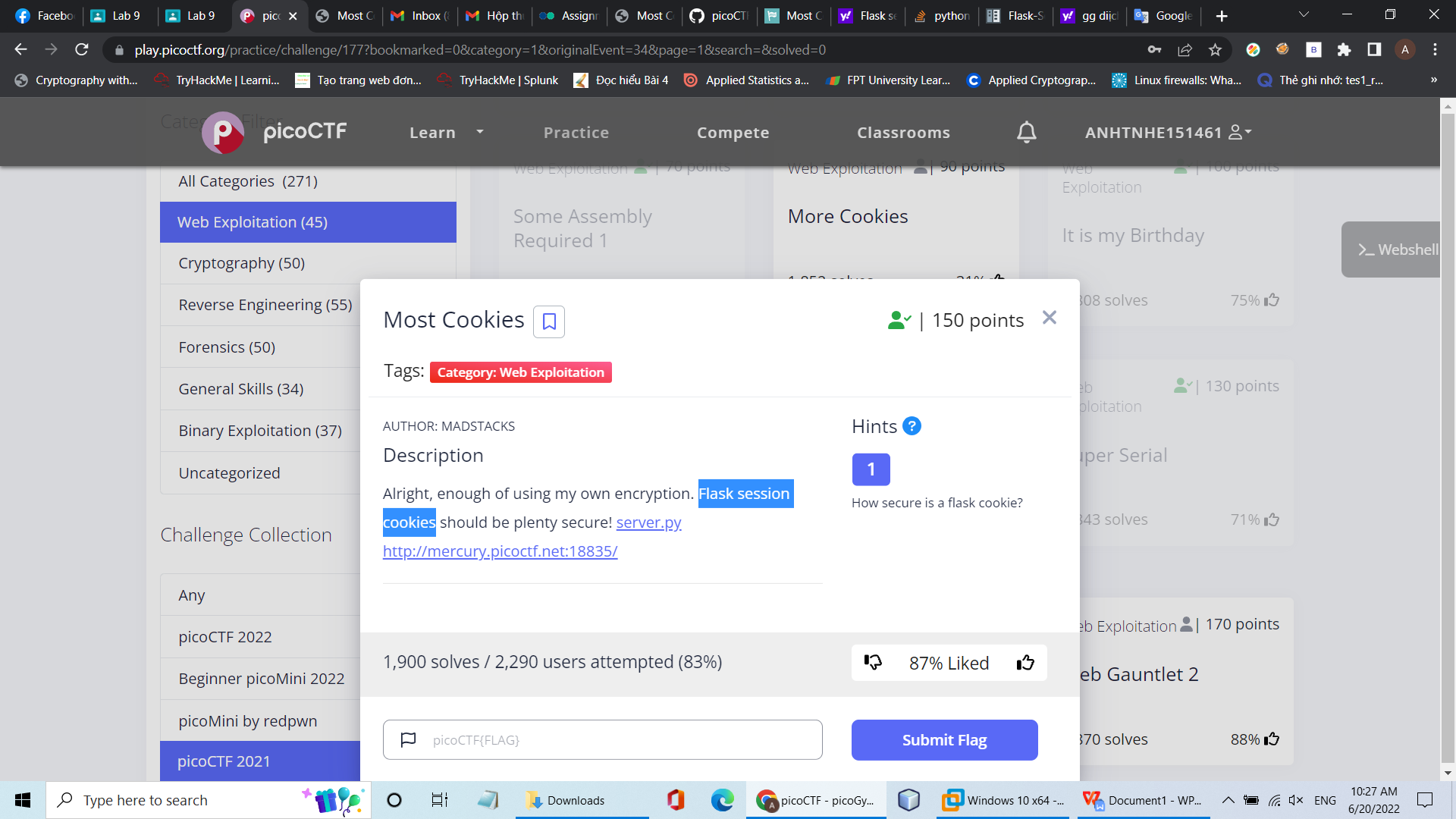
**Lab-Project 9: PicoCTF**

**Write up for Most Cookies challenge (Web Exploitation)**

- Mở đầu challenge , chúng ta đoán được ít nhiều về phần kiến thức được dùng ở đây là một trang web được xây dựng qua framework flask với ngôn ngữ Python về flask session cookie.



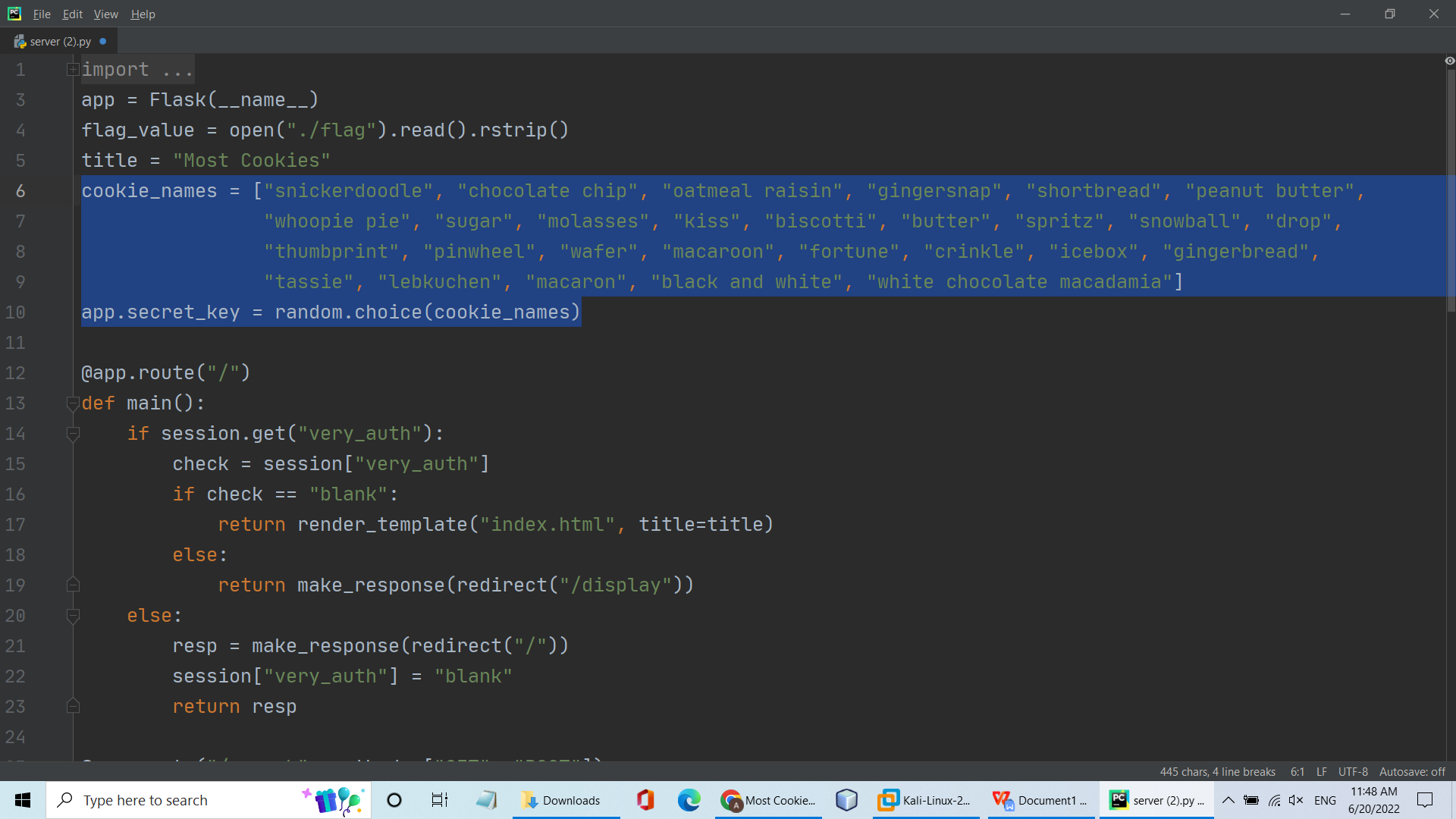
***- Vậy flask cookie là gì ?***

+ Trong flask, các cookie được liên kết với đối tượng. Yêu cầu làm đối tượng từ điển của tất cả các biến cookie và các giá trị của chúng được ứng dụng ở máy client truyền đi.

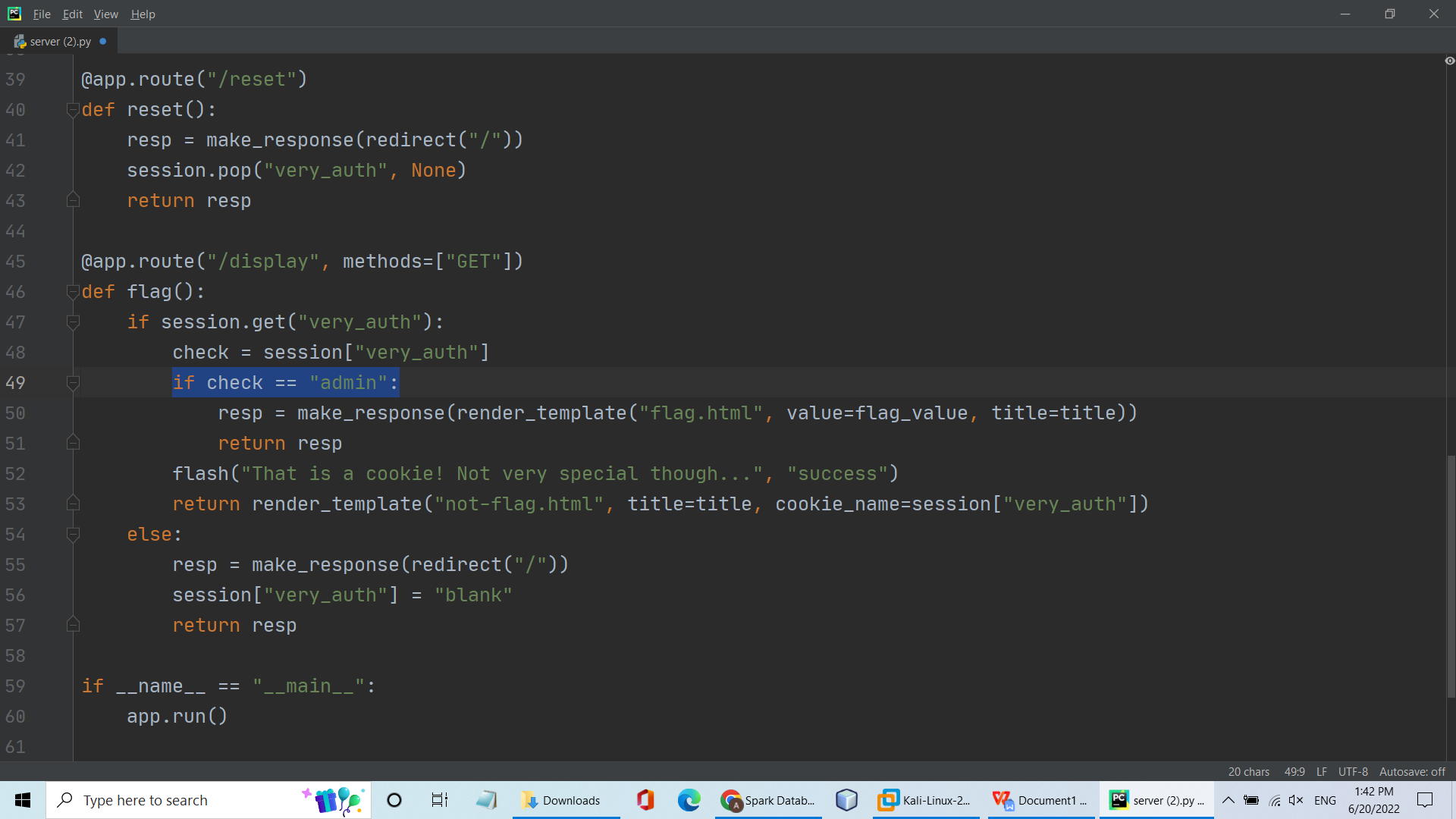
+ Bất kỳ dữ liệu nào bạn ghi vào phiên sẽ được ghi vào cookie và được gửi đến máy khách để lưu trữ. Máy khách sẽ gửi cookie trở lại máy chủ với mọi yêu cầu, đó là cách dữ liệu bạn viết trong phiên vẫn có sẵn trong các yêu cầu tiếp theo. Dữ liệu được lưu trữ trong cookie được ký mã hóa để ngăn chặn bất kỳ sự giả mạo nào.

+ Tuy nhiên , dữ liệu vẫn hiển thị cho bất kỳ ai biết cách xem, vì vậy bạn không bao giờ nên viết thông tin nhạy cảm trong phiên phía máy client.

- Sau khi biết được flask cookie rồi ta phân tích đến file server.py mà đề bài cho .

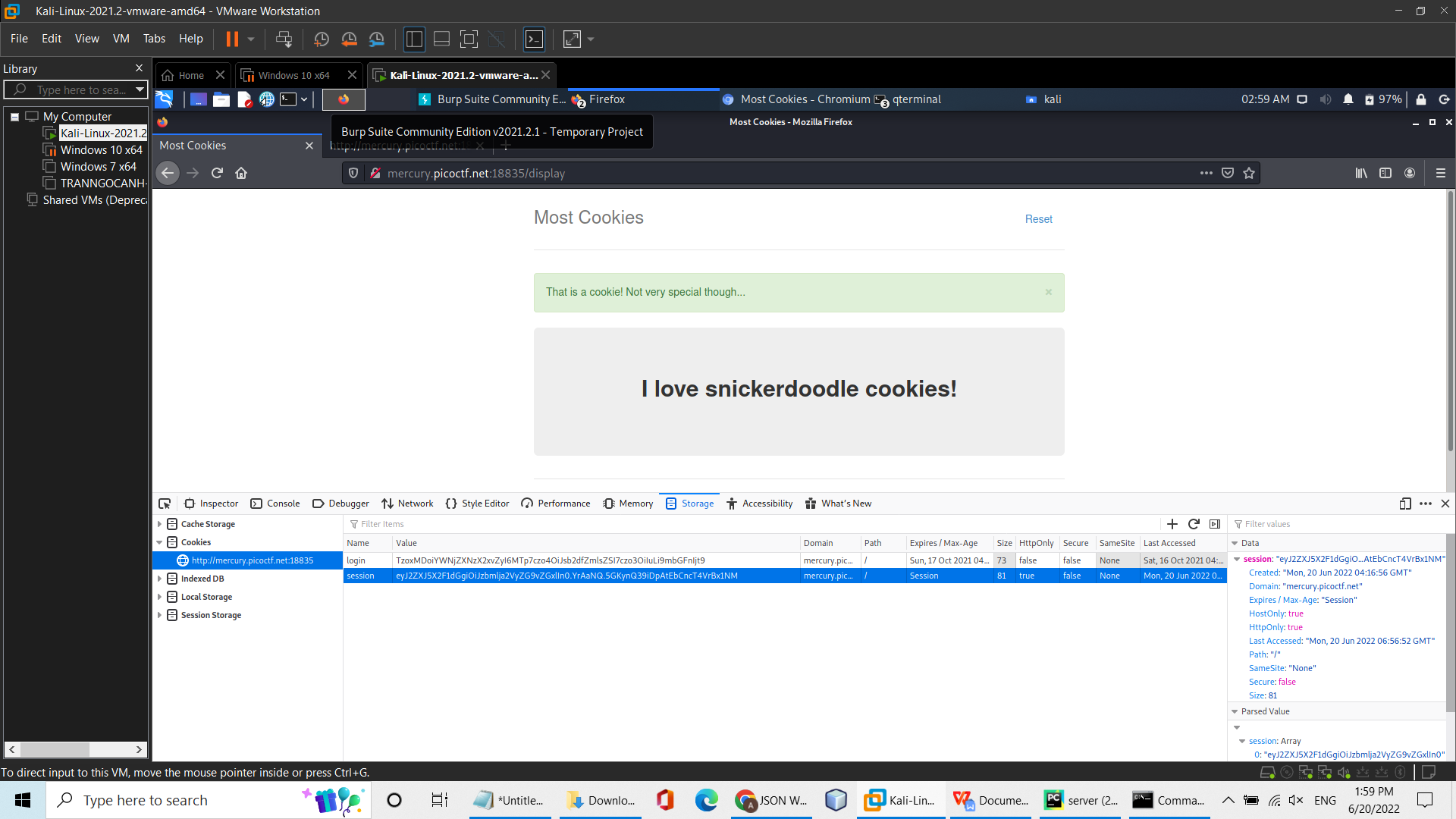


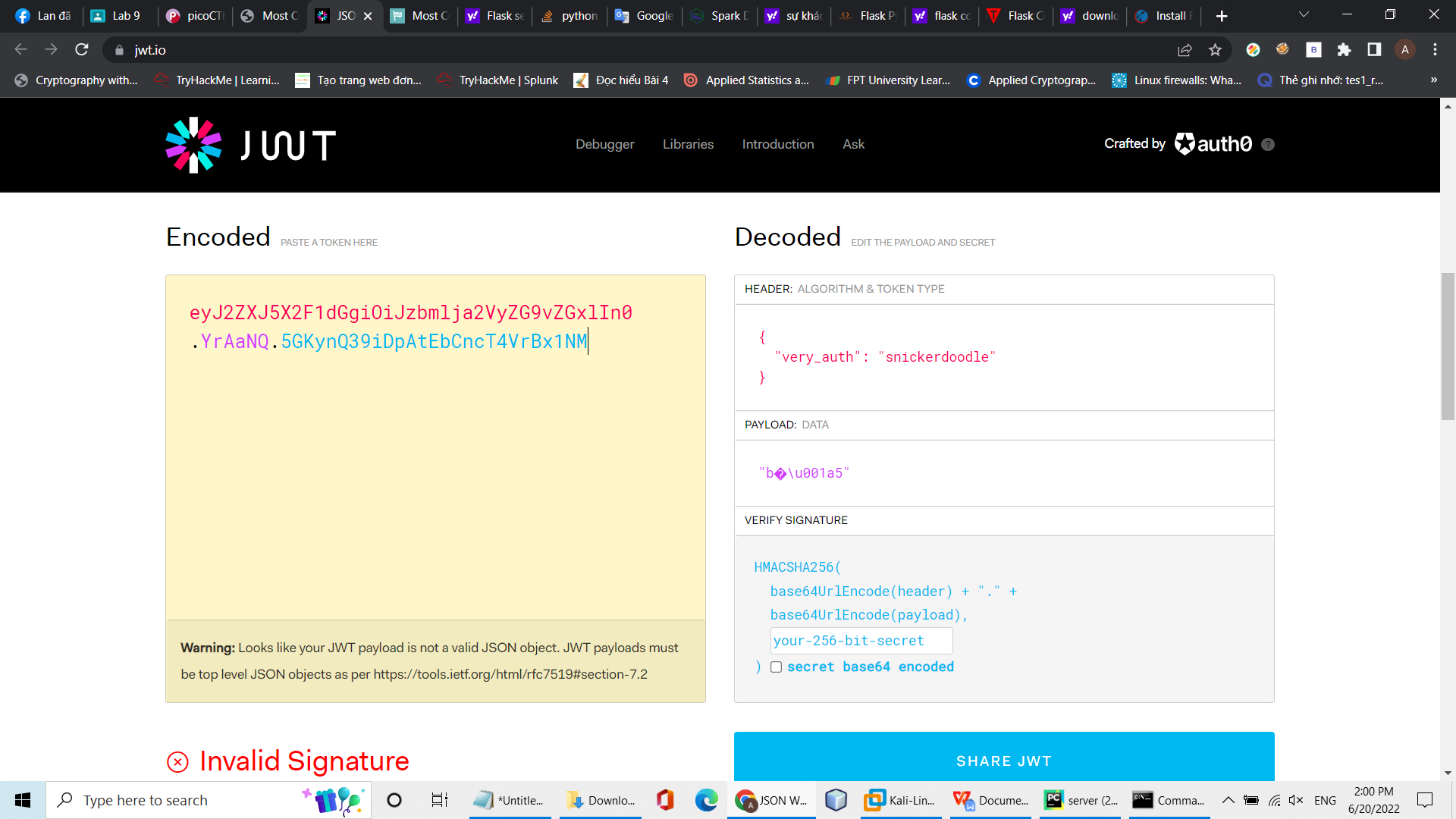
- Ở đây khóa bí mật được random trong danh sách cookie\_names bên trên. Nếu cái session bằng với “admin” thì sẽ lấy được flag và giải quyết được challenge này. Chính vì vậy ta phải làm sao để store được {"very\_auth": "admin"} trong cookie của client là ok .



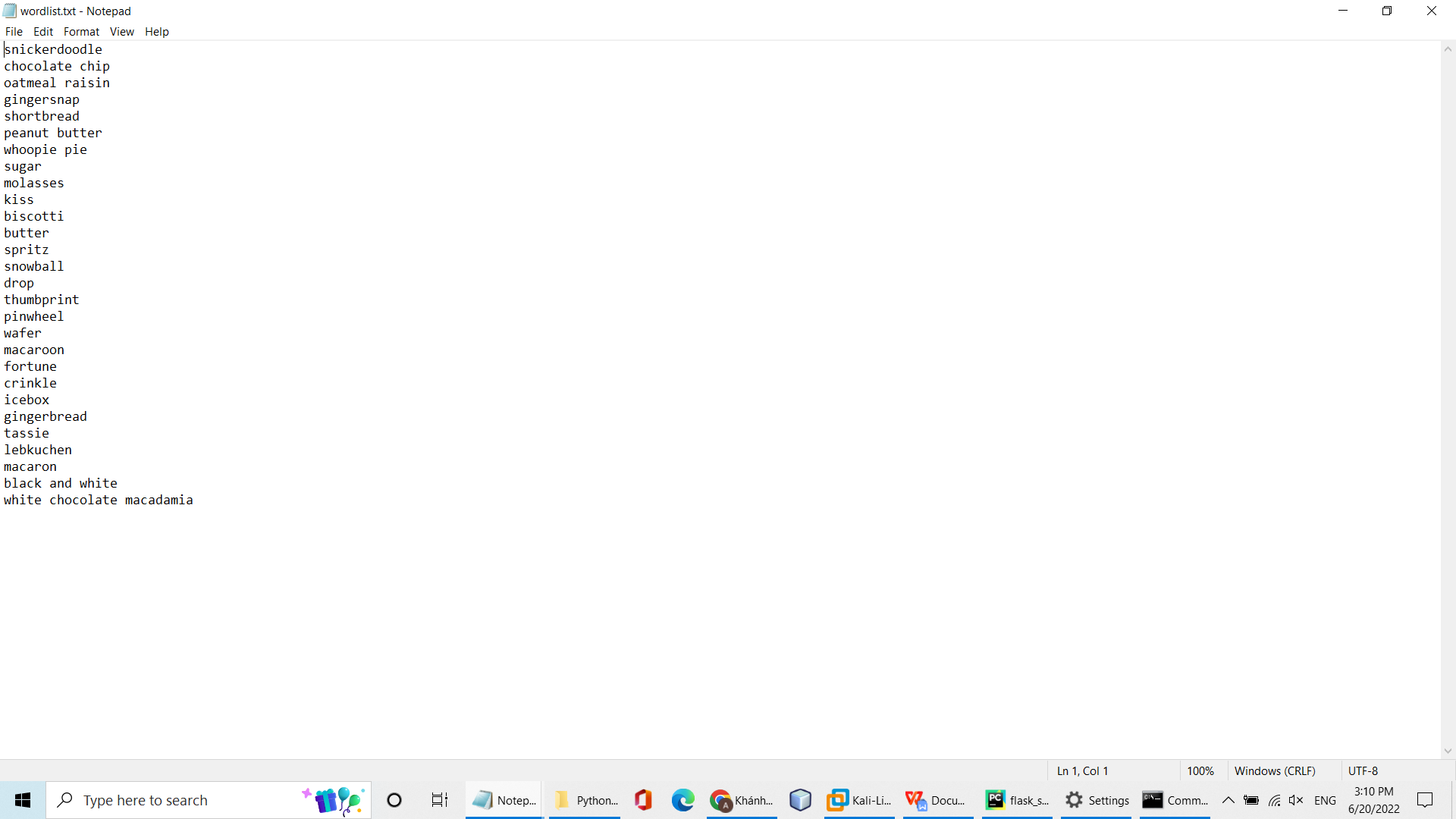
- Lấy cookie trong trang web và đưa sang jwt để decode thì thấy được snickerdoodle thông qua cookie đó.

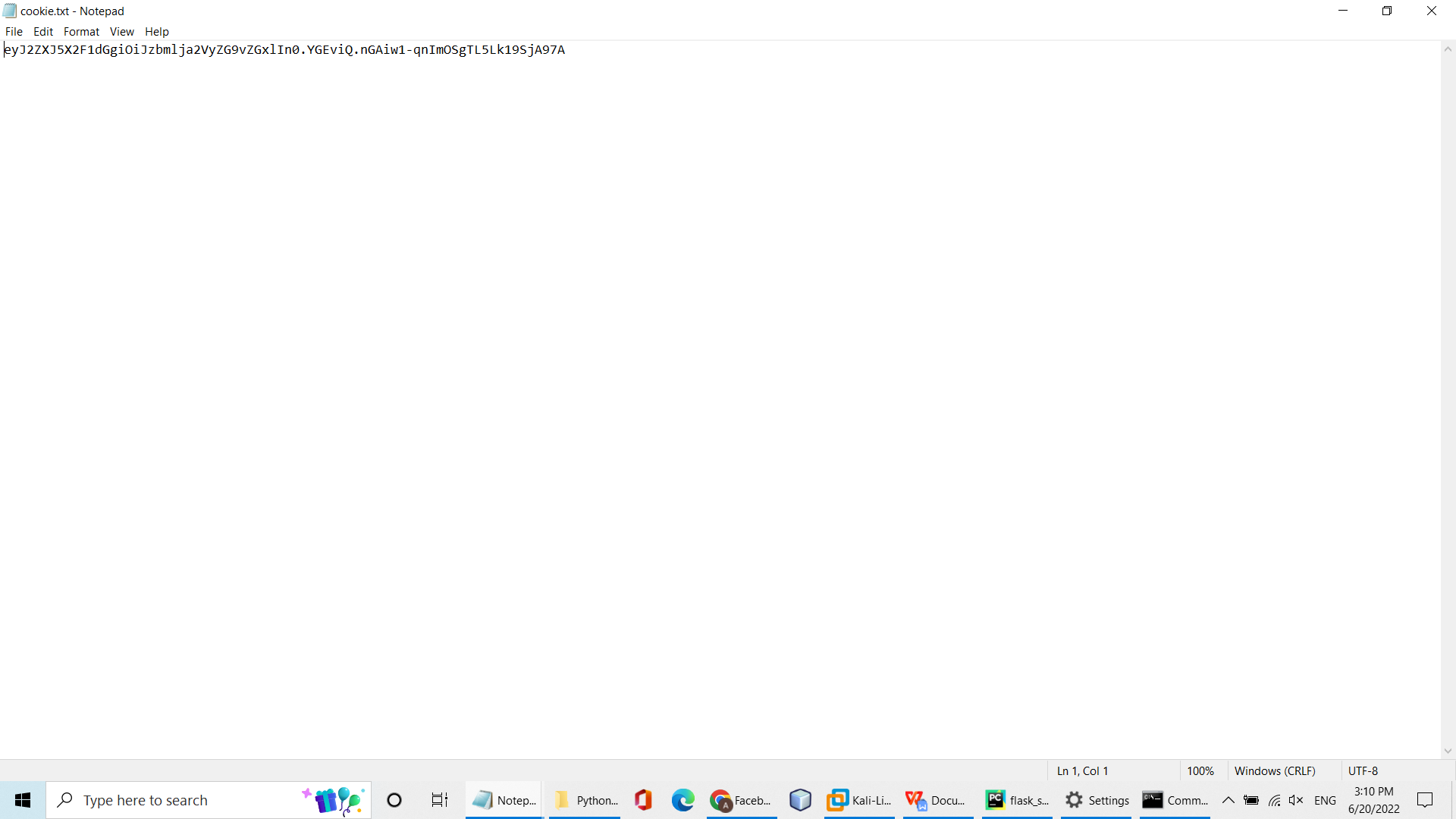
- Vì vậy trước khi store được “admin” trong cookie thì chúng ta phải đi tìm secret key trước (ở đây được dùng để encoded cookie\_name) .

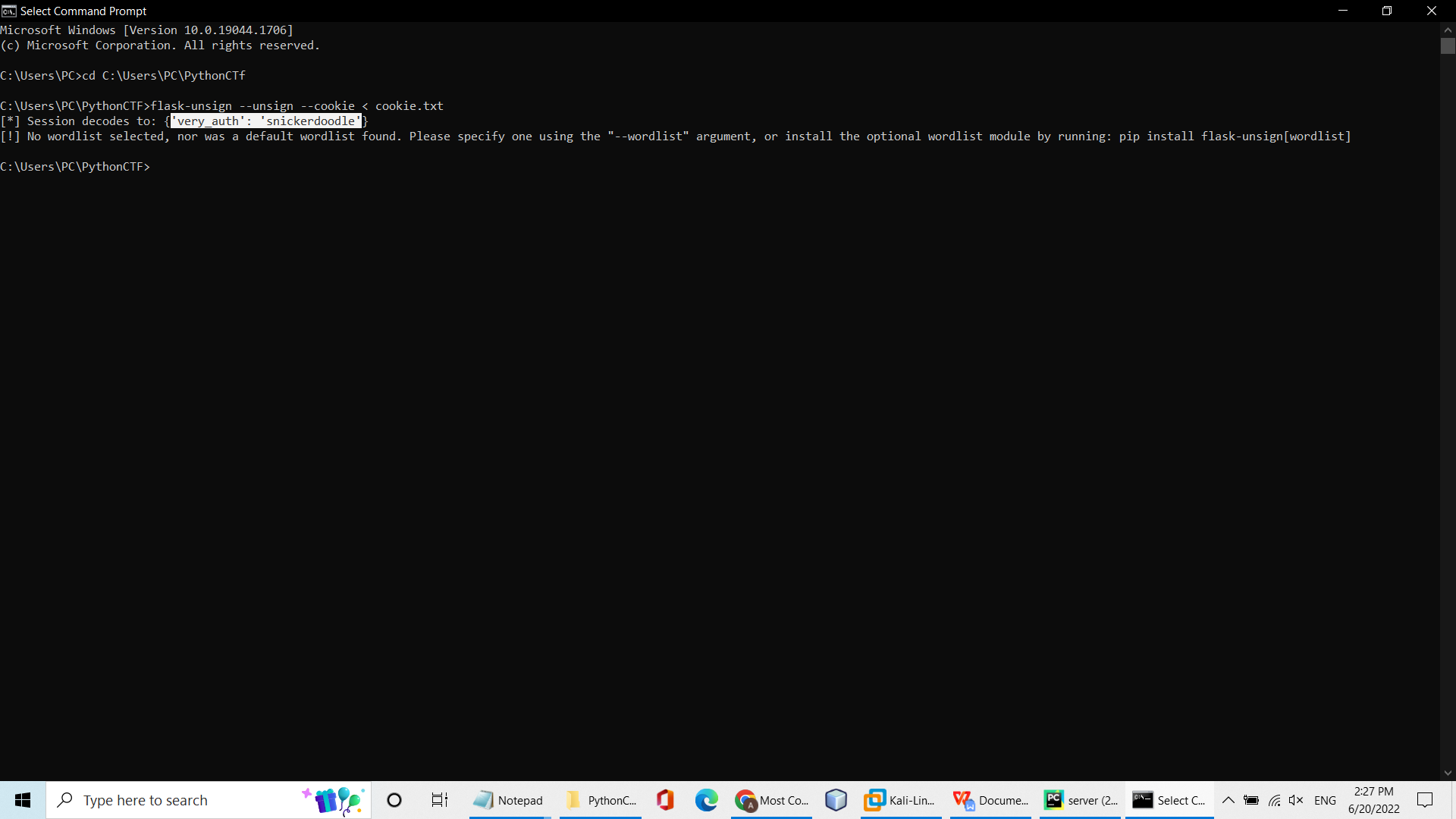


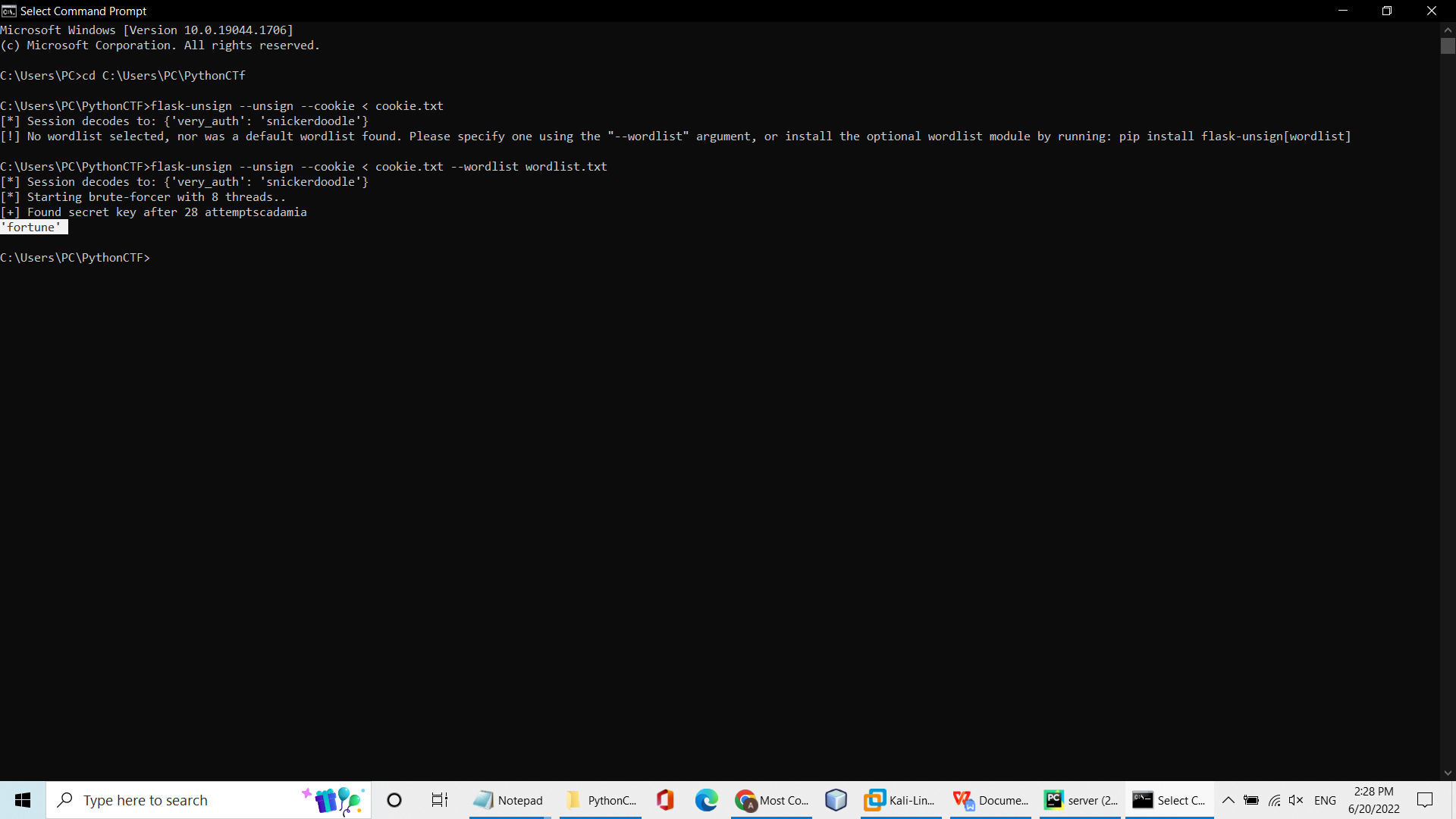


- Dùng flask unsign để duyệt hết cái danh sách wordlist.txt để tìm được ra secret key là “fortune”.

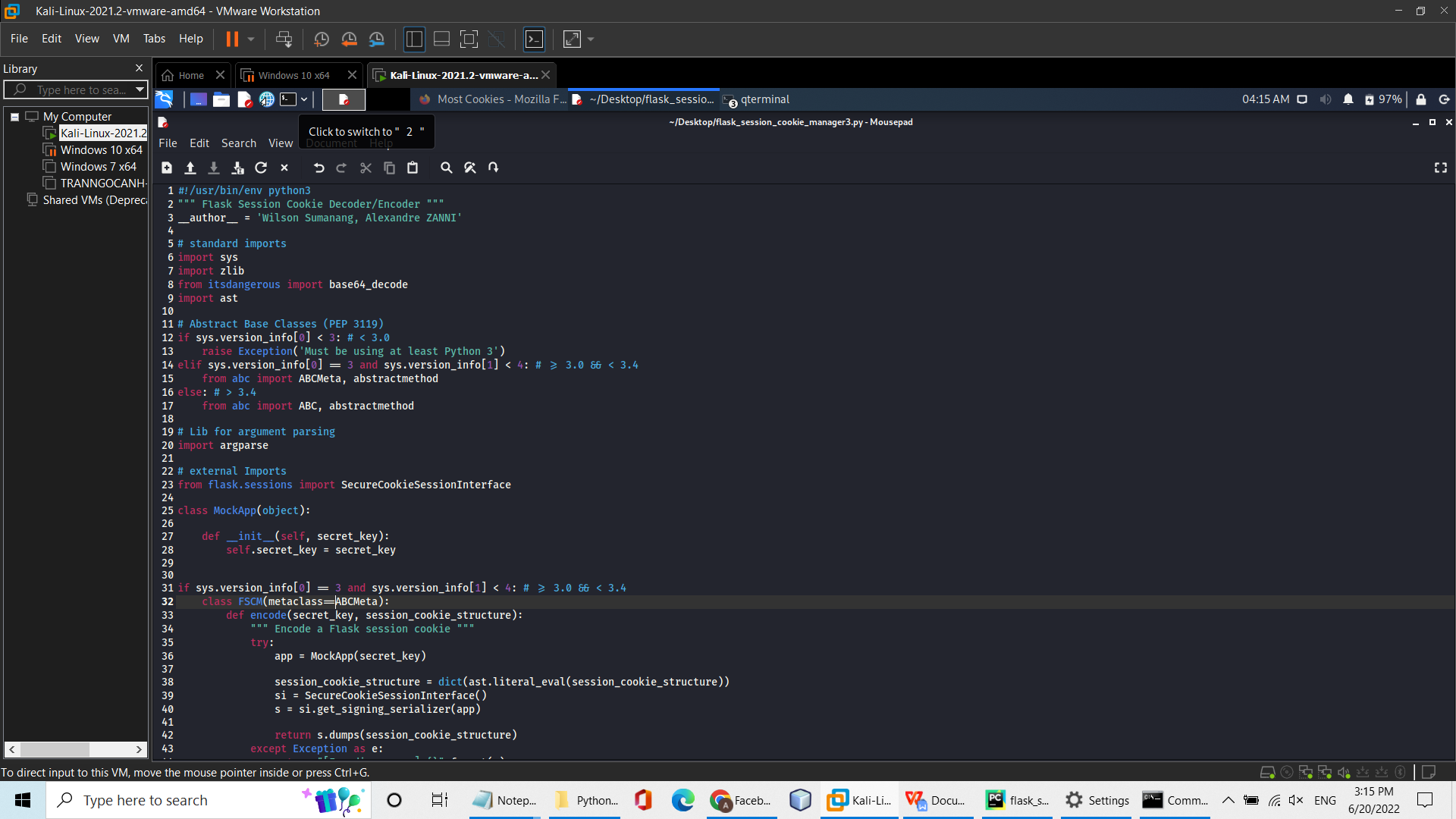


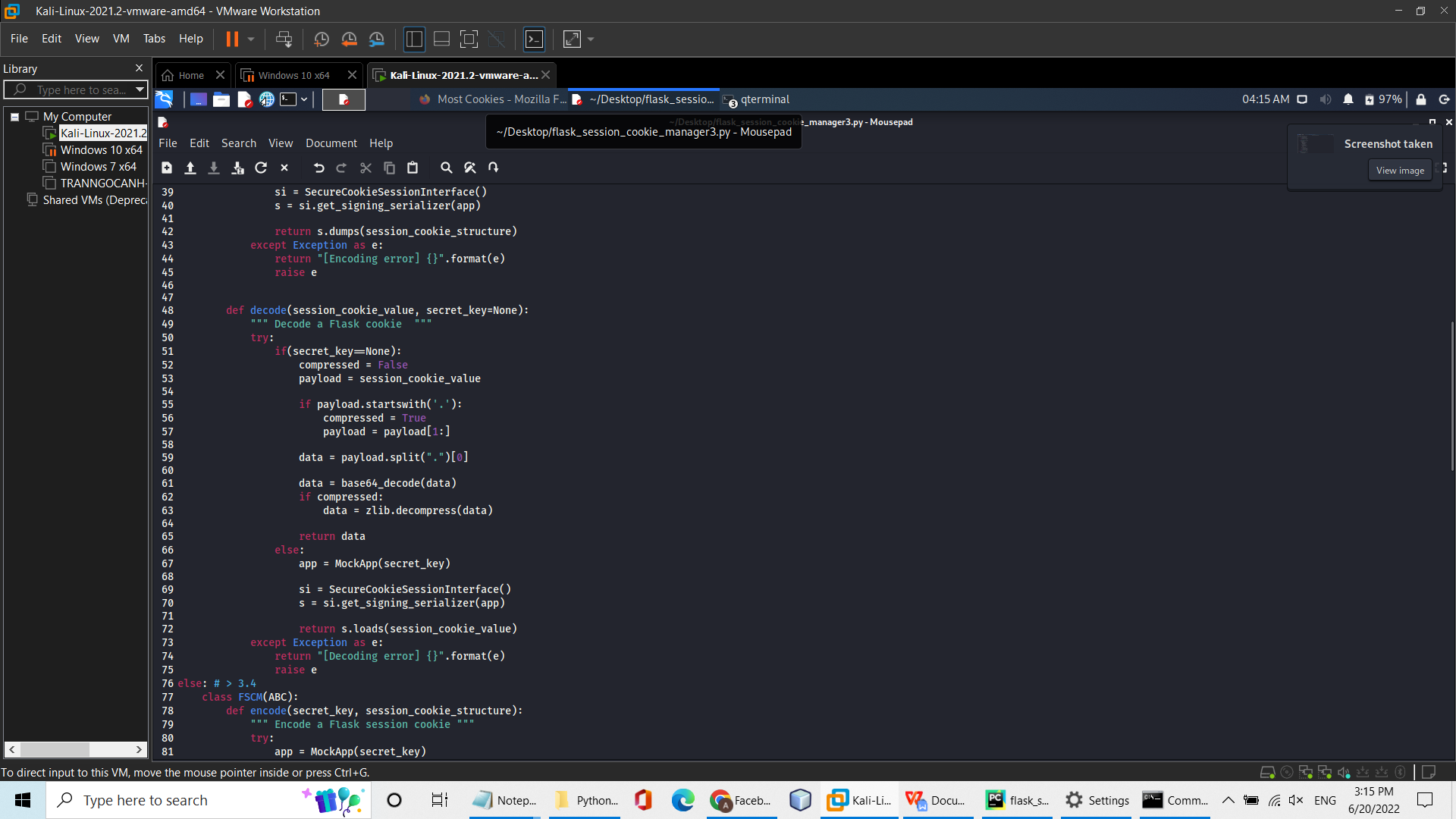


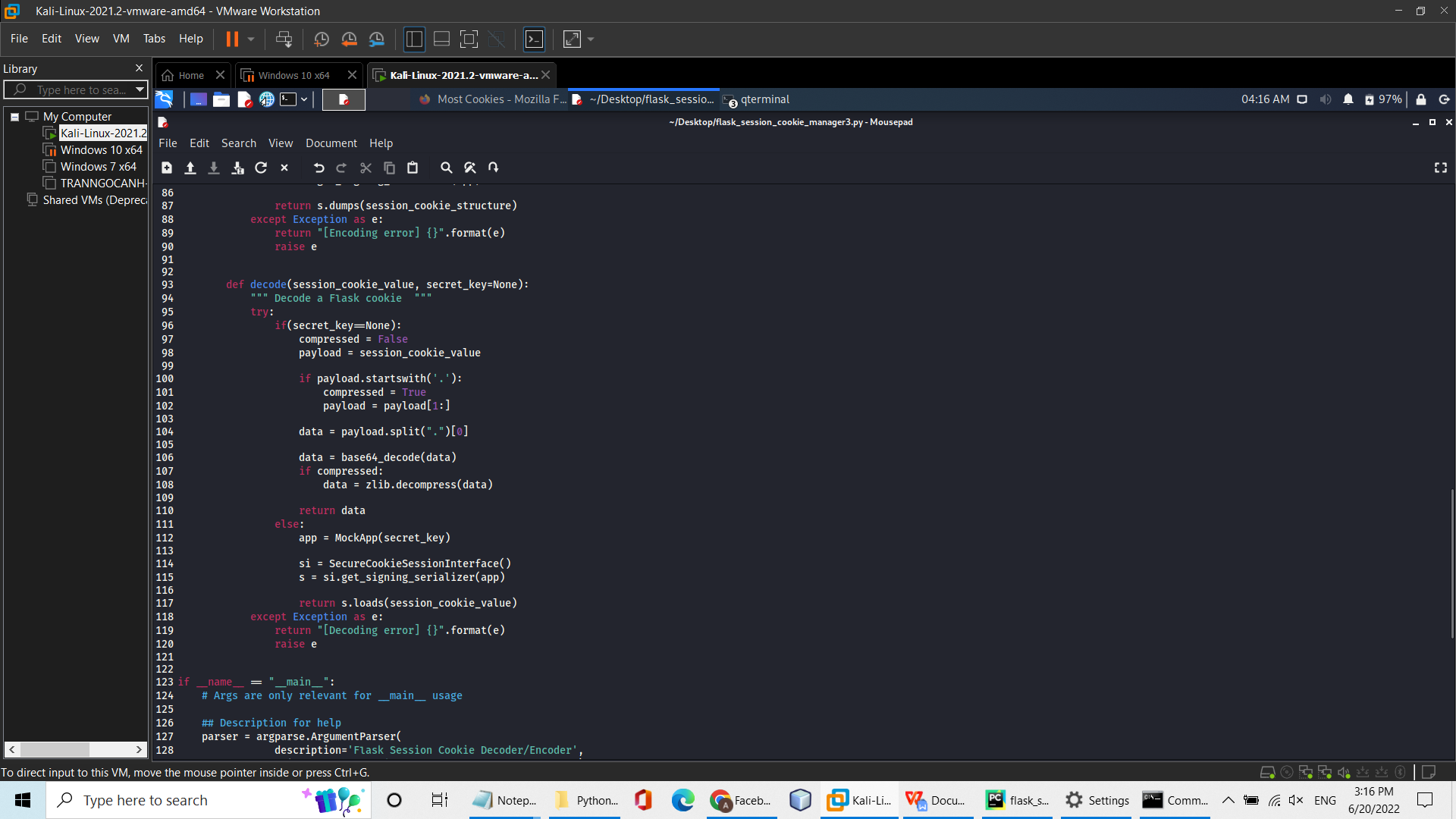


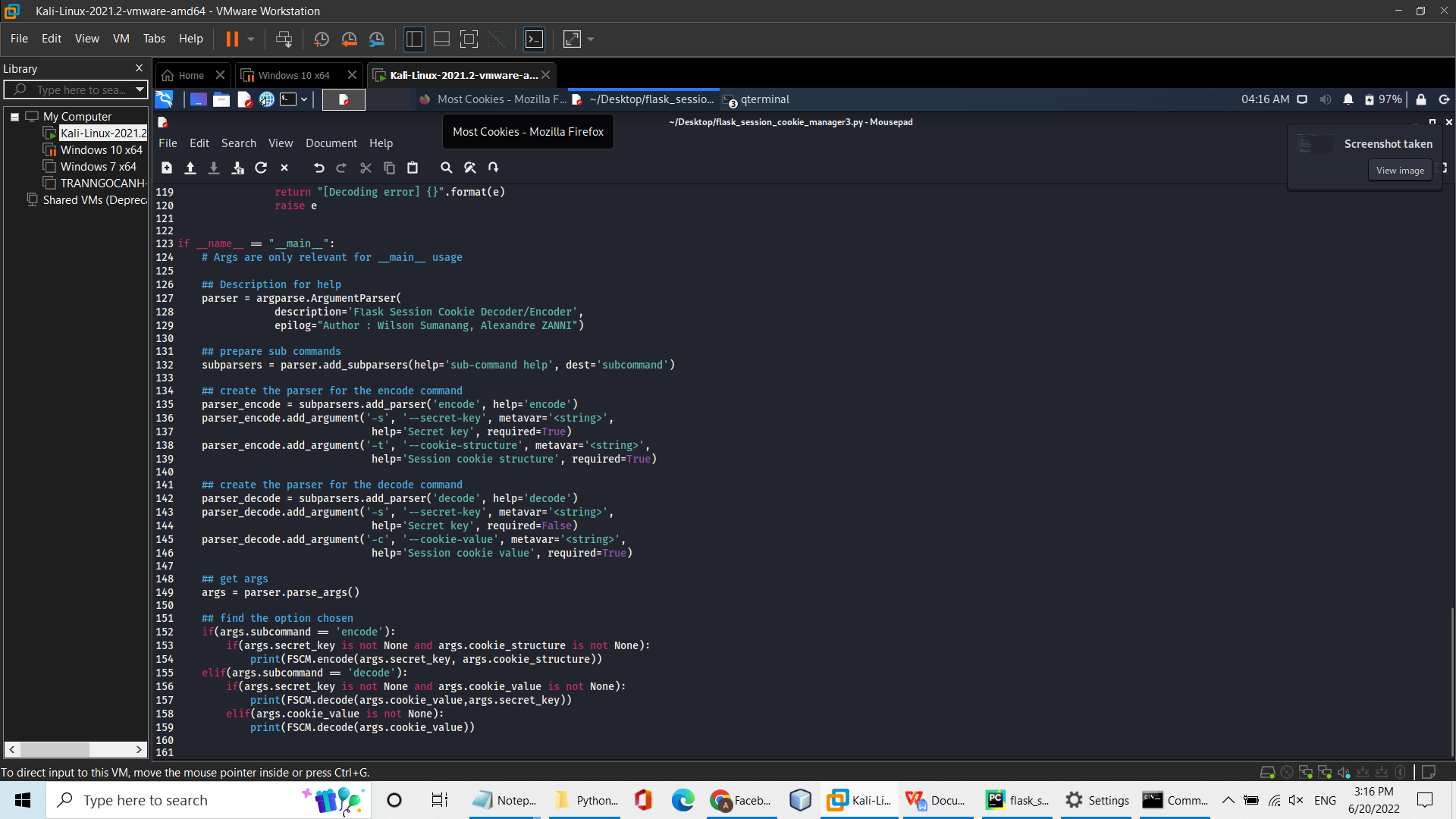


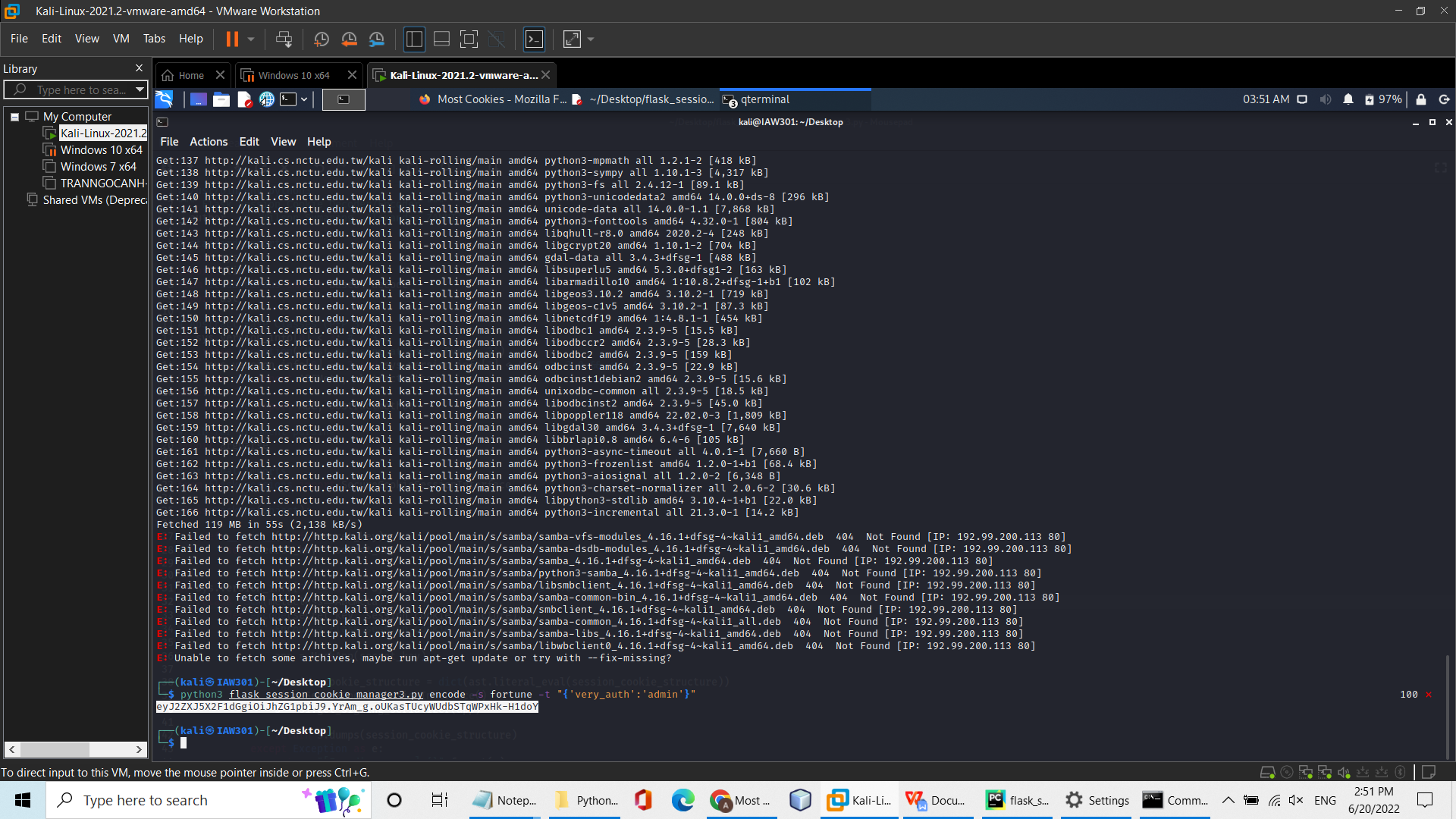
- Sau khi có secret key là “fortune” thì chúng ta chỉ cần việc chạy script để encoded {"very\_auth": "admin"} bằng key trên là được.











- Sau khi có được cookie encoded của {"very\_auth": "admin"} thì chúng ta chỉ việc bỏ cookie đó thay thế cho cookie cũ và refresh lại trang web vậy là đã solve được challenge !!!

eyJ2ZXJ5X2F1dGgiOiJhZG1pbiJ9.YrAm\_g.oUKasTUcyWUdbSTqWPxHk-H1doY

