

作业 写一个简单的远控

启动服务端

```
(venv_miansha3) root@ubuntu:~/code/miansha_3/server# ll
total 52
drwxrwxrwx 1 root root    0 Oct  3 11:49 ./
drwxrwxrwx 1 root root  4096 Oct  3 11:51 ../
drwxrwxrwx 1 root root  4096 Oct  3 08:30 app/
-rwxrwxrwx 1 root root 44032 Oct  3 11:48 miansha3.db*
-rwxrwxrwx 1 root root   216 Oct  3 11:49 requirements.txt*
-rwxrwxrwx 1 root root   233 Oct  3 11:52 web.py*
(venv_miansha3) root@ubuntu:~/code/miansha_3/server# python web.py
/root/venv_miansha3/lib/python3.7/site-packages/flask_sqlalchemy/__init__.py:873: FSADeprecationWarning: SQLAlchemy_
ress this warning.
'SQLALCHEMY_TRACK_MODIFICATIONS adds significant overhead and '
/root/venv_miansha3/lib/python3.7/site-packages/flask_sqlalchemy/__init__.py:873: FSADeprecationWarning: SQLAlchemy_
ress this warning.
'SQLALCHEMY_TRACK_MODIFICATIONS adds significant overhead and '
* Serving Flask app 'app'
* Debug mode: on
WARNING: This is a development server. Do not use it in a production deployment. Use a production WSGI server instea
* Running on all addresses (0.0.0.0)
* Running on http://127.0.0.1:5050
* Running on http://192.168.248.130:5050
Press CTRL+C to quit
* Restarting with stat
/root/venv_miansha3/lib/python3.7/site-packages/flask_sqlalchemy/__init__.py:873: FSADeprecationWarning: SQLAlchemy_
ress this warning.
'SQLALCHEMY_TRACK_MODIFICATIONS adds significant overhead and '
/root/venv_miansha3/lib/python3.7/site-packages/flask_sqlalchemy/__init__.py:873: FSADeprecationWarning: SQLAlchemy_
ress this warning.
'SQLALCHEMY_TRACK_MODIFICATIONS adds significant overhead and '
* Debugger is active!
* Debugger PIN: 277-515-839
```

启动被控端

```
问题 3 输出 终端 调试控制台 JUPYTER

PS D:\code\miansha_3\client> python .\client.py
[+] start client
```

这时可以在服务端看到心跳

```
WARNING: This is a development server. Do not use it in a production deployment. Use a production WSGI server instead.
* Running on all addresses (0.0.0.0)
* Running on http://127.0.0.1:5050
* Running on http://192.168.248.130:5050
Press CTRL+C to quit
* Restarting with stat
/root/venv_miansha3/lib/python3.7/site-packages/flask_sqlalchemy/__init__.py:873: FSADeprecationWarning: SQLAlchemy_TRACK_MODIFICATIONS adds significant overhead and 'SQLALCHEMY_TRACK_MODIFICATIONS' will be set to False by default in a future version.
ress this warning.
SQLALCHEMY_TRACK_MODIFICATIONS adds significant overhead and 'SQLALCHEMY_TRACK_MODIFICATIONS' will be set to False in a future version.
ress this warning.
SQLALCHEMY_TRACK_MODIFICATIONS adds significant overhead and 'SQLALCHEMY_TRACK_MODIFICATIONS' will be set to False in a future version.
* Debugger is active!
* Debugger PIN: 277-515-839
{'token': 'bkq98', 'name': 'f875a4043160', 'result': '', 'cmd_id': None}
192.168.248.1 - - [03/Oct/2022 13:33:33] "POST /heartbeat/ HTTP/1.1" 200 -
{'token': 'bkq98', 'name': 'f875a4043160', 'result': '', 'cmd_id': None}
192.168.248.1 - - [03/Oct/2022 13:33:36] "POST /heartbeat/ HTTP/1.1" 200 -
{'token': 'bkq98', 'name': 'f875a4043160', 'result': '', 'cmd_id': None}
192.168.248.1 - - [03/Oct/2022 13:33:39] "POST /heartbeat/ HTTP/1.1" 200 -
{'token': 'bkq98', 'name': 'f875a4043160', 'result': '', 'cmd_id': None}
192.168.248.1 - - [03/Oct/2022 13:33:42] "POST /heartbeat/ HTTP/1.1" 200 -
```

浏览器访问服务端

可以看到 注册的客户端

miansha3 client list

name	ip	执行命令	历史记录	上次心跳时间
f875a4043160	192.168.248.1	操作	查看	2022-10-03 13:34:21

执行命令

点击操作

miansha3 cmd

name: f875a4043160 ip: 192.168.248.1

cmd:

结果

输入命令 ipconfig 点击提交 会显示命令执行中

miansha3 cmd

name: f875a4043160 ip: 192.168.248.1

cmd:

结果

命令执行中

等待会可以看到完整的结果

miansha3 cmd

name: f875a4043160 ip: 192.168.248.1

cmd:

结果

Windows IP 配置

以太网适配器 以太网:

媒体状态 : 媒体已断开连接
连接特定的 DNS 后缀 :

无线局域网适配器 本地连接* 1:

媒体状态 : 媒体已断开连接
连接特定的 DNS 后缀 :

无线局域网适配器 本地连接* 2:

媒体状态 : 媒体已断开连接
连接特定的 DNS 后缀 :

以太网适配器 VMware Network Adapter VMnet1:

连接特定的 DNS 后缀 :
本地链接 IPv6 地址. : fe80::5df0:e2b:a136:33d8%17
IPv4 地址 : 192.168.57.1
子网掩码 : 255.255.255.0
默认网关. :

以太网适配器 VMware Network Adapter VMnet8:

连接特定的 DNS 后缀 :
本地链接 IPv6 地址. : fe80::f1ad:d071:efbc:f9b2%12
IPv4 地址 : 192.168.248.1
子网掩码 : 255.255.255.0
默认网关. :

无线局域网适配器 WLAN:

连接特定的 DNS 后缀 :
本地链接 IPv6 地址. : fe80::c581:ea3b:6de1:3150%9
IPv4 地址 : 192.168.0.106
子网掩码 : 255.255.255.0
默认网关. : 192.168.0.1

修改下次上传时间

默认是3s

执行命令 sleep 10 修改延迟时间为10s

这时再执行命令就要等10s才会有结果

[←](#) [→](#) [↻](#) [🏠](#) [⚠ 不安全](#) | 192.168.248.130:5050/cmd/f875a4043160/192.168.248.1/

miansha3 cmd

name: f875a4043160 ip: 192.168.248.1

cmd:

结果

time set ok

数据上传

数据上传和心跳是一个请求

每次心跳会带上一次命令执行的结果以及下一次是否有需要执行的命令

