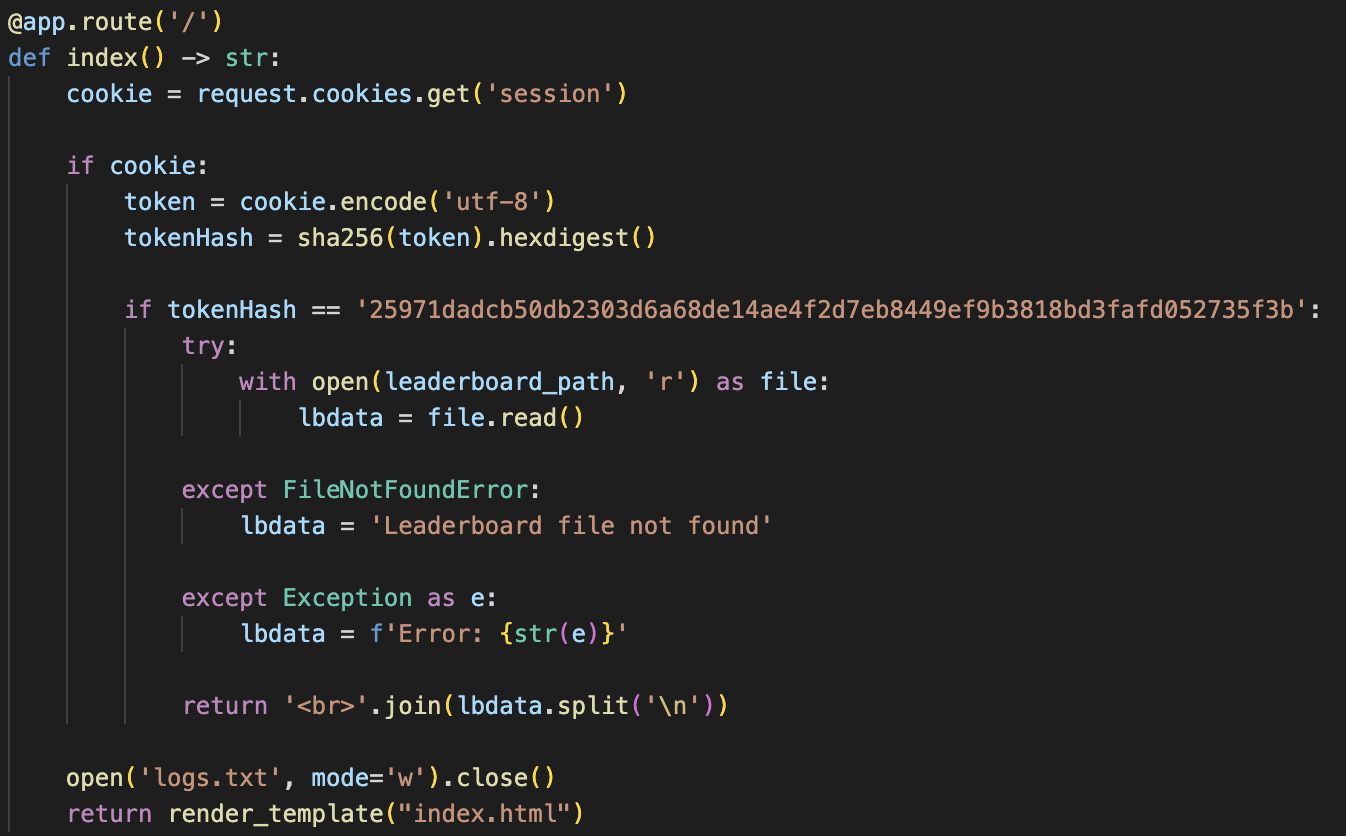
**Phân tích code (theo quan điểm của mình)**

**Trang chủ**



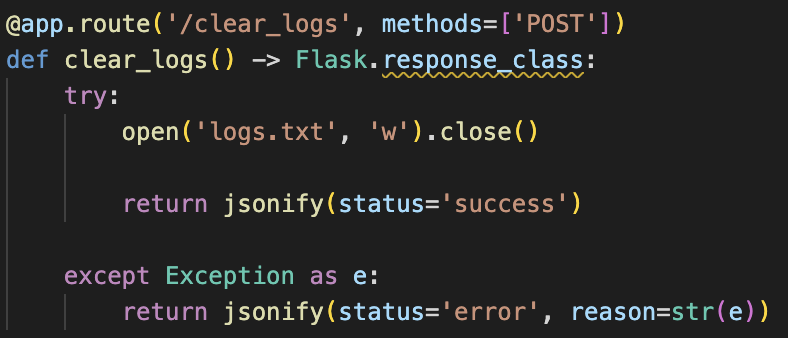
Lấy session trong biến COOKIE🡪sha256(token)

Nếu sha256(token) bằng hash đã cho, đọc file leaderboard.txt. Ngược lại, mở logs.txt và trả về trang index.html

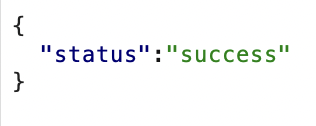
**/report**



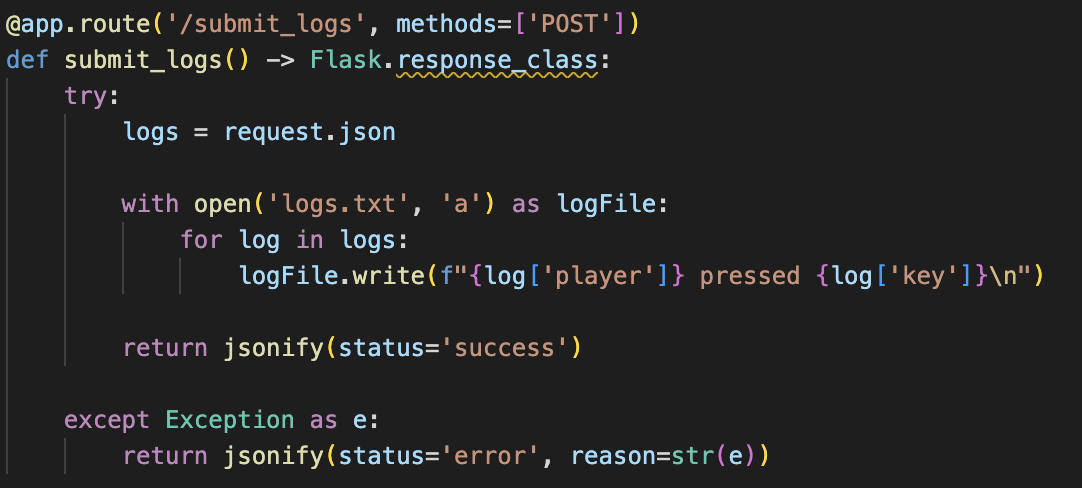
**/clear\_logs**



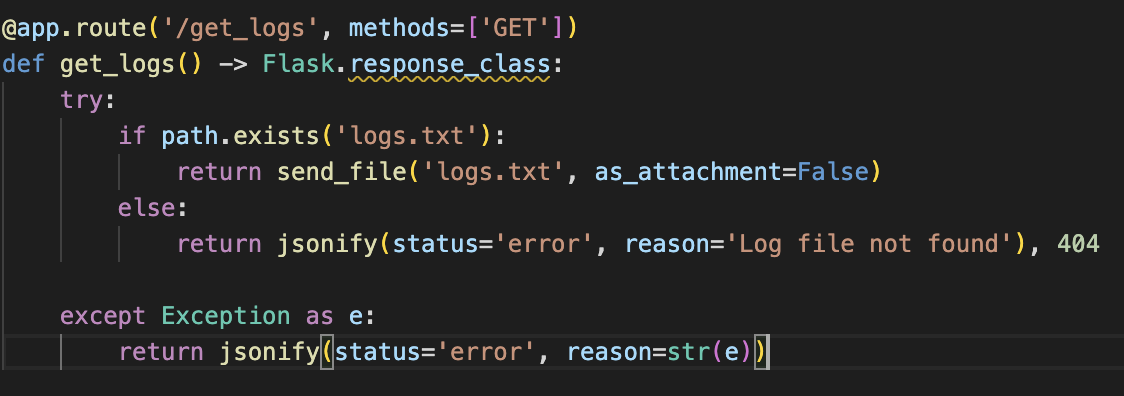
POST /clear\_logs

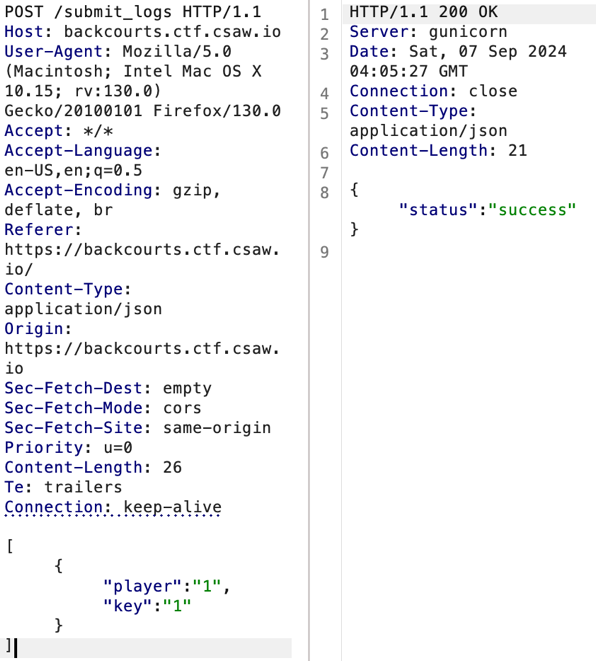
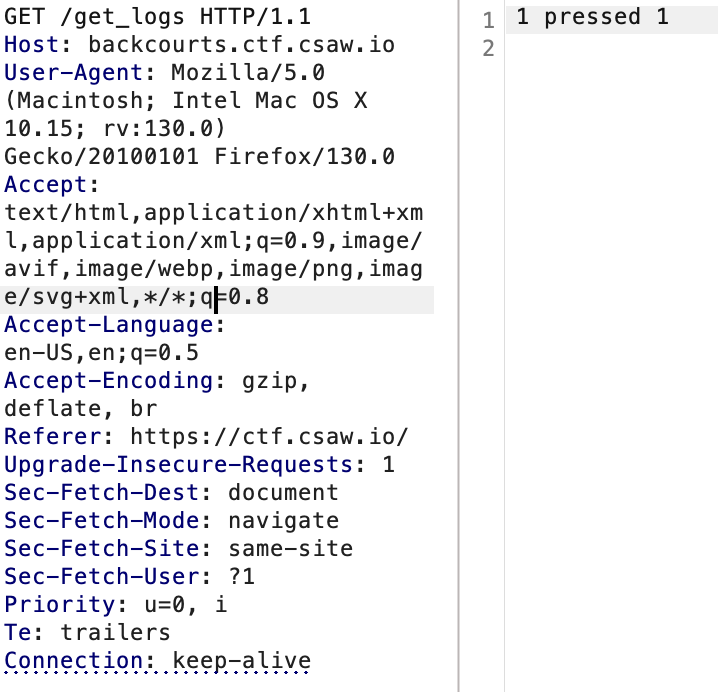


**/submit\_logs**

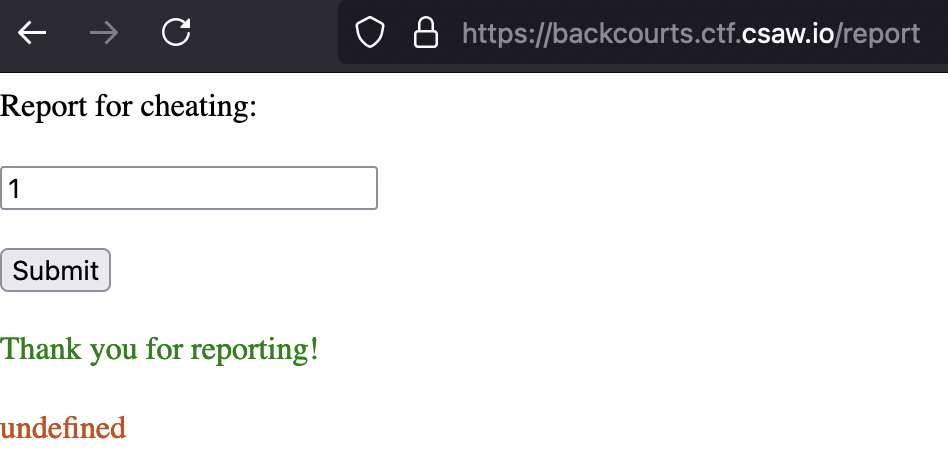


**/get\_logs**



Khi bạn report 1 player thì trang web sẽ /get\_moves và /get\_eval



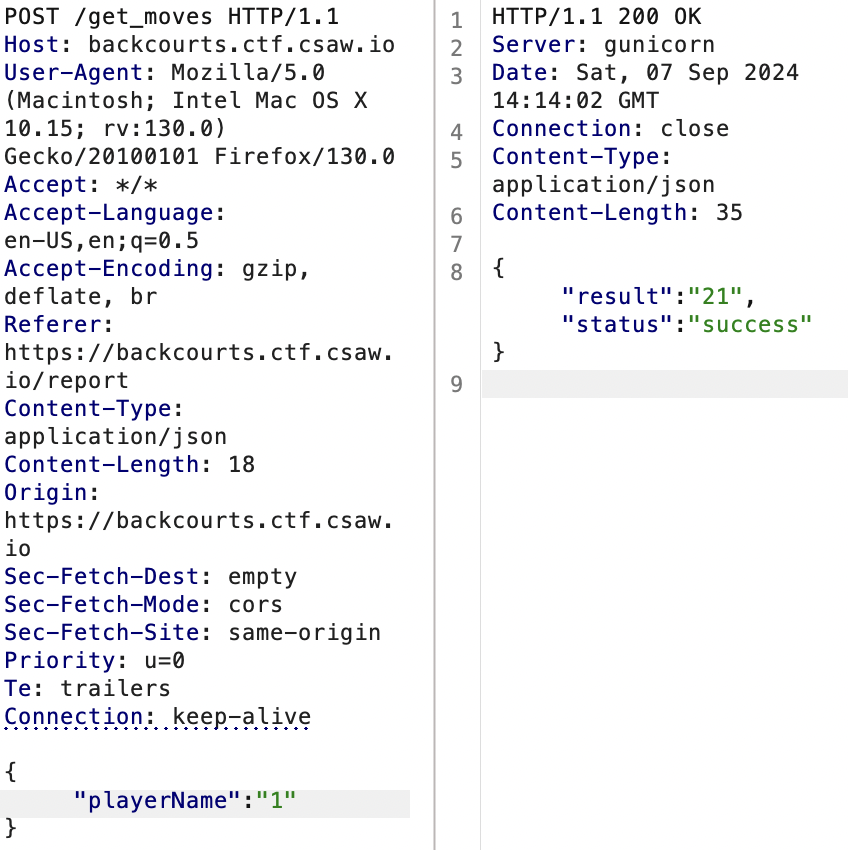
**/get\_moves**



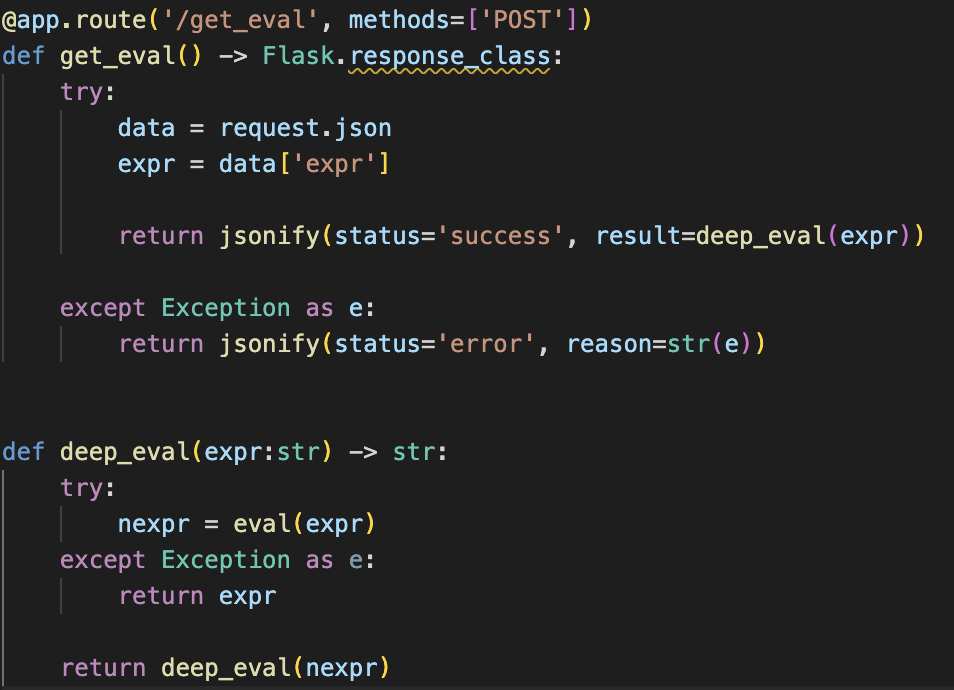
Bạn đã biết cách ghi log.txt, tuyến /get\_moves sẽ đếm số bước player di chuyển

1 pressed 2 (log.txt)

1 pressed 1



**/get\_eval**



Hàm get\_eval() cho phép bạn truyền vào 1 biểu thức expr, biểu thức lại truyền vào hàm deep\_eval(). Có 1 hàm nguy hiểm trong deep\_eval(): eval() nhưng nó là hàm đệ qui. Chạy xong hàm eval() lấy nexpr để chạy deep\_eval() lần 2, để thoát được vòng lặp này bạn phải kích hoạt được ngoại lệ.

eval("\_\_import\_\_('os').popen('cat leaderboard.txt').read()")

**Flag: csawctf{5H1774K3\_Mu5Hr00M5\_1\_fuX0R3d\_Up\_50n\_0F\_4\_81207CH}**