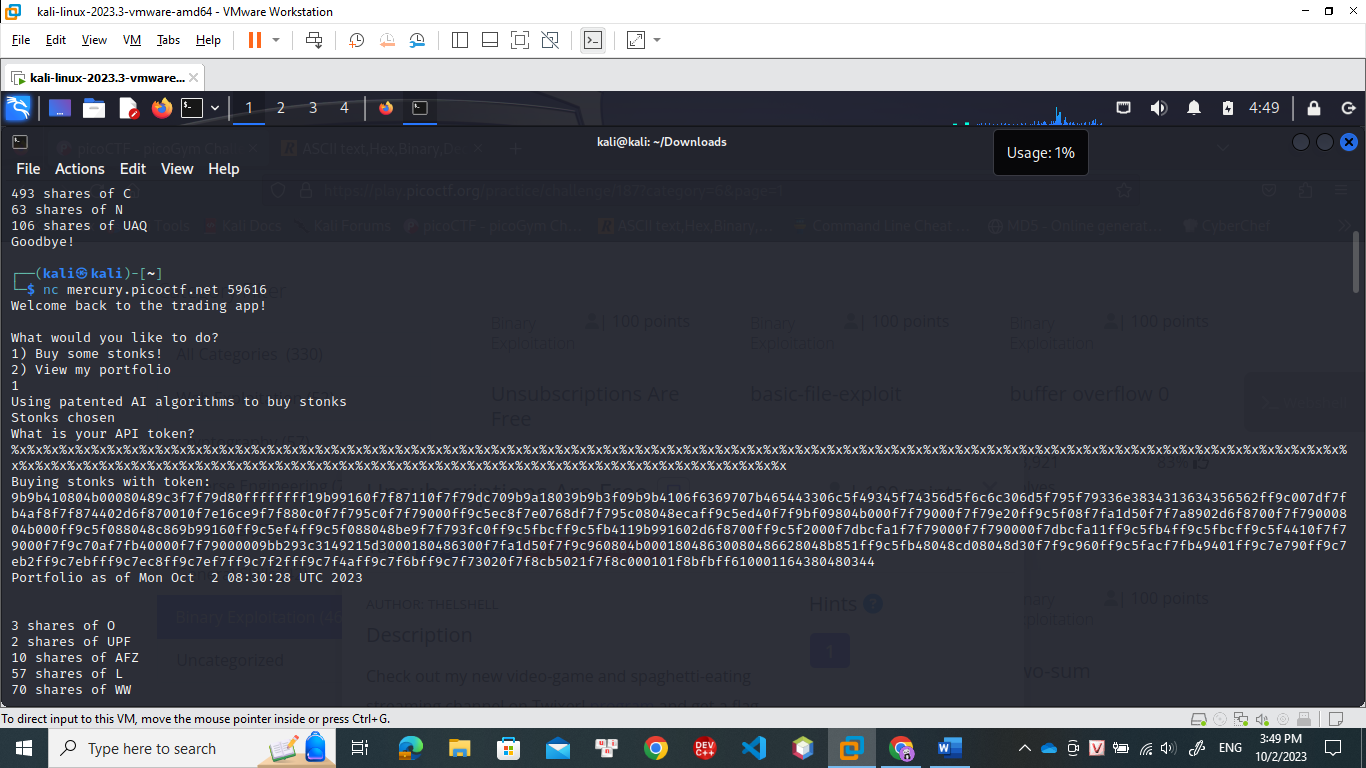
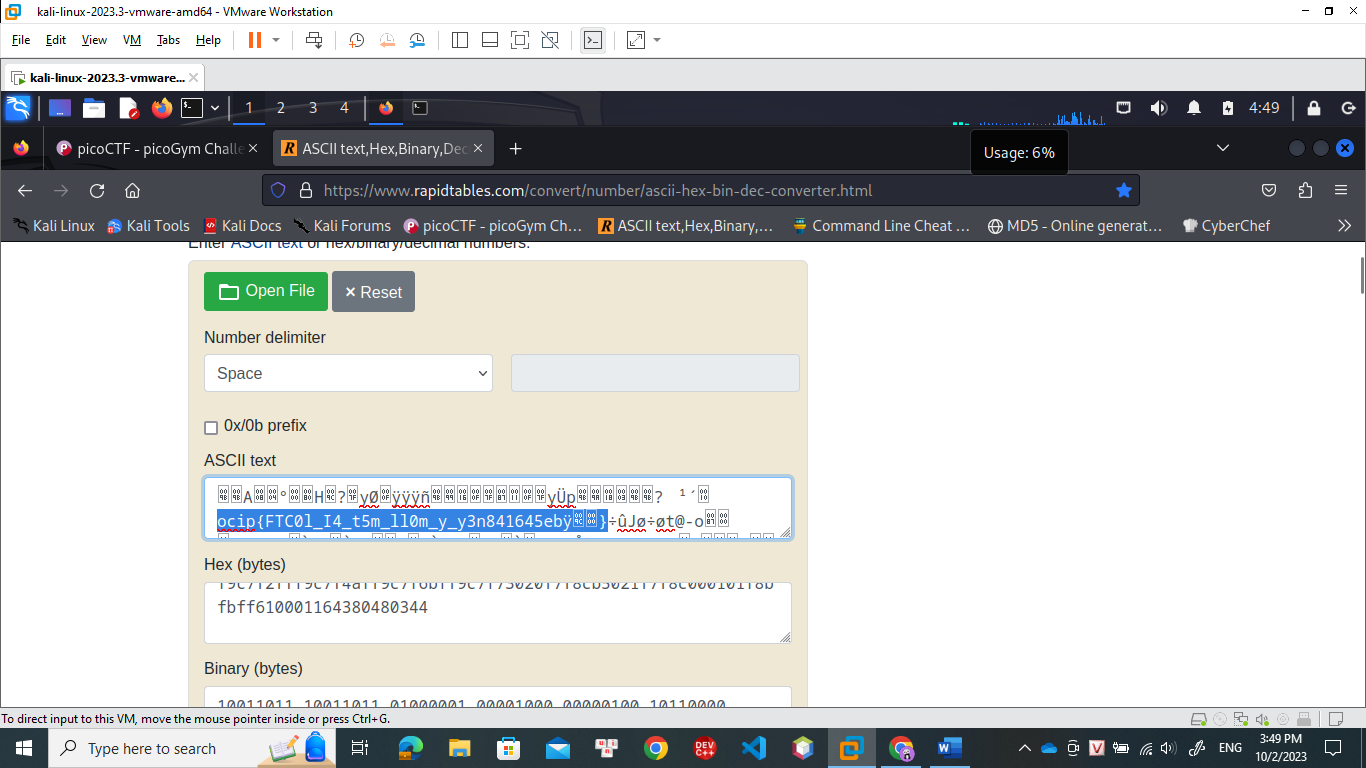
1. **Stonks**

* Đây là lỗ hổng định dạng chuỗi.
* Cờ được giấu trong Stack, cần lôi nó ra.
* Trong Stack, mỗi ô lưu trữ 4 bytes, tương ứng với 1 ký tự là 1 byte.
* Khi cho cờ vào trong Stack, cụm 4 ký tự 1 sẽ bị đảo ngược, do đó cần in ngược lại mỗi lần 4 ký tự rồi nối vào thì sẽ lấy được cờ ban đầu.
* netcat theo đề bài
* Nhấn 1 để chọn mua cổ phiếu
* Nhập API token (API token là 1 chuỗi ký tự được sử dụng để xác thực và ủy quyền truy cập cho 1 ứng dụng hoặc người dùng khi giao tiếp với 1 API)
* Để lấy được cờ (dạng đảo ngược), trước hết phải nhập %x (để hiển thị 1 biến số nguyên không dấu dưới dạng số hexa 4 byte), tức là mỗi ô trong Stack lưu trữ 1 định dạng %x và giờ chúng ta cần xem mỗi ô đó chứa 4 ký tự hexa nào.
* Nhập càng nhiều %x càng tốt vì không biết rằng cờ sẽ nằm ở đầu, giữa hay sâu trong stack

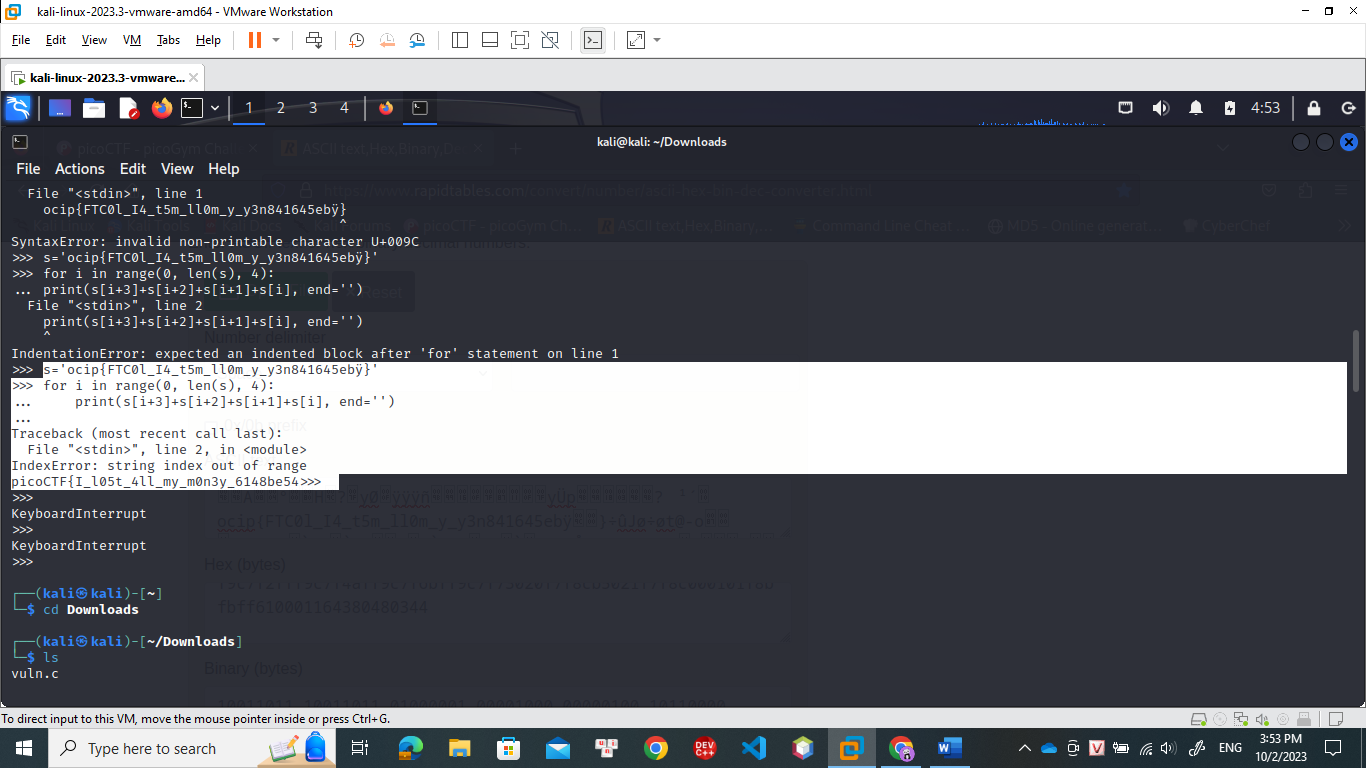


* Sau khi có được đoạn mã hexa, cần chuyển nó sang mã ASCII



Ta đã thấy được cờ dạng đảo ngược ở đây

* Để reverse lại cờ, sử dụng code python trong terminal, đặt s là chuỗi cờ đảo ngược, duyệt từ i=0 đến hết chiều dài s với bước nhảy là 4, in ra s[i+3]+s[i+2]+s[i+1]+s[i], end=’’. Tức là mỗi lần in ngược 4 ký tự và sau khi in xong (end) thì kết thúc là dấu nháy không có khoảng trắng (Việc này sẽ làm các lần in tiếp theo nối đuôi nhau cùng trên 1 dòng).



Đã tìm được cờ

* Bổ sung thêm dấu } ở cuối cờ rồi submit.