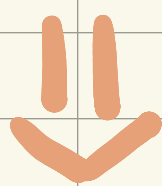
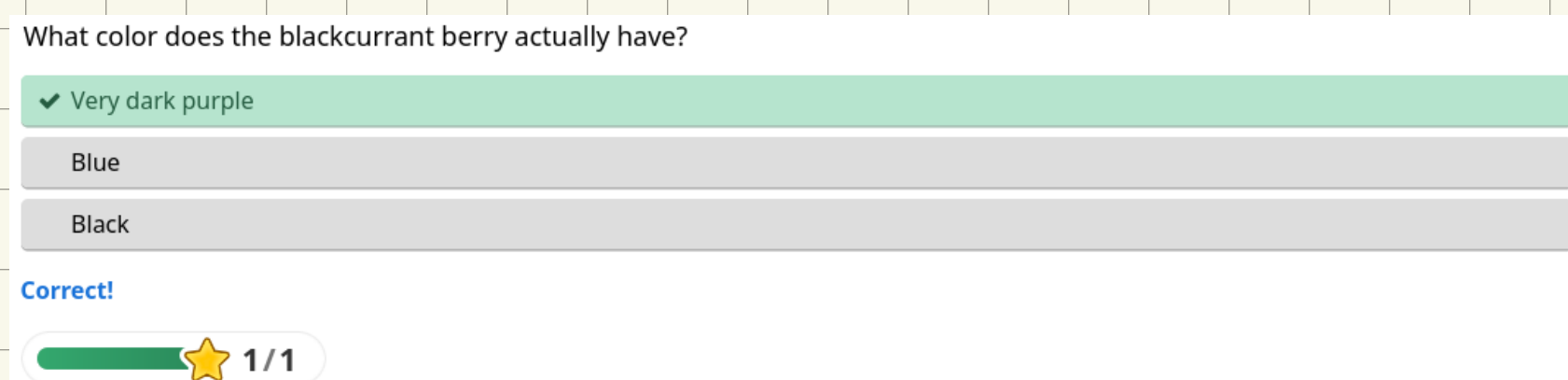


# Giải thích cách lms360hack.pages.dev hoạt động.

by HiennNek

- Đầu tiên, chúng ta phải biết rằng LMS360 sử dụng H5P làm Engine để render và xử lý bài giảng và bài tập trên trang web
- Qua code example của H5P trên h5p.org thì đáp án của H5P được hiển thị như sau:



- Trong ví dụ này, chúng ta có thể thấy rằng là những câu trả lời có giá trị "correct" là "true" sẽ là (những) đáp án đúng; và ngược lại với "false"

"Vậy thì ta tìm cái file mà có chứa đáp án là được đúng không?"

- Um, đúng đấy, trong ví dụ của H5P thì cả file đó và đáp án được lưu trong phần `<script>` của website.

```
'{"answers":[{"correct":true,"text":"<div>Very dark purple</div>"}
```

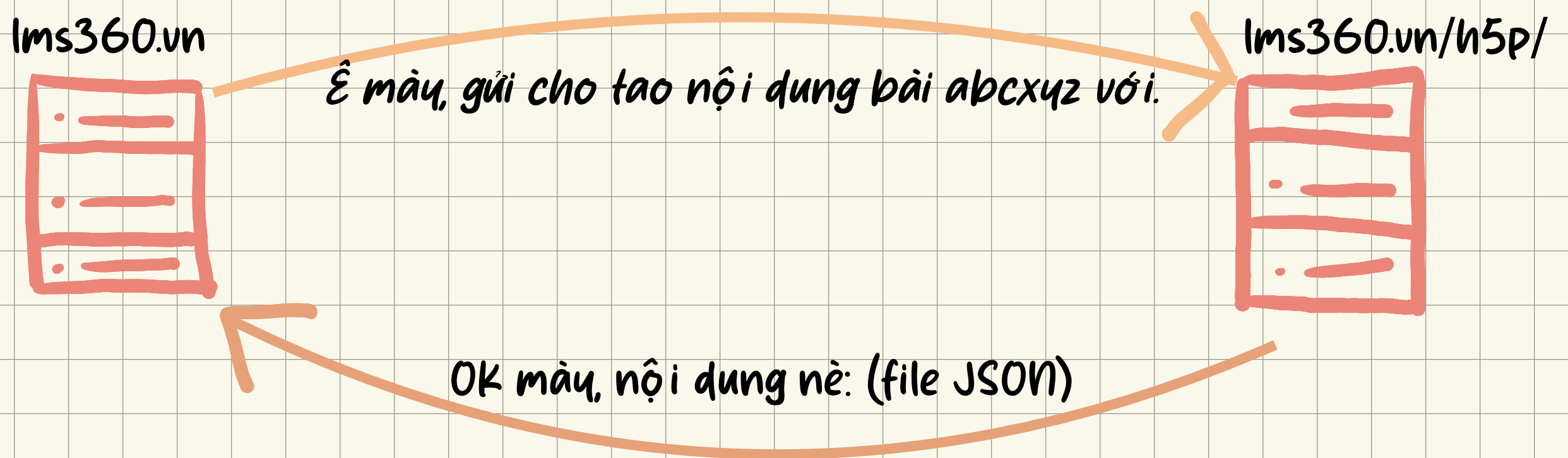
- Nhưng trên lms360.vn thì không đơn giản như vậy. Phần file mà chứa đáp án không được hiển thị trực tiếp trong mã nguồn website :(

- Và thế là mình chuyển qua một cách khác ngoài sử dụng developer tool.

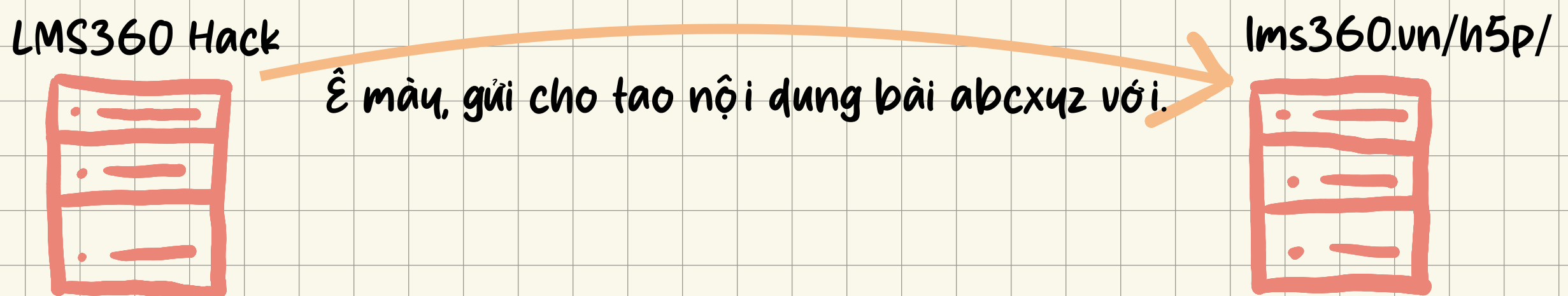
Type	Direction	Method	URL
HTTP	→ Request	GET	https://lms360.vn/h5p/68d7a88aed9a262a5e2cc822/play

- Mình đã sử dụng Burp Suite để theo dõi những request mà lms360.vn thực hiện khi load đáp án

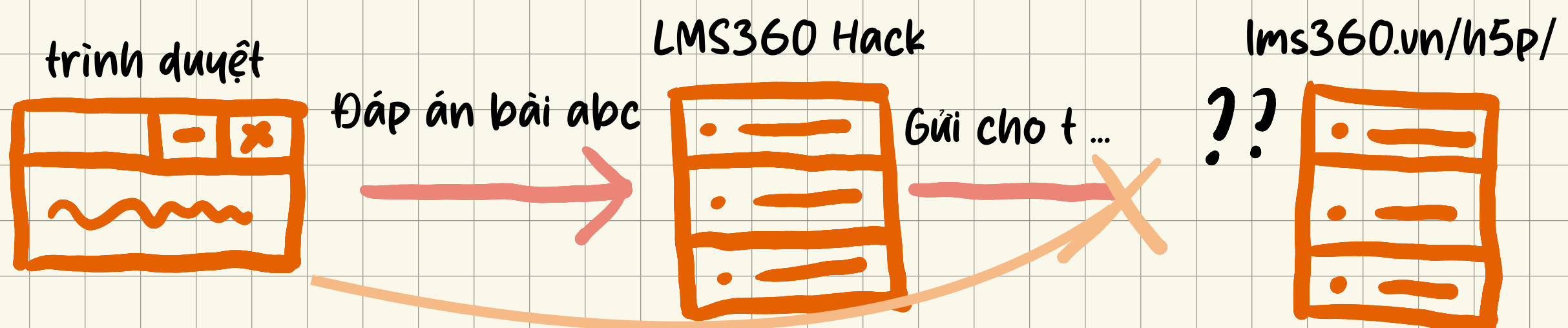
- Qua đó, chúng ta có thể tóm tắt cách lms360 hoạt động như sau:



- Vì vậy, lms360hack.pages.dev có thể lấy đáp án bằng cách như sau:

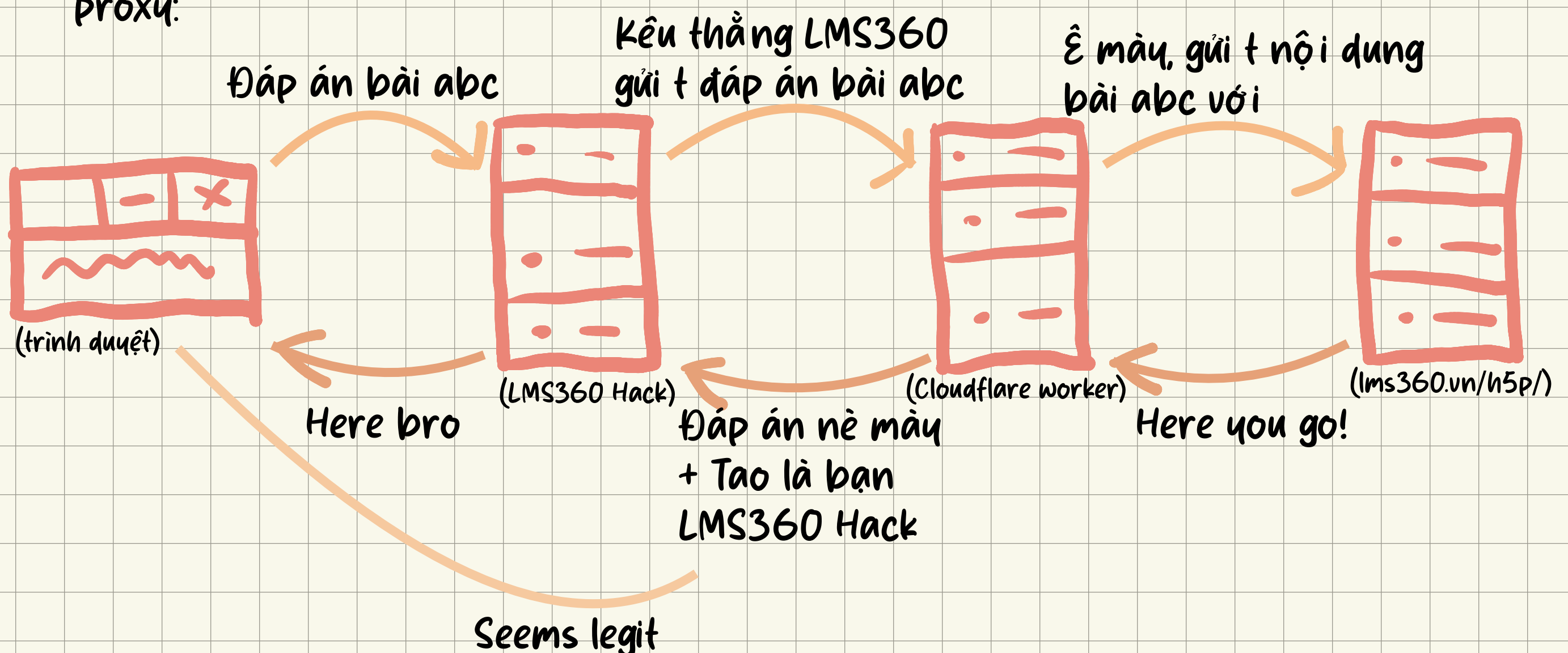


- Nhưng... có một vấn đề là trình duyệt của chúng ta không cho phép chúng ta làm thế.



cái thứ này này muốn gửi request đến lms360.vn/h5p/, nhưng lms360.vn/h5p/ lại không quen biết nó. Thôi chặn vậy.

- Sau đó, mình đã kiếm được cách bypass bằng cách sử dụng Cloudflare worker làm proxy:



- Và đó là cách LMS360 Hack ra đời!

- Lời nói cuối cùng... LMS360 thực sự rất tệ.