Mức độ đề: 200

Trang web có chức năng:

Input text

Chức năng bị lỗi:

Input text

Chức năng này bị lỗi như nào:

Payload được gửi đến server, server xử lý payload và có thể brute force từng kí tự flag

Cách khai thác:

Tại server có được file flag.html và thẻ input có flag



File flag.html có thẻ link với input css được nhập từ người dùng.

Và input này có thể là 1 file css. Trong file shell.css sẽ chứa payload brute force từng kí tự trong thẻ input chứa flag

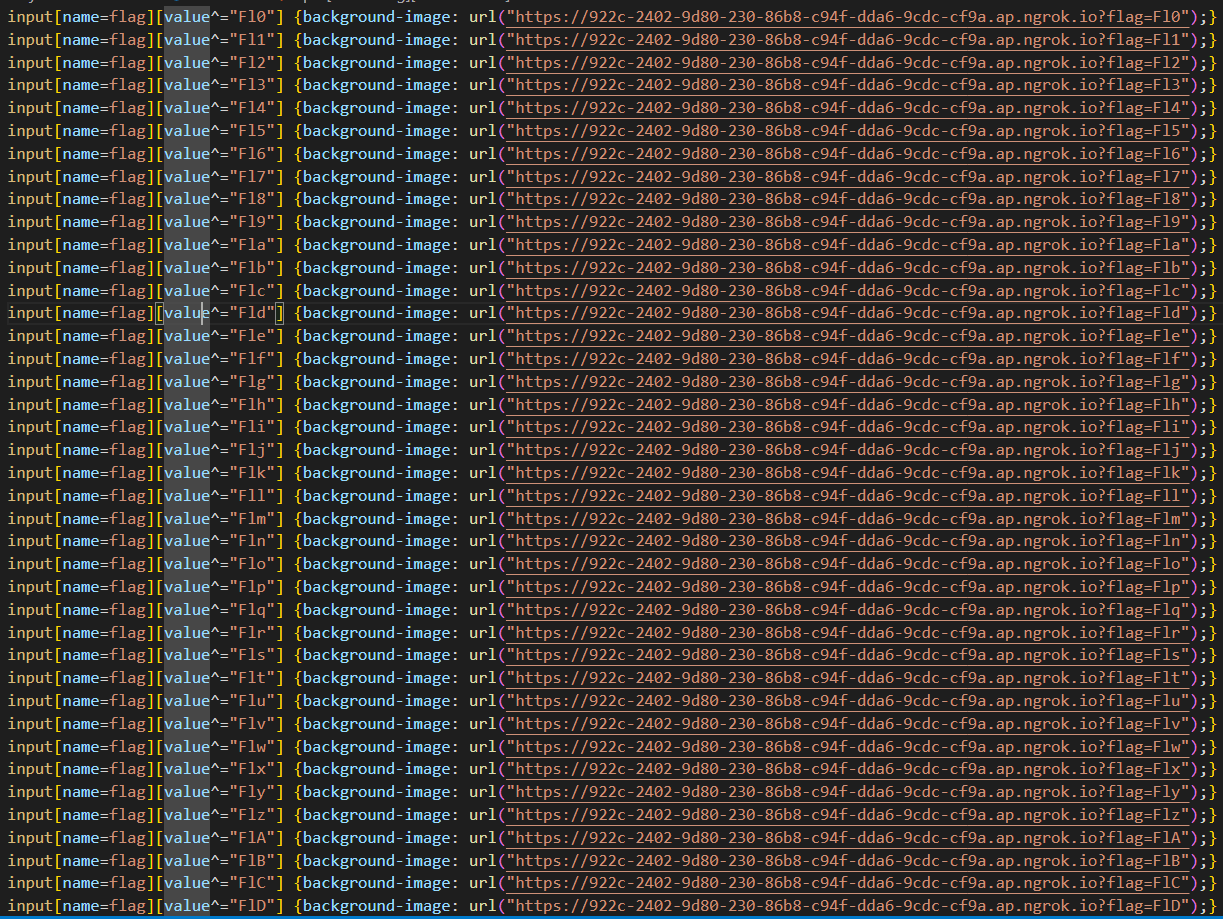
File solve.py



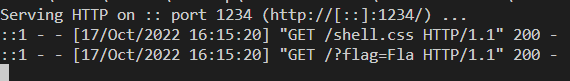
Run file solve



File shell.css sẽ có được



Brute flag sẽ được lưu trong log



Brute cho đến khi nhận được flag