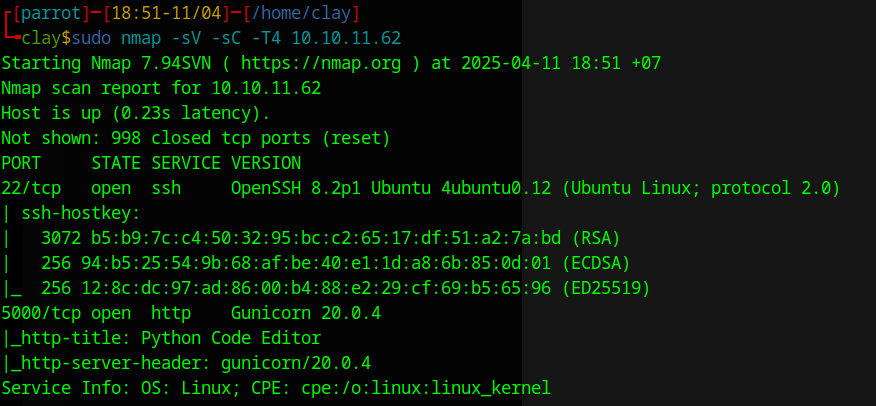
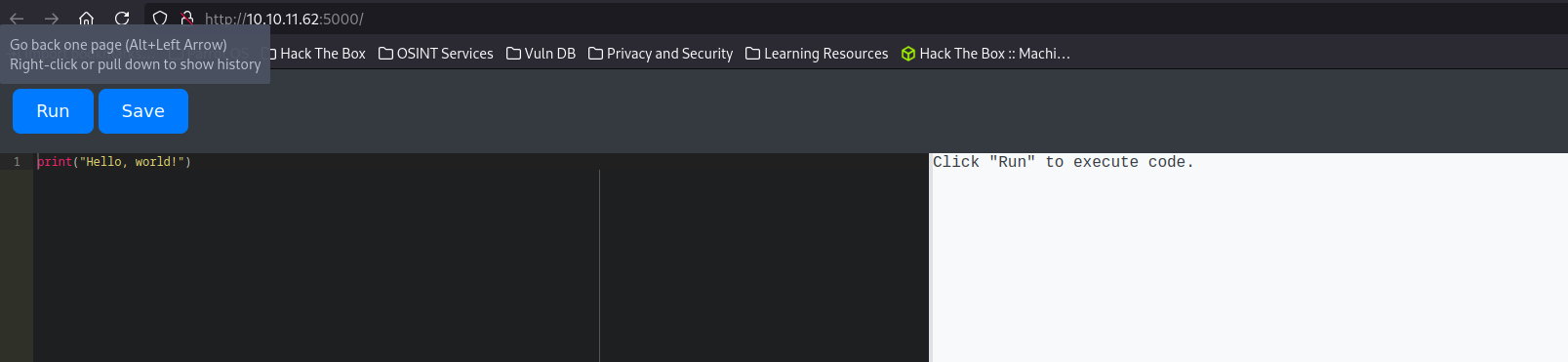
B1: Scanning

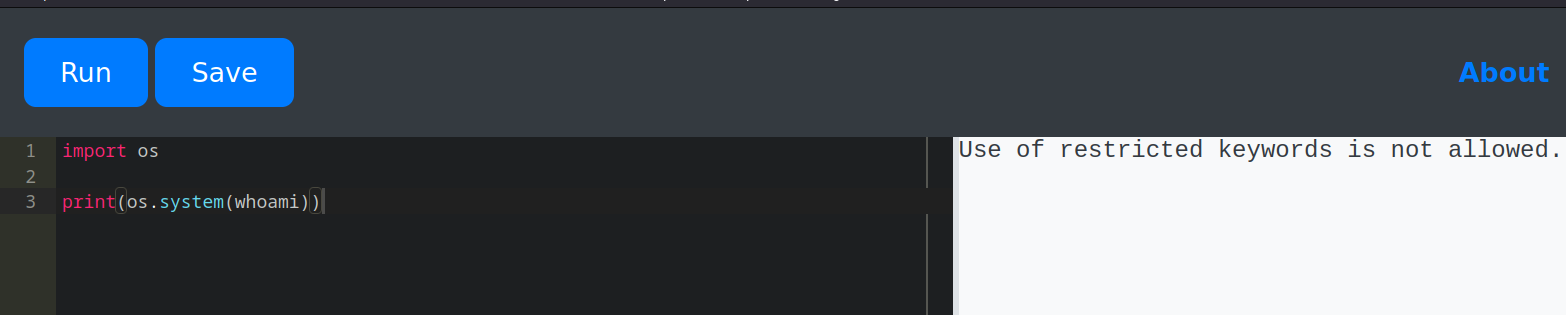


Ta thấy cổng 5000 mở

Và là cổng python editor



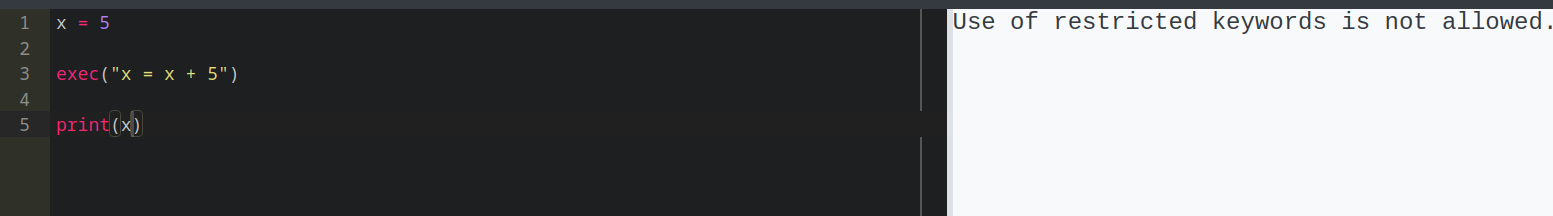
Ta thử 1 vài biến



Os đã bị chặn



Eval cũng bị chặn



Exec() cũng bị chặn

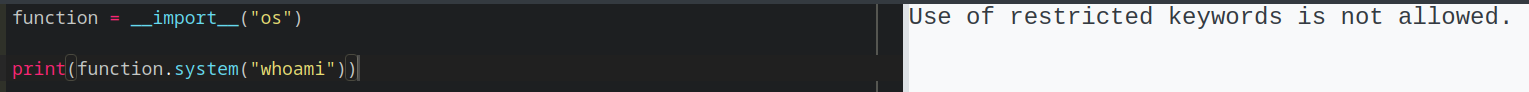
Thử 1 vài module thì đều có lẽ đã bị block k dùng dược

Thử sử dụng indirect import

function = \_\_import\_\_("os")

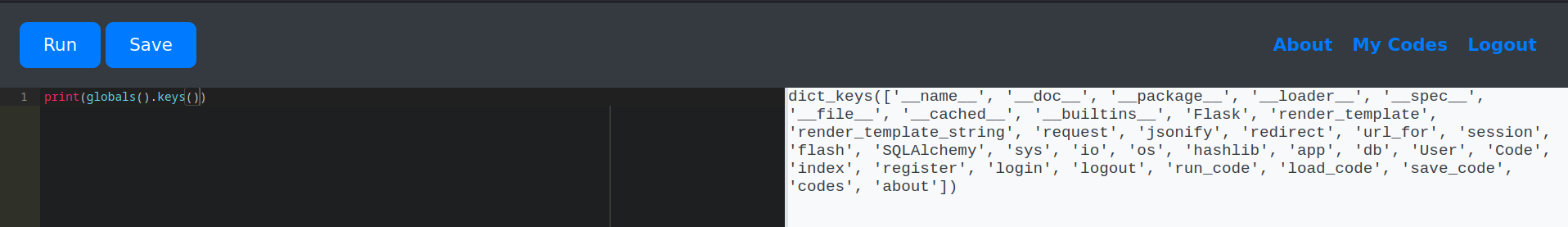
print(function.system(whoami))

Ta k gọi trực tiếp import os mà dùng hàm \_\_import\_\_(“os”)



Nhưng cũng bị chặn

Ta có thể thử 1 vài cách như xem những biến global và những module đã được thêm vào sẵn.



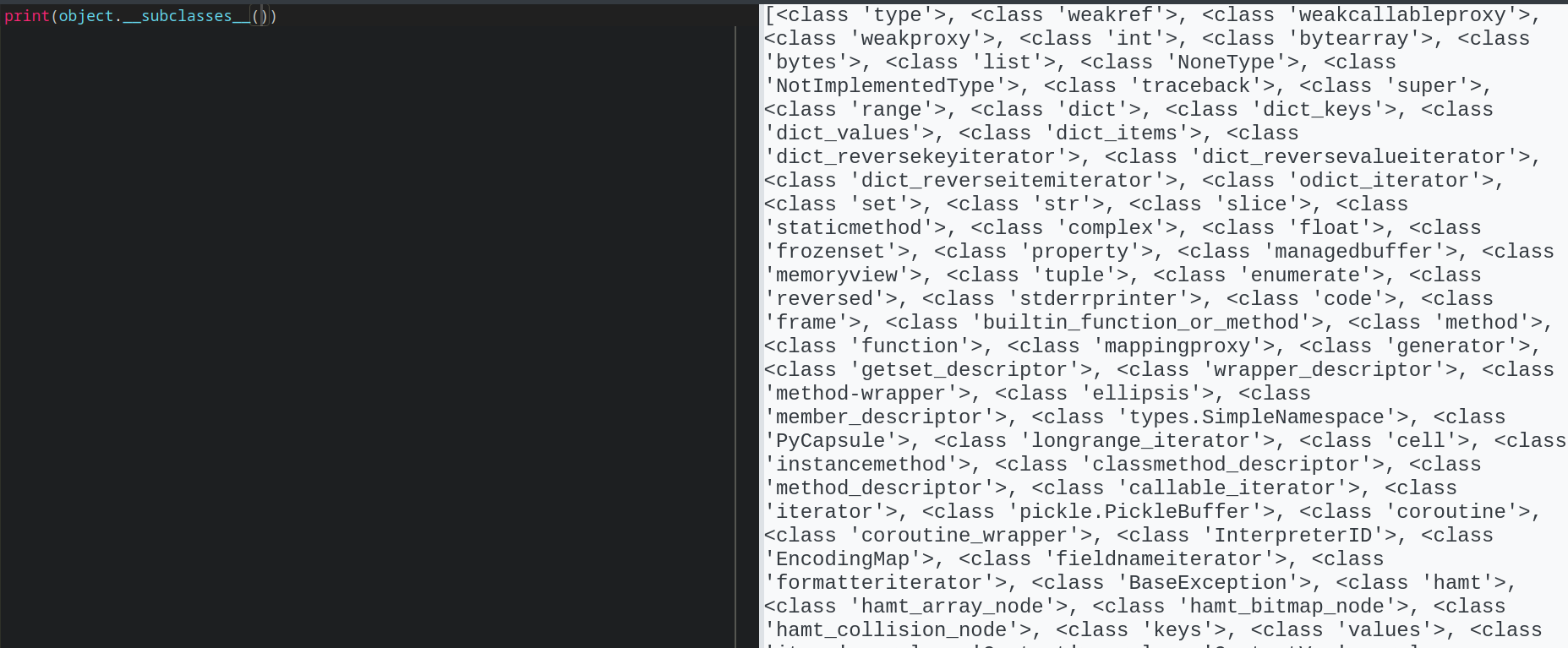
Ta tìm thử class của biến int -> thuộc lớp type



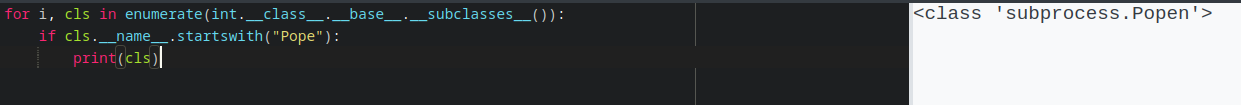
Ta thấy lớp cha của lớp type



Ta tìm tất cả các lớp kế thừa lớp object này

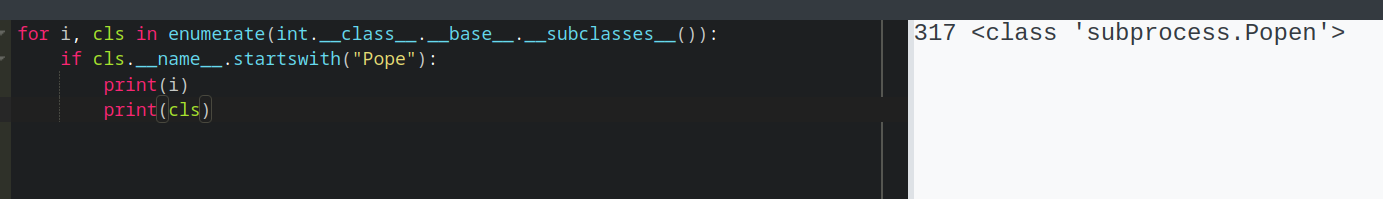


Ta đi tìm hàm subProcess vì nó là lớp con của lớp object cho nên ta đi lần từ lớp của int rồi sang lớp cha của nó chính là object và rồi đi tìm các lớp con của object.   
Ta chạy qua vòng for rồi tìm Popen

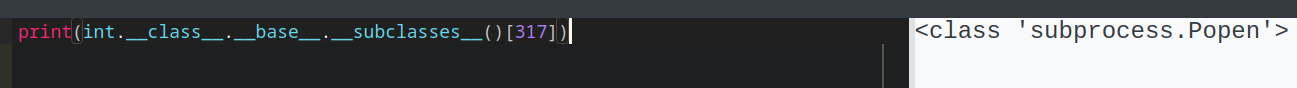


Hàm subprocess.Popen là hàm cho khả năng tương tác với process hệ thống thông qua tạo process con

Ta tìm vị trí của Popen trong dãy ở đây là 317

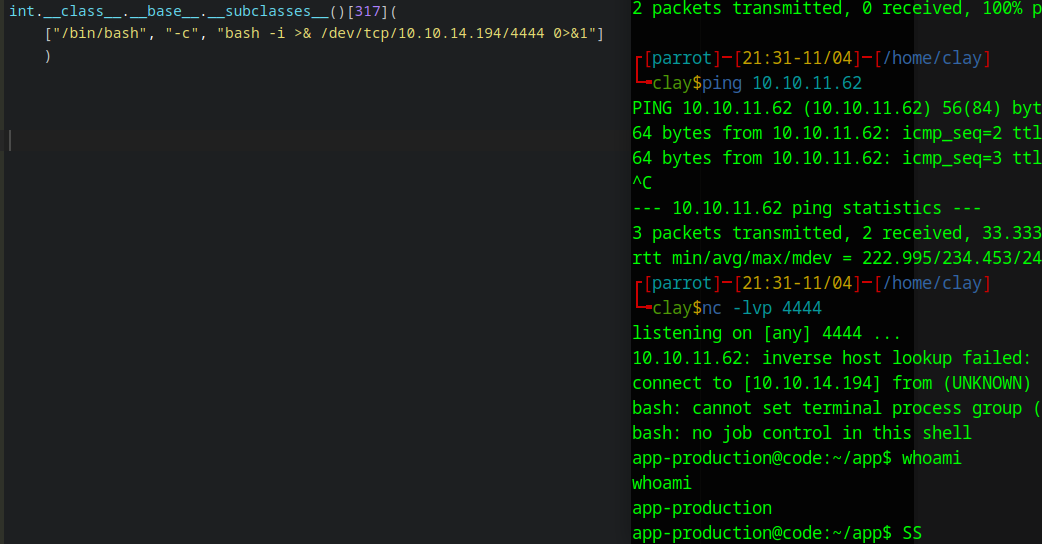


Ta đã tìm ra cách truy cập vào subprocess.Popen

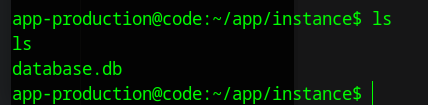


B2: exploit

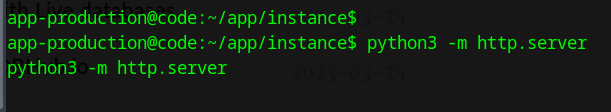
Ta từ đó có thể gọi hàm subprocess.Popen để mở 1 tiến trình mới, ở đây ta mở 1 reverse shell trả ngược về và bật netcat lắng nghe



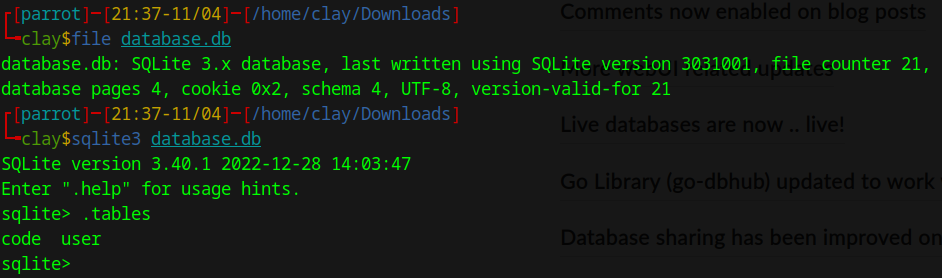
Có thể thấy có 1 db ở đây



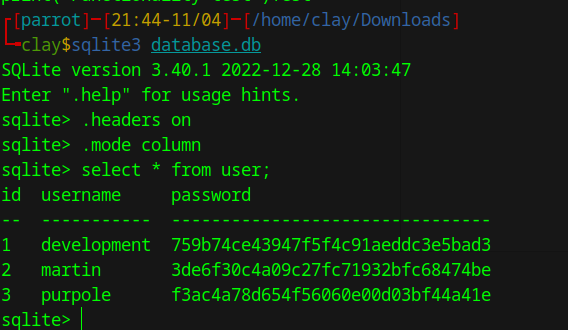
Ta dùng file server lấy file đó về



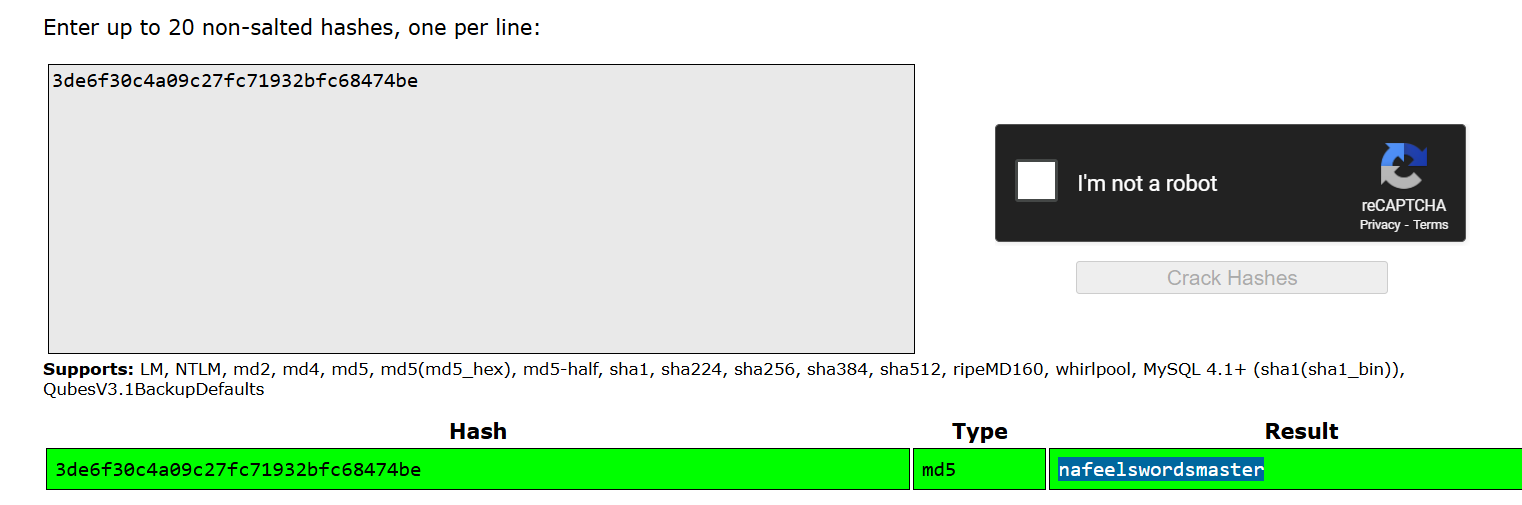
Dùng sqlite để xem thông tin



Ở đâycó 2 bảng user và code



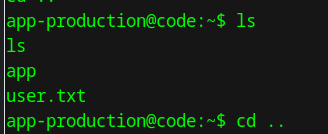
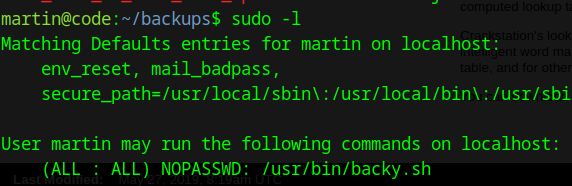
Ta thấy được 2 user và ta có thể thấy hash



Ta có được mk của tk martin

nafeelswordsmaster

Ta đăng nhập vào với thông tin có dc

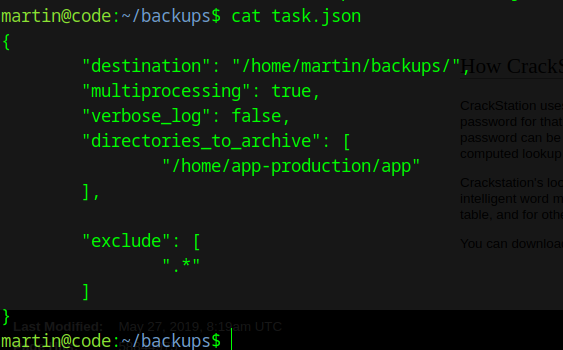


Lấy được user flag

Ta thấy tài khoản này có quyền thự thi backy.sh

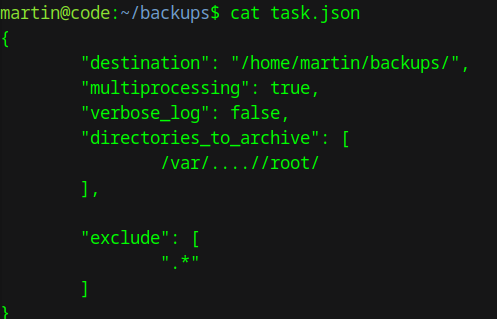


Nó yêu cầu 1 file json

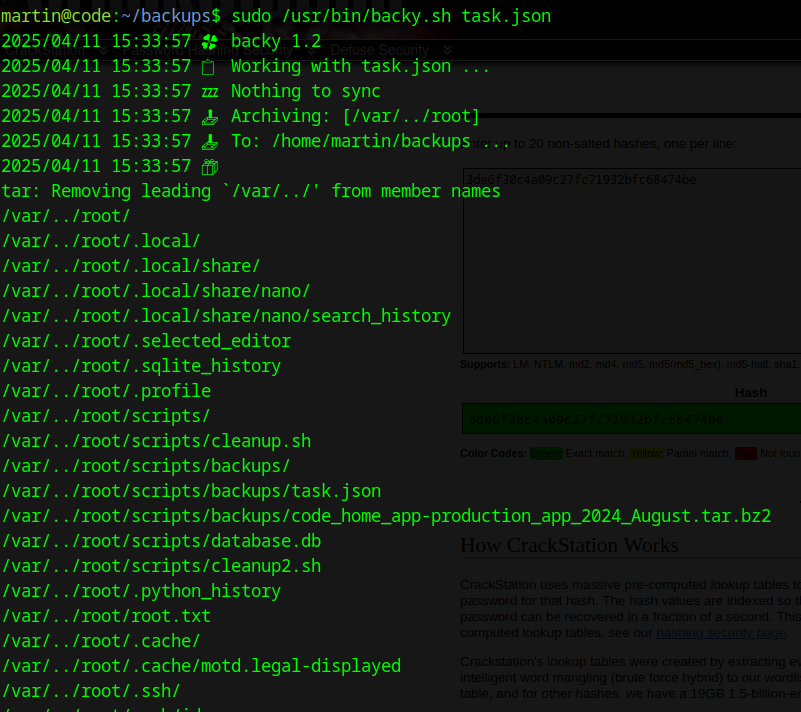


Thông tin của file json

Ta dùng path traversal để sửa đổi file nhằm lấy dc thông tin ở root



Ta dùng backy.sh là có thể nén được thư mục root



Ta truyền file về



Truyền file về và ta giải nén ra

