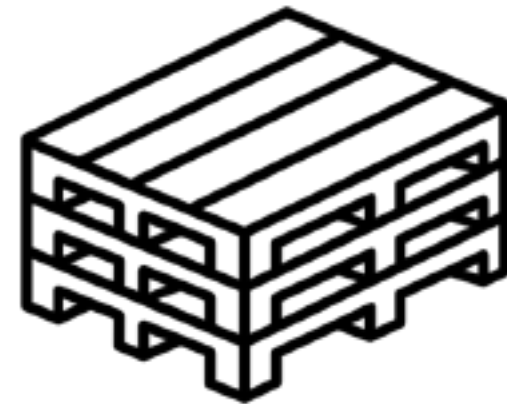


Hsiaoming Yang

lepture

<https://github.com/lepture>

<https://lepture.com/about>

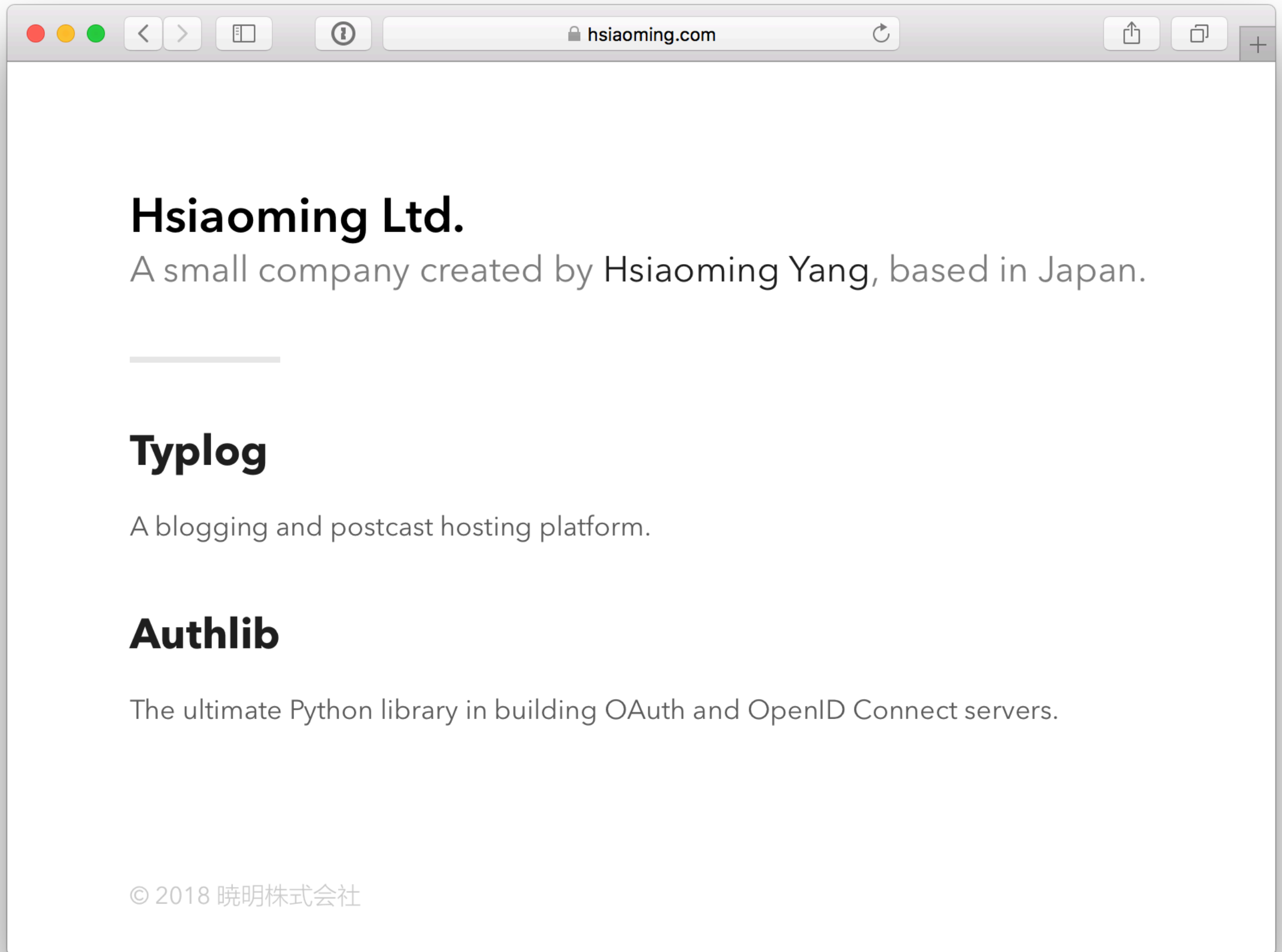


The Pallets Projects



Flask

web development,
one drop at a time



Hsiaoming Ltd.

A small company created by Hsiaoming Yang, based in Japan.

Typlog

A blogging and postcast hosting platform.

Authlib

The ultimate Python library in building OAuth and OpenID Connect servers.

https://typlog.com/



SITE

[Analytics](#)

[Posts](#)

[Pages](#)

[Tags](#)

SETTINGS

[General](#)

[Design](#)

[Links](#)

[Apps](#)

[Labs](#)

[What's New](#)

[Need help?](#)

[« Collapse](#)

SUBSCRIBERS

Inoreader

1316

Feedly

837

MailChimp

65

The Old Reader

61

NewsBlur

51

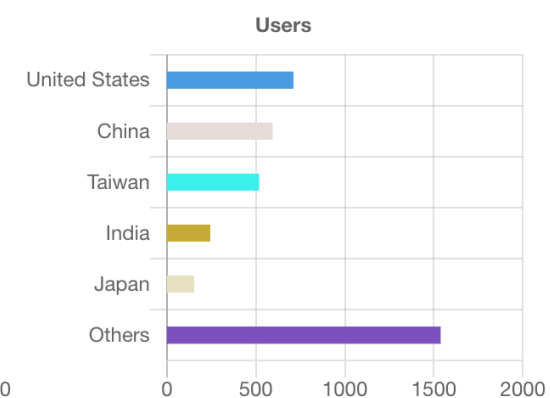
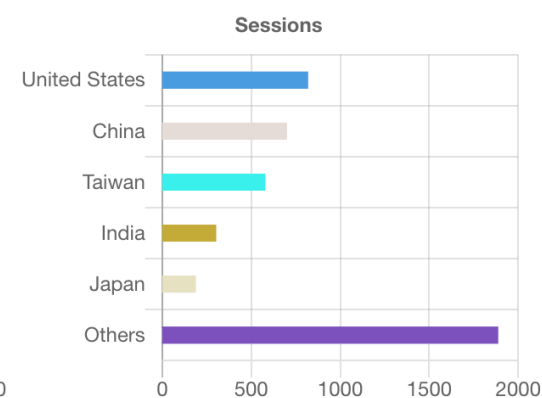
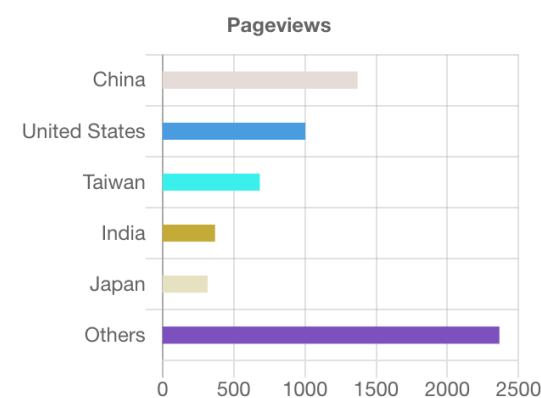
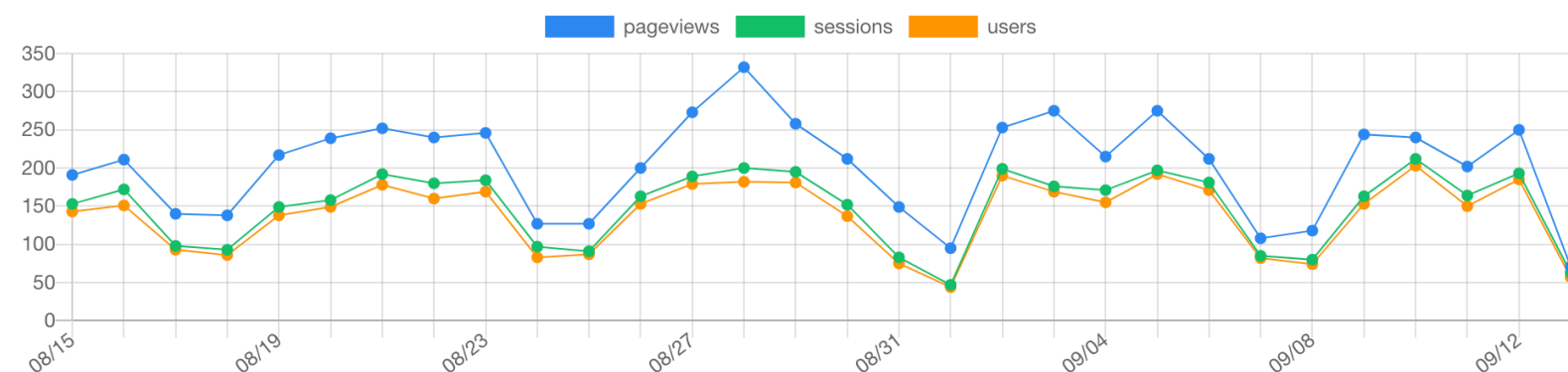
Feedbin

28

Feed Wrangler

4

SITE STATS



<https://authlib.org/>



Authlib

The ultimate Python library in building OAuth and OpenID Connect servers.


[GITHUB](#)

[DOCS](#)

1

Session

app.py



```
1 from flask import Flask, session
2
3 app = Flask(__name__)
4 app.secret_key = 'secret'
5
6
7 @app.route('/')
8 def hello():
9     session['msg'] = 'Hi'
10    return 'ok'
11
```


\$ flask run

http://127.0.0.1:5000

▼ Response Headers [view source](#)

Content-Length: 2

Content-Type: text/html; charset=utf-8

Date: Fri, 13 Sep 2019 06:26:32 GMT

Server: Werkzeug/0.15.5 Python/3.7.4

Set-Cookie: session=eyJtc2ciOiJJJaSJ9.XXs2mA.GAZzFxyv_RCuX-zyR6oXPB0PRXI; HttpOnly; Path=

Vary: Cookie

session



payload

eyJtc2ciOiJJaSJ9

•

XXs2mA



timestamp

•

GAZzFxyv_RCuX-zyR6oXPBOPRXI



signature

2

URLSafeTimedSerializer

flask/sessions.py

389 lines (312 sloc) | 14 KB

Raw

Blame

History



● You're using jump to definition to discover and navigate code. [Opt out](#) Beta

[Learn more](#) or [give us feedback](#)

```
1  # -*- coding: utf-8 -*-
2  """
3      flask.sessions
4      ~~~~~~
5
6      Implements cookie based sessions based on itsdangerous.
7
8      :copyright: 2010 Pallets
9      :license: BSD-3-Clause
10 """
11 import hashlib
12 import warnings
13 from datetime import datetime
14
15 from itsdangerous import BadSignature
16 from itsdangerous import URLSafeTimedSerializer
17 from werkzeug.datastructures import CallbackDict
18
19 from ._compat import collections_abc
20 from .helpers import is_ip
21 from .helpers import total_seconds
22 from .json.tag import TaggedJSONSerializer
23
```



payload

eyJtc2ciOiJIaSJ9

```
>>> import base64
>>> payload = base64.urlsafe_b64decode(b'eyJtc2ciOiJIaSJ9')
>>> print(payload)
b'{"msg": "Hi"}'
```

XXs2mA



timestamp

```
>>> import base64
>>> data = base64.urlsafe_b64decode(b'XXs2mA==')
>>> print(data)
b']{6\x98'
>>> bytes_to_int(data)
1568355992
```

GAZzFxyv_RCuX-zyR6oXPBOPRXI



```
>>> sign(payload, timestamp, secret)
```

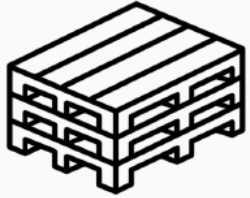
Signature

- SHA1, SHA256, SHA384, SHA512
- HMAC with SHA
- base64

DEMO

3

itsdangerous




The Pallets Projects

Home of some popular Python web libraries

📍 Around The World 🔗 <https://palletsprojects.com/> ✉ contact@palletsprojects.com

 **Repositories** 23

 Packages

 People 24

 Teams 9

 Projects

Pinned repositories

 **flask**

The Python micro framework for building web applications.

● Python ★ 46.4k 🍷 12.9k

 **jinja**

The Jinja template engine

● Python ★ 6.5k 🍷 1.2k

 **werkzeug**

The comprehensive WSGI web application library.

● Python ★ 4.9k 🍷 1.4k

 **click**

Python composable command line interface toolkit

● Python ★ 8.1k 🍷 804

 **itsdangerous**

Safely pass trusted data to untrusted environments and back.

● Python ★ 1.8k 🍷 157

 **markupsafe**

Safely add untrusted strings to HTML/XML markup.

● Python ★ 281 🍷 78

History

- **Flask 0.10**: Changed default cookie serialization format from pickle to JSON to limit the impact an attacker can do if the secret key leaks.
- **Flask 0.10**: add **itsdangerous** to dependencies

WHAT IS
itsdangerous

e.g. session

koa.js

express.js

Cookie: session=xxx

Cookie: session.sig=xxx

```
session.sig =  
Sign(session, secret)
```

self-made

4

Json Web Signature

JWS in itsdanerouse

- JSONWebSignatureSerializer
- TimedJSONWebSignatureSerializer

JWS

header

eyJ0eXAiOiJKV1QiLA0KICJhbGciOiJIUzI1NiJ9

.

payload

eyJpc3MiOiJqb2UiLA0KICJleHAiOiJ0eMDA4MTkzODAsDQogImh0dHA6Ly9leGFtcGxlLmNvbS9pc19yb290Ijp0cnVlfQ

.

dBjftJeZ4CVP-
mB92K27uhbUJU1p1r_wW1gFWFOEjXk

signature

TimedJSONWebSignatureSerializer

eyJhbGciOiJIUzI1NiIsI
mV4cCI6MTU2ODM1NTk5Mi
wiaWF0IjoxNTE2MjM5MDI
yfQ



header

•

```
{  
  "alg": "HS256",  
  "exp": 1568355992,  
  "iat": 1516239022,  
}
```

alg

- HS256, HS384, HS512
- RS256, RS384, RS512
- ES256, ES384, ES512
- PS256, PS384, PS512

alg is
defined sign method

5

Json Web Token

JWT based on JWS

header

eyJ0eXAiOiJKV1QiLA0KICJhbGciOiJIUzI1NiJ9

.

payload

eyJpc3MiOiJqb2UiLA0KICJleHAiOiJ0eXMDA4MTkzODAsDQogImh0dHA6Ly9leGFtcGxlLmNvbS9pc19yb290Ijp0cnVlfQ

.

dBjftJeZ4CVP-
mB92K27uhbUJU1p1r_wW1gFWFOEjXk

signature

6

JWE & JWK & JWA



**Real dangerous
thing in Flask**

```
{{ config.SOME_SECRET_CONFIG }}
```

8

Session Again

Backend Session

Thanks