



**Back Home** (../index.html)

2022年5月9日 💎 python

# 实战：python开发jsrpc服务与演示

项目地址：https://github.com/sixgad/py-jsrpc

## **py-jsrpc**

python实现一套轻量、协程异步、websocket远程调用服务，js逆向、混淆加密一把梭，再也不用扣js了。

雪重

Python Developer  
知识 汗水 灵感 机遇

## 1.食用方法

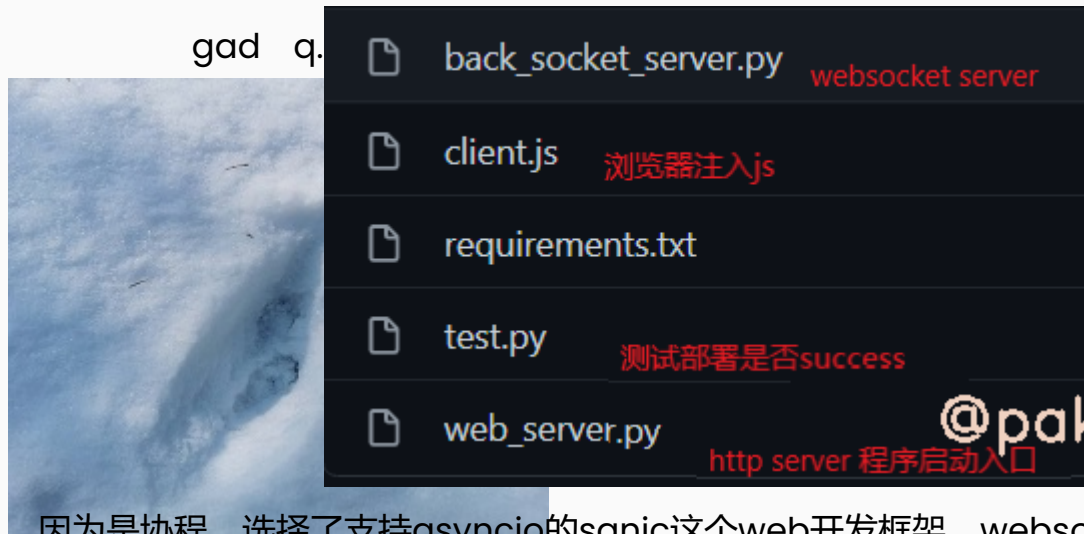


(htt   ✉  
ps:/ (ma  
/git   ilto:2  
hub. 7827  
com 023

```
git clone git@github.com:sixgad/py-jsrpc.git  
pip install -r requirements.txt
```

50M

## 2.模块说明



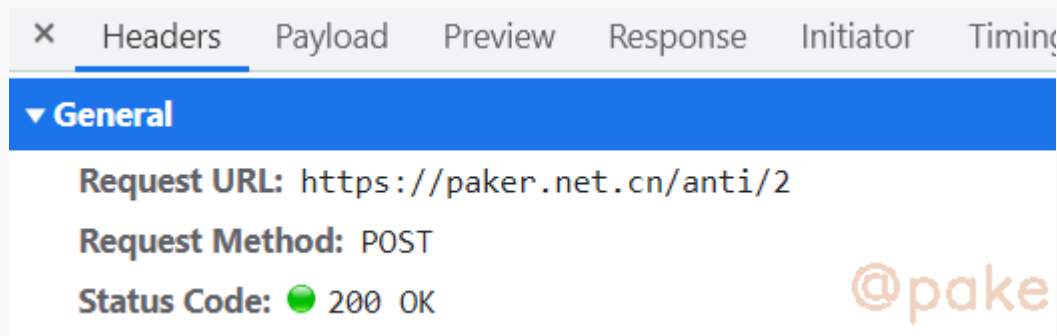
因为是协程，选择了支持asyncio的sanic这个web开发框架，websockets这个websocket包

雪重

## 3.实战

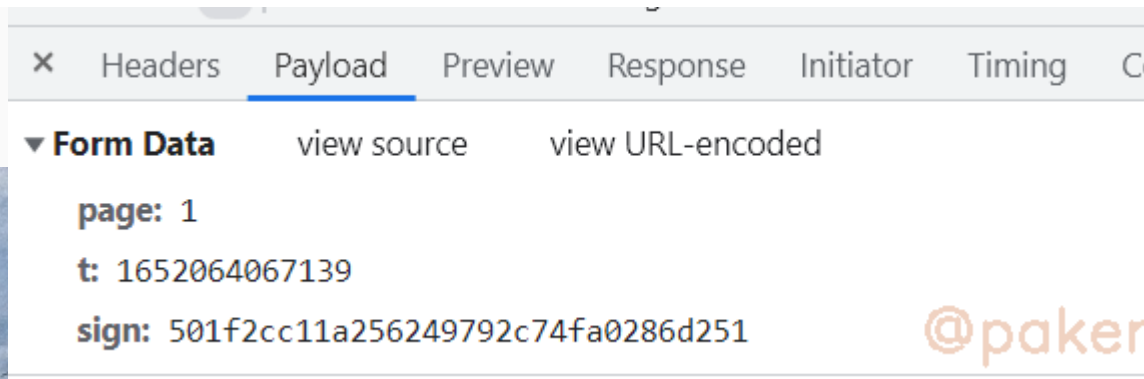
以反爬演示平台下的示例2为例，地址：<https://paker.net.cn/anti/2>

数据是从这个接口返回，post请求



请求数据如下，page为页码，t为时间戳，sign为加密数据

com 023



js请求是从这里发出的

```
call = function (num) {  
    var list = encry(String(num));  
    $.ajax({  
        url: url,  
        dataType: "json",  
        async: true,  
        data: list,  
        type: "POST",  
        beforeSend: function (request) {  
            (function () {  
            })()  
        },  
    });  
}
```

其中encry(String(num))返回了post请求需要的参数

按照以前的方法，追进encry方法里还原加密逻辑算法，或者把encry方法js全部扣下来，用node环境执行。

使用rpc调用pyjsrpc (<https://github.com/sixgad/py-jsrpc>)，只能说不要太简单，具体操作如下：

1.修改client.js

直接拉到底部，注册function "encry"

```

//demo /six 0@q
//group很重要，每个项目应该有一个独立的group，比如爬百度时group=baidu-group，爬抖音时group=
dy-group, ggd q.co
//可以同时存在多个group，互不影响
var client = new JsClient("ws://localhost:6789/register?group=ws-group&clientId="+guid());
//获取服务器时间
client.registerAction("clientTime",function(request, resolve,reject ){
    resolve(""+new Date());
})
//encry
client.registerAction("encry",function(request,resolve,reject){
    //num 是调用http接口时我们传递过来的参数
    var num = request['num'];
    //直接抄原网页上的调用
    var list = encry(String(num));
    //返回数据
    resolve(list)
})

```

雪重

## 2.启动WebServer.py & 浏览器注入js

启动 http server 知识 汗水 灵感 机遇

```
python web_server.py
```



浏览器注入js，在目标网站https://paker.net.cn/anti/2，打开控制台(F12), Console下  
注入client.js

ps:/ (ma

/git ilto:2

hub. 7827

com 023

[返回首页](#)

## 古诗欣赏

渡漢江

李頻

嶺外音書絕，經年復歷春。

近鄉情更怯，不敢問來人。

```
Elements Console Sources CSS Overview Performance Memory Application Security Lighthouse Welcome Network +
top Filter Default levels 25
}
return (S4()+S4()+"-"+S4()+"-"+S4()+"-"+S4()+"-"+S4()+S4()+S4());
}
}
//demo
var client = new JsClient("ws://localhost:6789/register?group=ws-group&clientId="+guid());
//获取服务器时间
client.registerAction("clientTime",function(request, resolve,reject ){
    resolve(""+new Date());
});
//encry
client.registerAction("encry",function(request,resolve,reject){
    //num 是调用http接口时我们传递过来的参数
    var num = request['num'];
    //直接抄原网页上的调用
    var list = encry(String(num));
    //返回数据
    resolve(list)
});
jsclient begin of connect to wsURL: ws://localhost:6789/register?group=ws-group&clientId=c4d8d099-3c68-6692-f39e-1894466152dd
jsclient register action: clientTime
jsclient register action: encry
< JsClient {wsURL: 'ws://localhost:6789/register?group=ws-group&clientId=c4d8d099-3c68-6692-f39e-1894466152dd', handlers: {...}, socket: WindowWebSocketWrapp
jsclient open a connection
>|
```

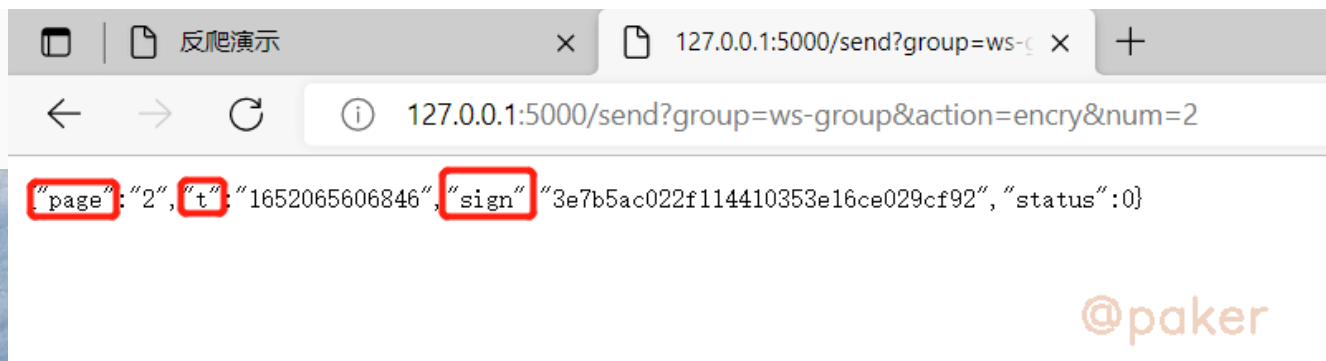
jsclient open a connection, 说明已经连接成功，可以调用请求http接口获取在浏览器内js执行返回的结果

### 3.调用接口，获取js执行结果

ps: (ma  
http接口: http://127.0.0.1:5000/send?group=ws-group&action=encry&num=2  
接口里的action, num对应第一步 client.js。

hub. 7827

com 023



本文只是提供了最简单的demo, jsrpc可以使用的场景很多, 比如某数的cookie, 某音, 98k等等

雪重

Python Developer


知识 汗水 灵感 机遇

Copyright © 2021 爬客 All rights reserved

辽ICP备2021000509号-1 (<https://beian.miit.gov.cn/#/Integrated/index>) 辽公网安备



21032302210389号 (<http://www.beian.gov.cn/portal/index.do>)

(http 

联系邮箱: 278270230@qq.com

ps:/ (ma

/git ilto:2

hub. 7827

com 023