Đại học Quốc gia Thành phố Hồ Chí Minh
Trường Đại học Công nghệ Thông tin (UIT)

BÁO CÁO BÀI TẬP

Môn học: Bảo mật Web và Ứng dụng

Kỳ báo cáo: Thi giữa kỳ

Tên chủ đề: thi

GV: Nghi Hoàng Khoa

Ngày báo cáo: 22/04/2023

1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT101.N21.ANTN

STT	Họ và tên	MSSV	Email
1	Võ Anh Kiệt	20520605	20520605@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:[1]

STT	Công việc	Kết quả tự đánh giá	Flag
1	Kịch bản 01: welcome	100%	flag{ckuc_c4c_b4n_l4m_b4j_tkj_tk4t_t0t}
2	Kịch bản 02: find document	100%	flag{c769e47914ed6f3cd793d0b09e9acafe}
3	Kịch bản 03: whoisservice	100%	flag{bLind_os_command_injecTion}
4	Kịch bản 04:	0%	
5	Kịch bản 05	0%	

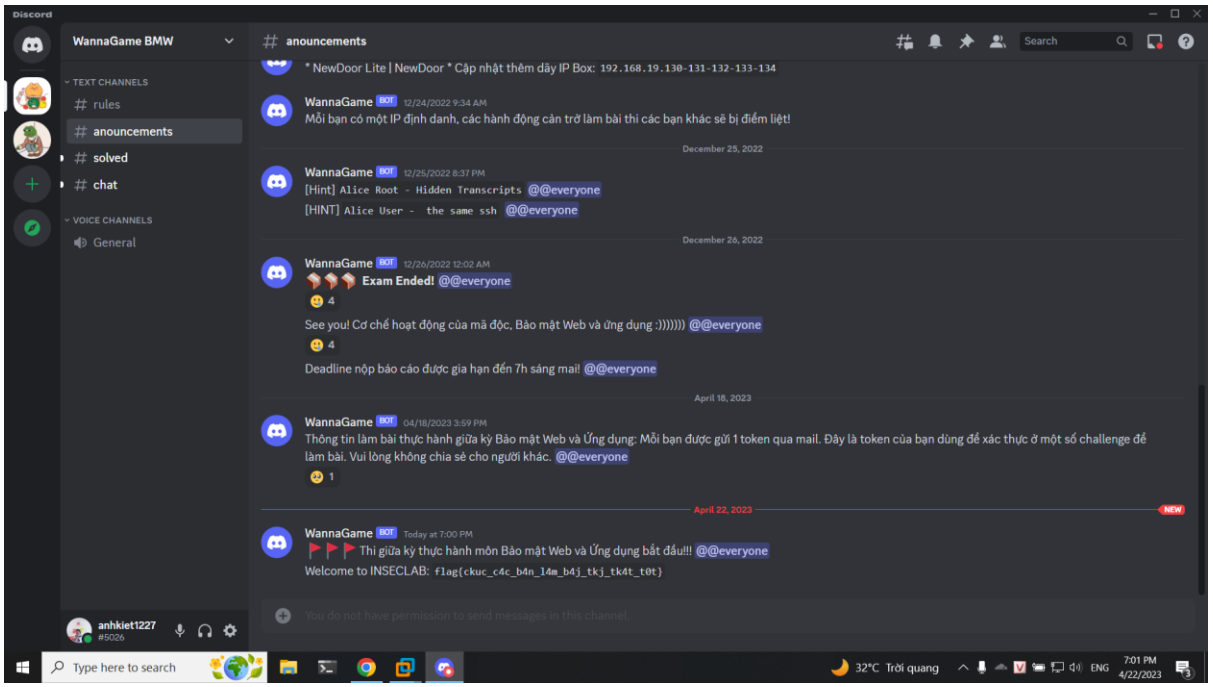
Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.

[1] Ghi nội dung công việc, các kịch bản trong bài Thực hành

BÁO CÁO CHI TIẾT

1. Kịch bản 01: welcome

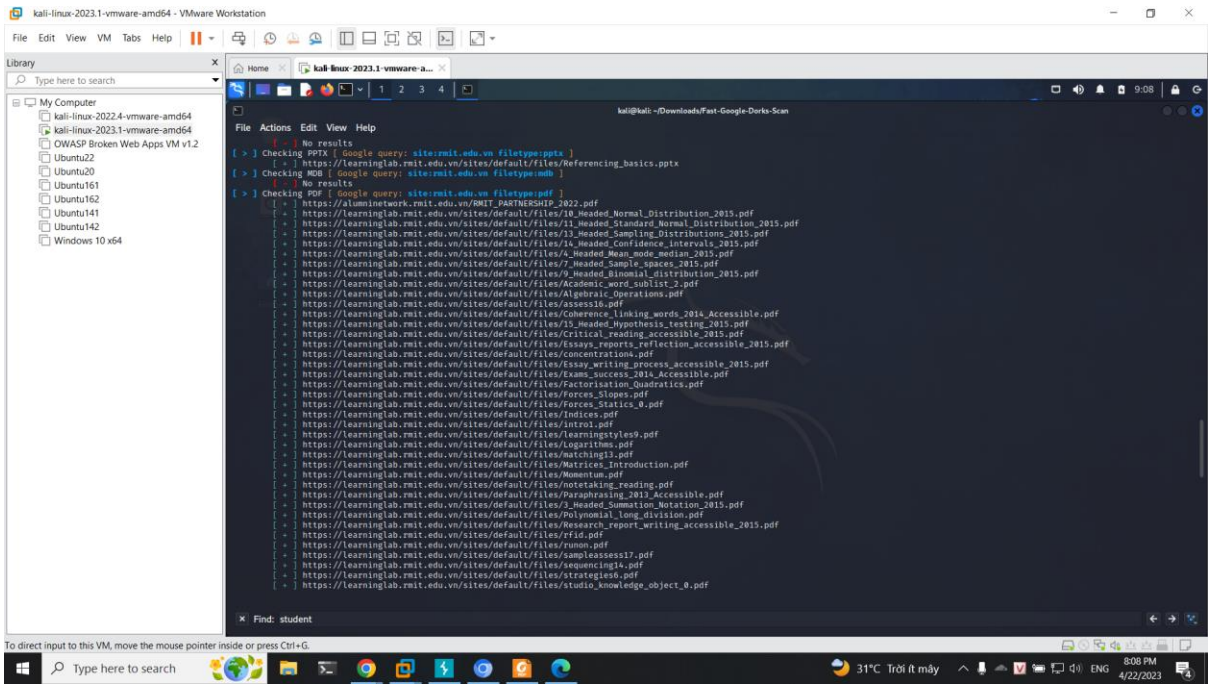
Vào discord để lấy flag nộp



ta có được flag: flag{ckuc_c4c_b4n_l4m_b4j_tkj_tk4t_t0t}

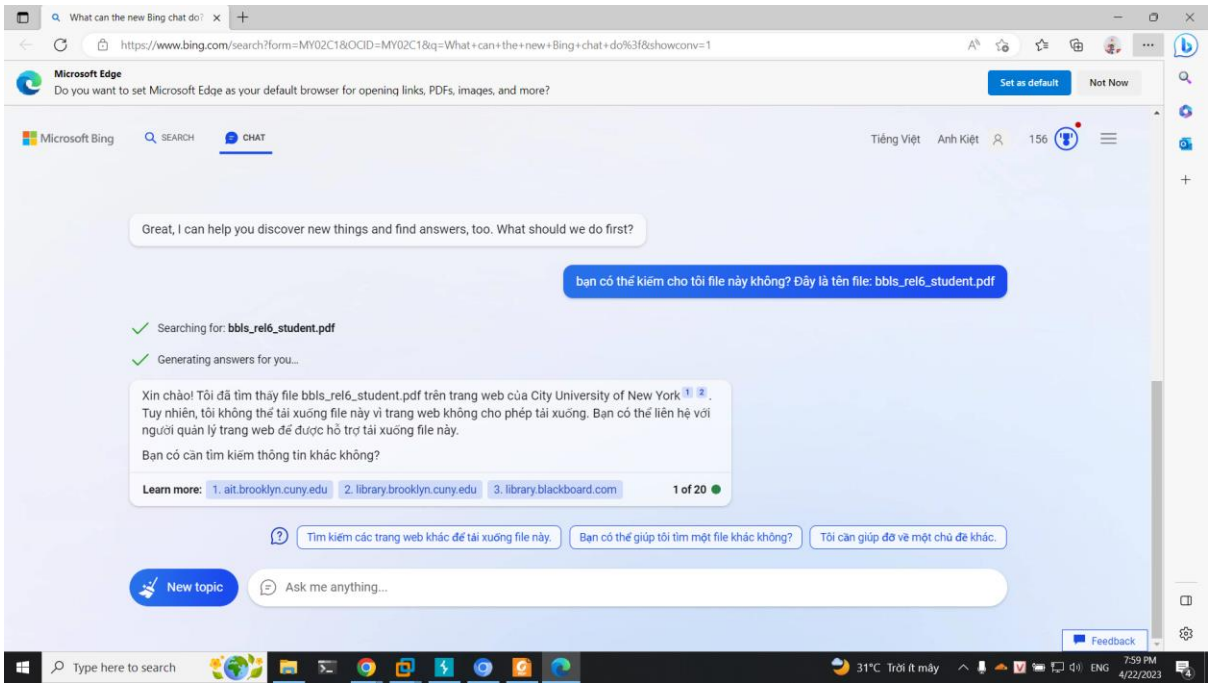
2. Kịch bản 02: Find document

Đầu tiên ta sẽ sử dụng tool Fast Google Dorks Scan để quét (https://github.com/IvanGlinkin/Fast-Google-Dorks-Scan)

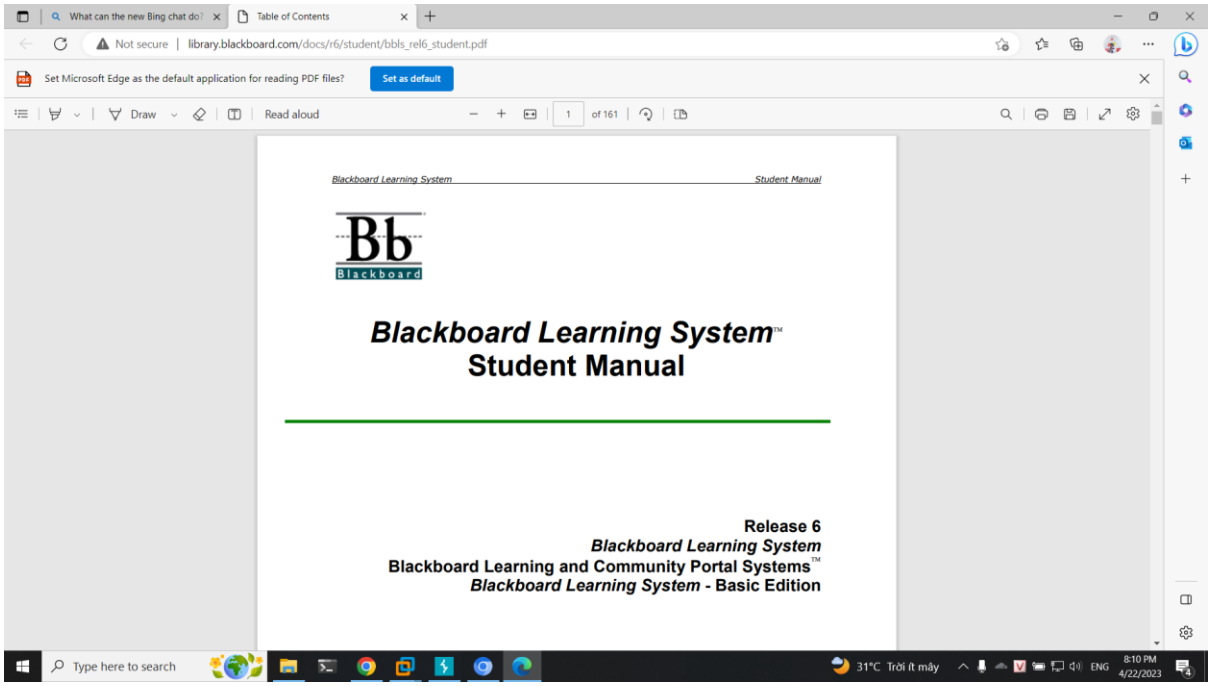


Ta không thấy có thông tin nào hết, dự đoán rằng là trang chứa file đã ngừng hoạt động

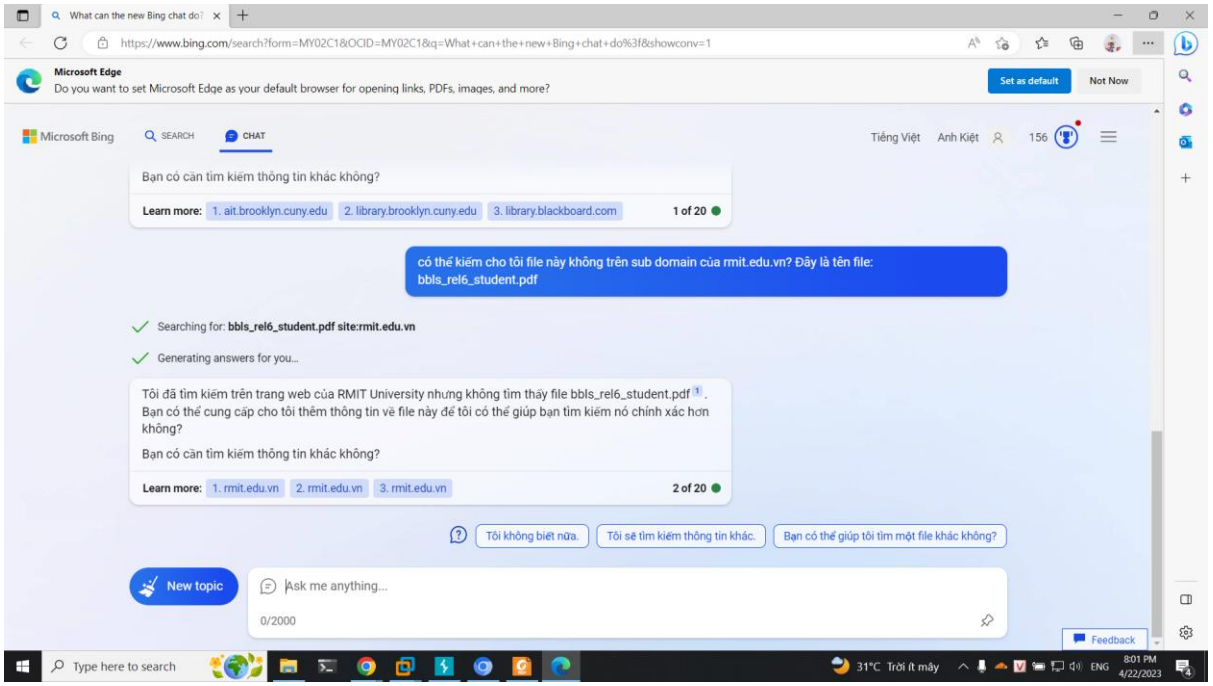
Ta sẽ hỏi một số tool AI



Ta thấy trang này cung cấp một số file không đến từ rmit nhưng đây là một file sách tài liệu



Và ta có hỏi thêm thông tin về tìm kiếm trên subdomain rmit thì kết quả không tìm thấy chứng tỏ trang cần tìm đã bị đóng



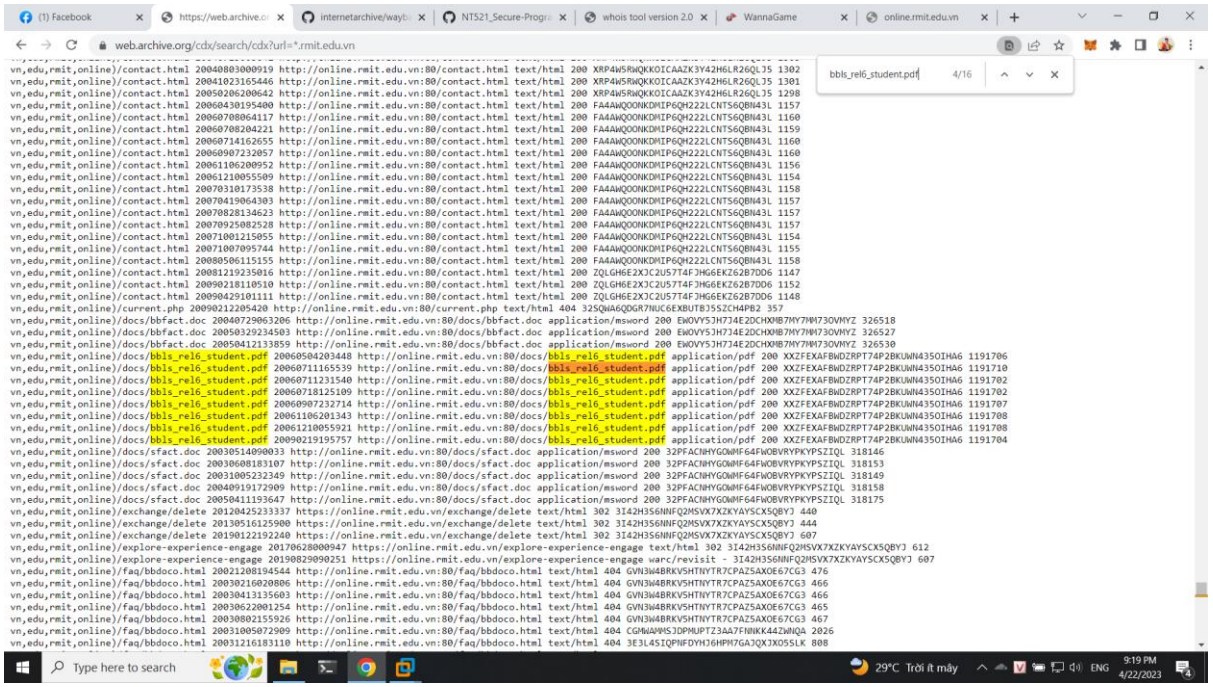
Tiếp tục ta sẽ thực hiện sử dụng tool wayback cdx server (Tham khảo: https://medium.com/hackernoon/guide-to-handling-internet-archives-cdx-server-api-response-c469df5b81f4)

Tool này hướng dẫn nhập đường dẫn https://web.archive.org/cdx/search/cdx?url=<url>

để thực hiện tìm kiếm

https://web.archive.org/cdx/search/cdx?url=*.rmit.edu.vn

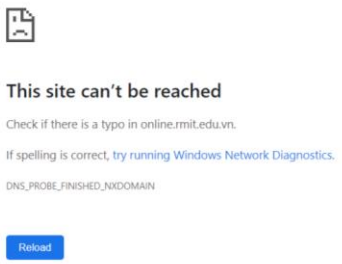
Sau đó ta tìm tên file thì thấy được đường dẫn như hình



Ta có được đường dẫn

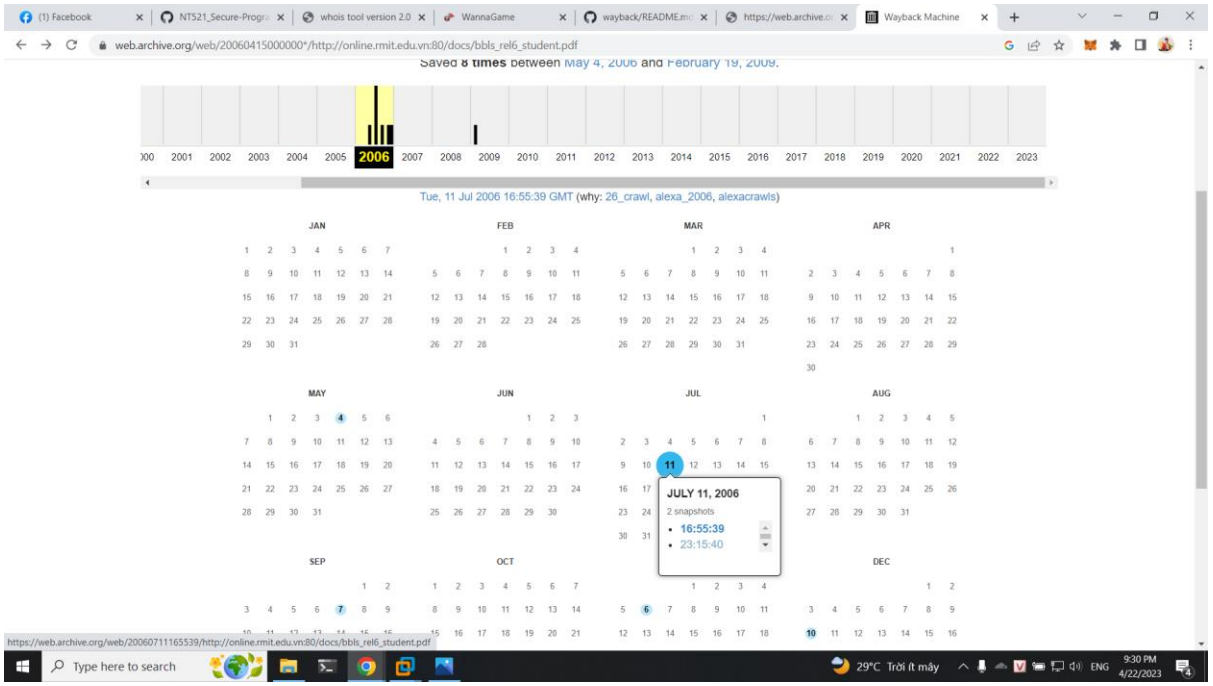
http://online.rmit.edu.vn:80/docs/bbls_rel6_student.pdf

Truy cập đường dẫn thì càng chắc chắn đường dẫn không còn hoạt động

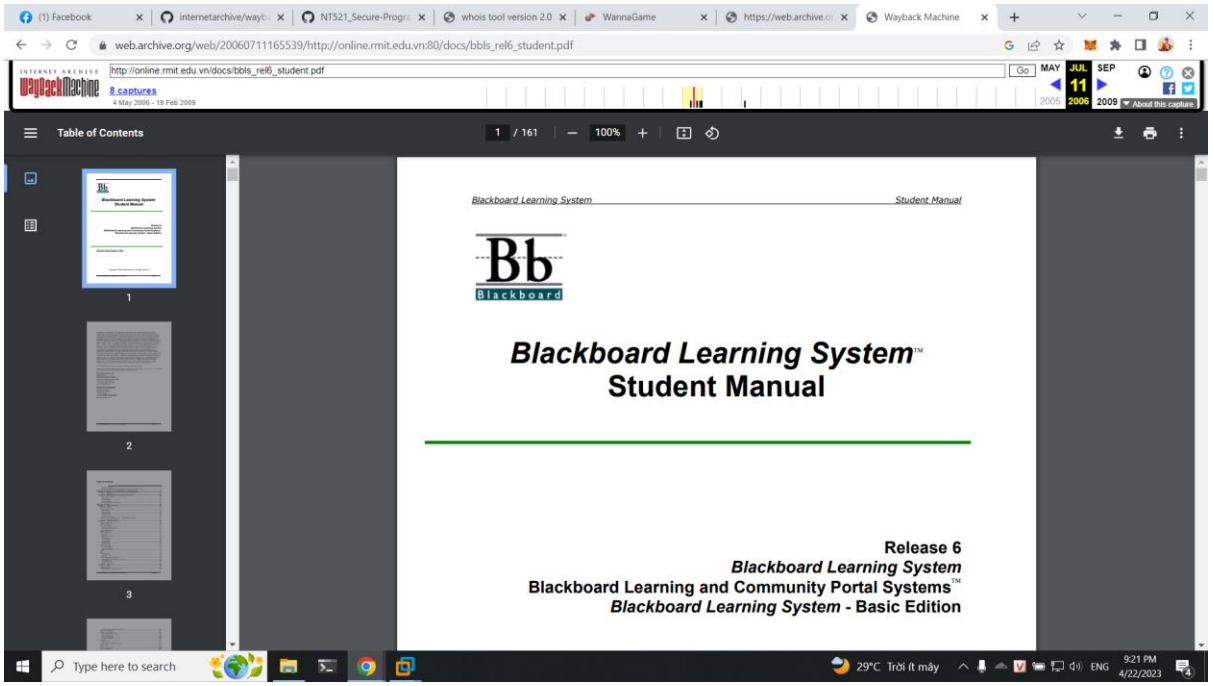


Ta sẽ vào web archive để tìm kiếm với đường dẫn đã tìm được:
http://online.rmit.edu.vn:80/docs/bbls_rel6_student.pdf

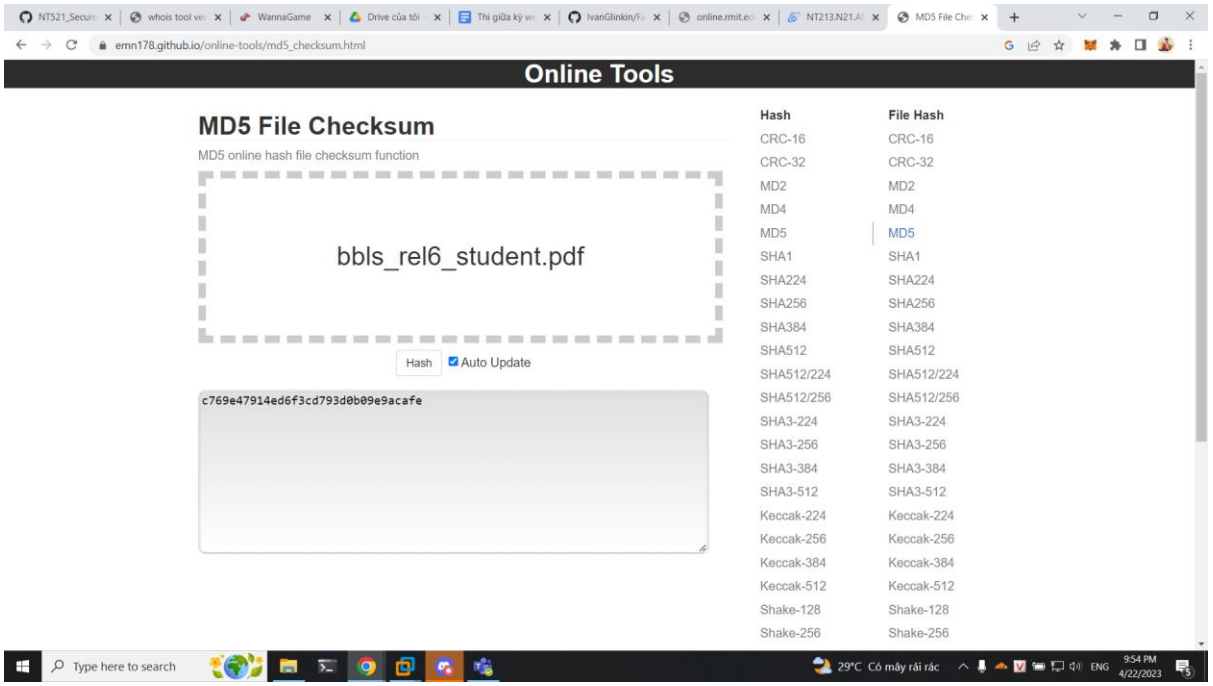
Thì ta có được trang hoạt động vào ngày 11/7/2006



Tiếp tục vào xem thì ta có được file



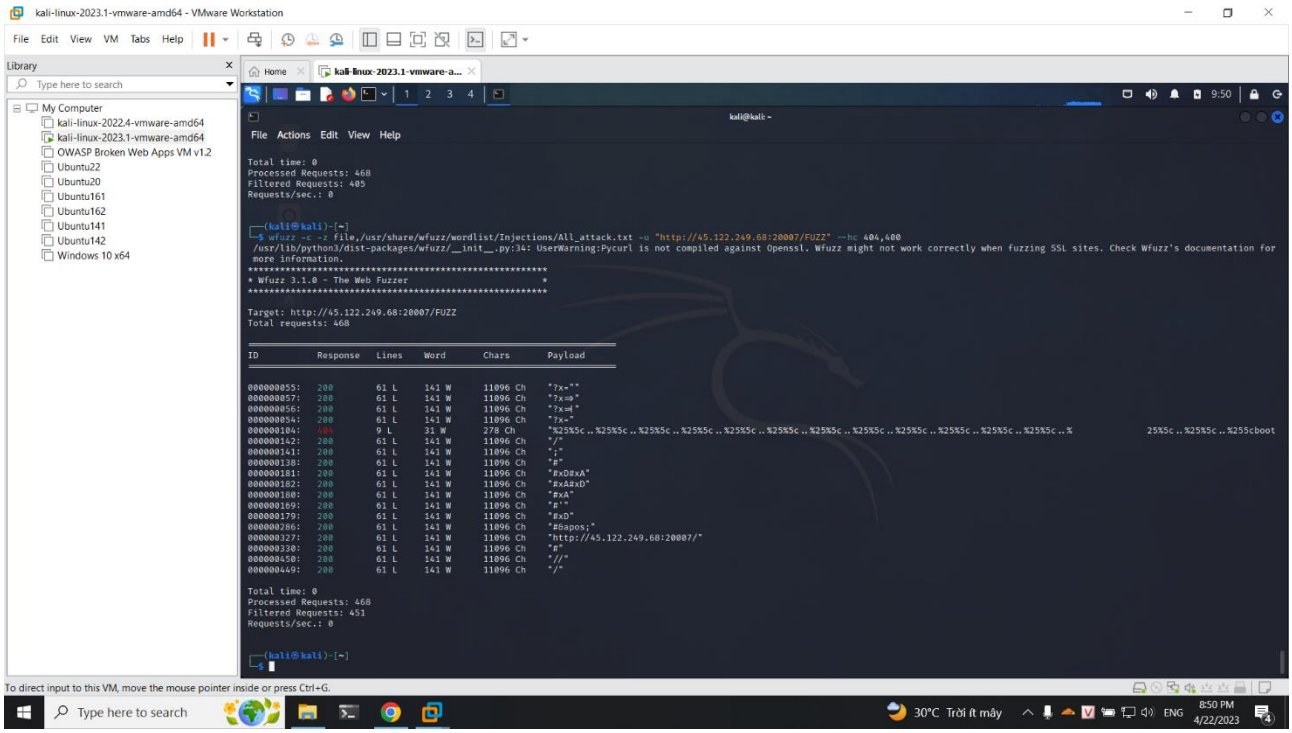
Sau đó ta thực hiện băm



Ta có được flag là: flag{c769e47914ed6f3cd793d0b09e9acafe}

3. Kịch bản 3: whois server

Đầu tiên ta sẽ sử dụng kỹ thuật fuzzing để thử xem trang có thể accept hoặc không accept thông tin nào



Ở đây ta thấy thông tin chính là việc / không bị chặn và có thể truyền payload. Nhưng ở phía trang thì bị chặn bởi trang, vì vậy ta cần vượt qua chặn của trang để xuống root và truy cập

Ở đây việc chuyển đổi sẽ được quy đổi như sau:

Tham khảo:
http://doc.isilon.com/onefs/zzz_archive/cloudpools_staging/ifs_r_supported_home_dir_expansion_variables.html

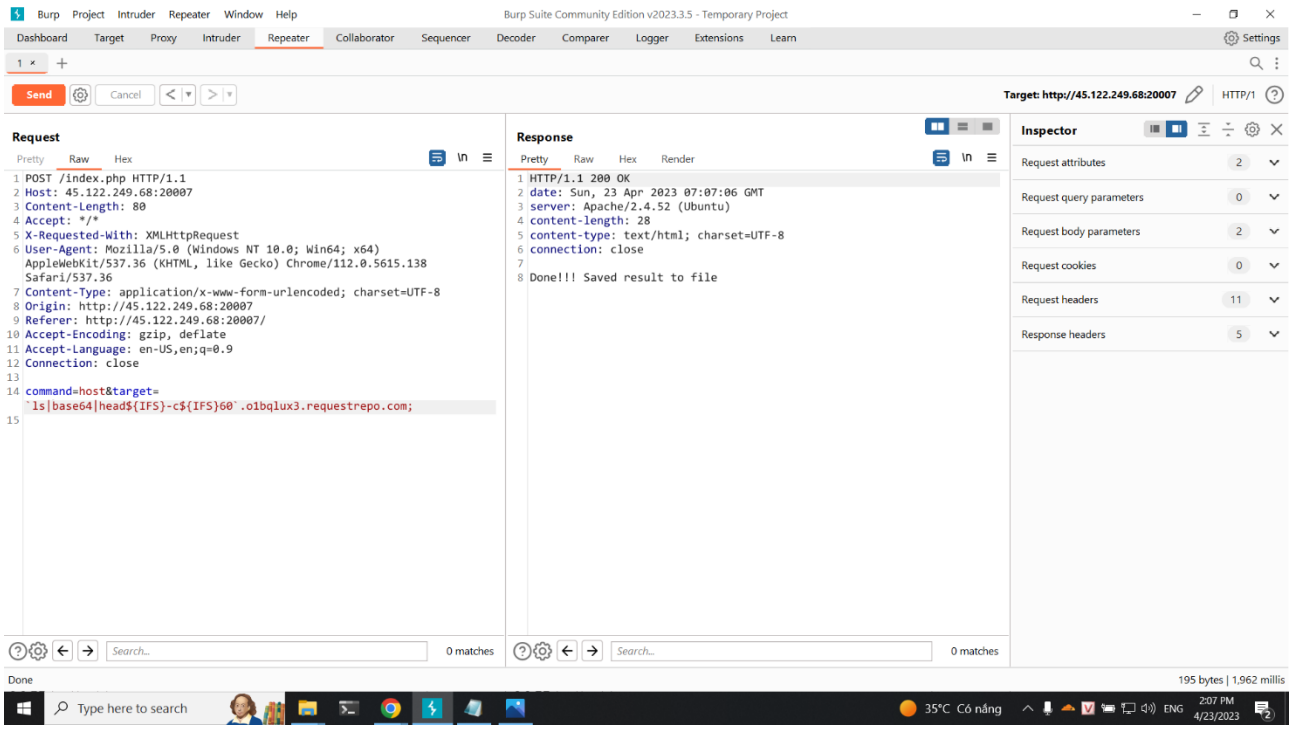
https://unix.stackexchange.com/questions/184863/what-is-the-meaning-of-ifs-n-in-bash-scripting

<cách>: ${IFS}

/: ${PATH%%u*}

Tiếp theo ta sẽ triển khai tấn công bằng cách bắt burp suite:

Đầu tiên ta sẽ ls ra để xem

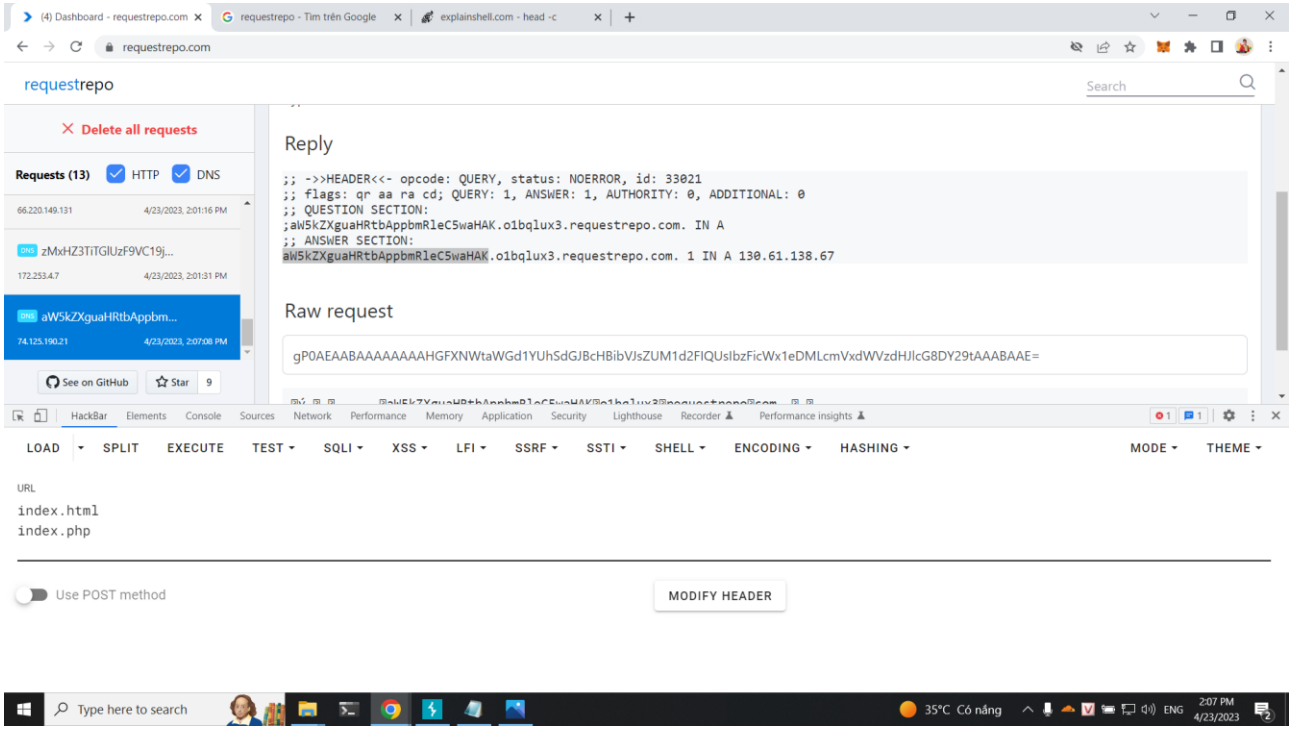


Với câu lệnh này ls để show các file, folder tại vị trí hiện tại

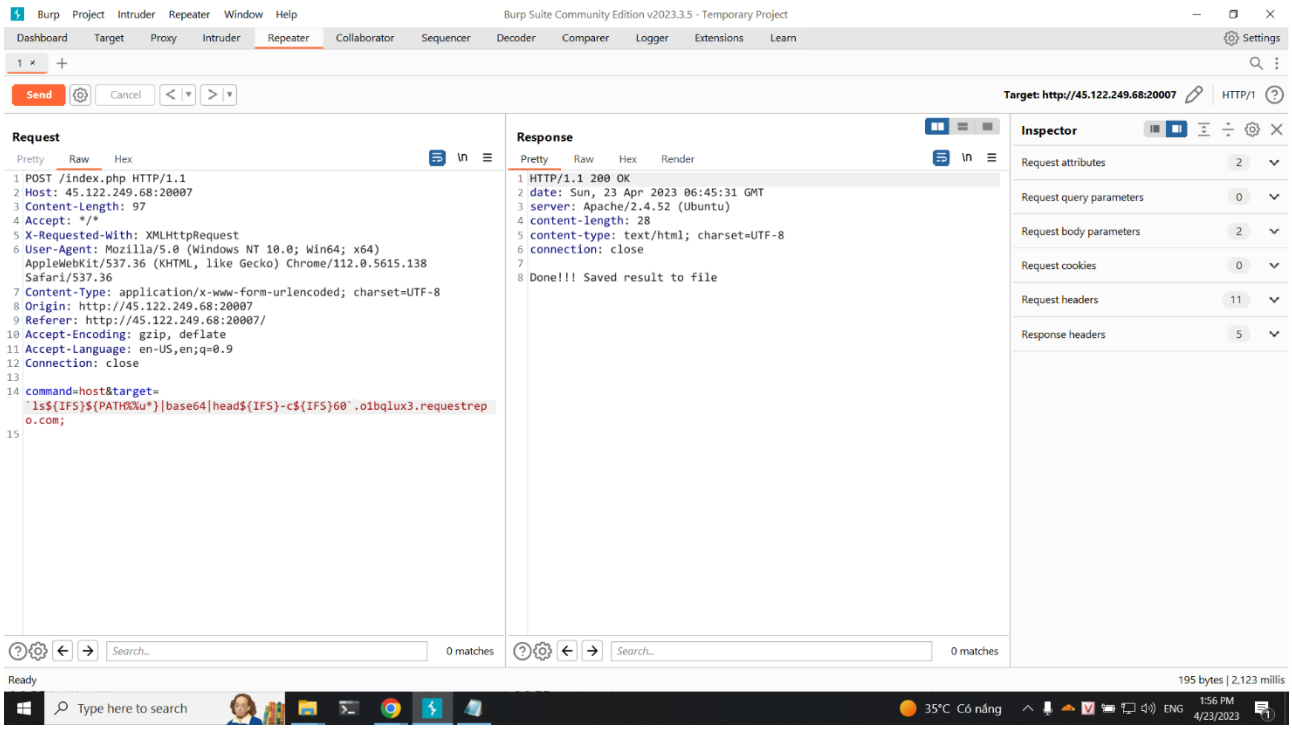
Base64 để thực hiện encode

Và head -c 60 là để lấy 60 btye đầu của những thông tin được lấy ra để thực hiện giảm khối lượng lấy giúp cho việc trả về được thực hiện

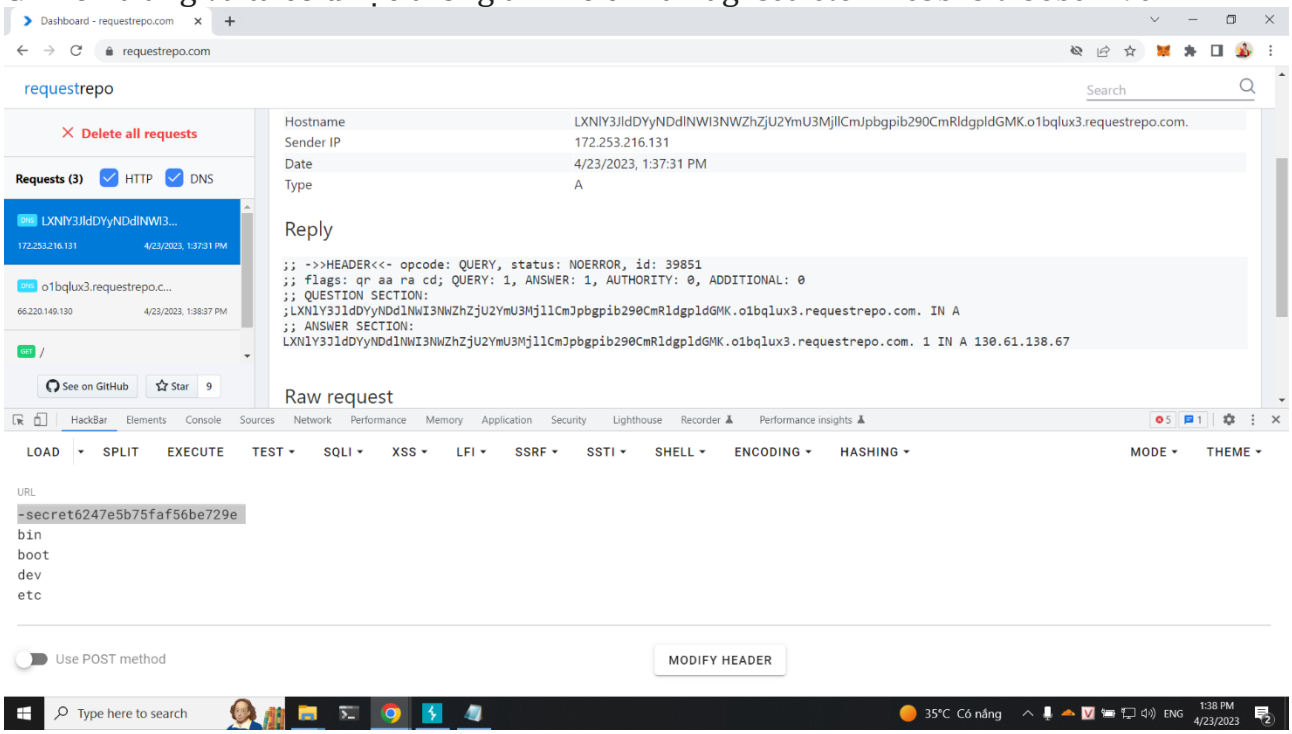
Kết quả ta có được là thông tin 2 file index.html và index.php, với 2 file này thì ta không có thông tin gì (Sau khi có kết quả ta sẽ sử dụng hackbar để decode base64 để xem lại)



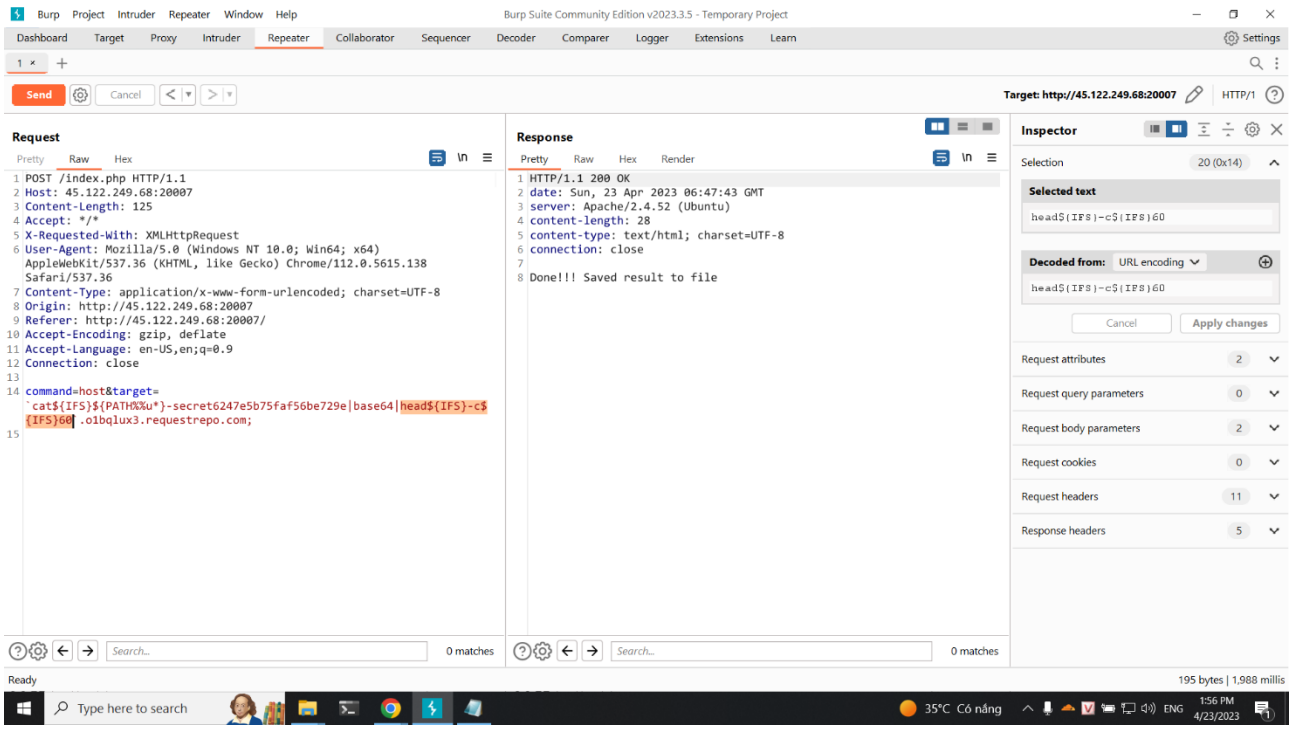
Tiếp tục thực hiện truyền lệnh ls /



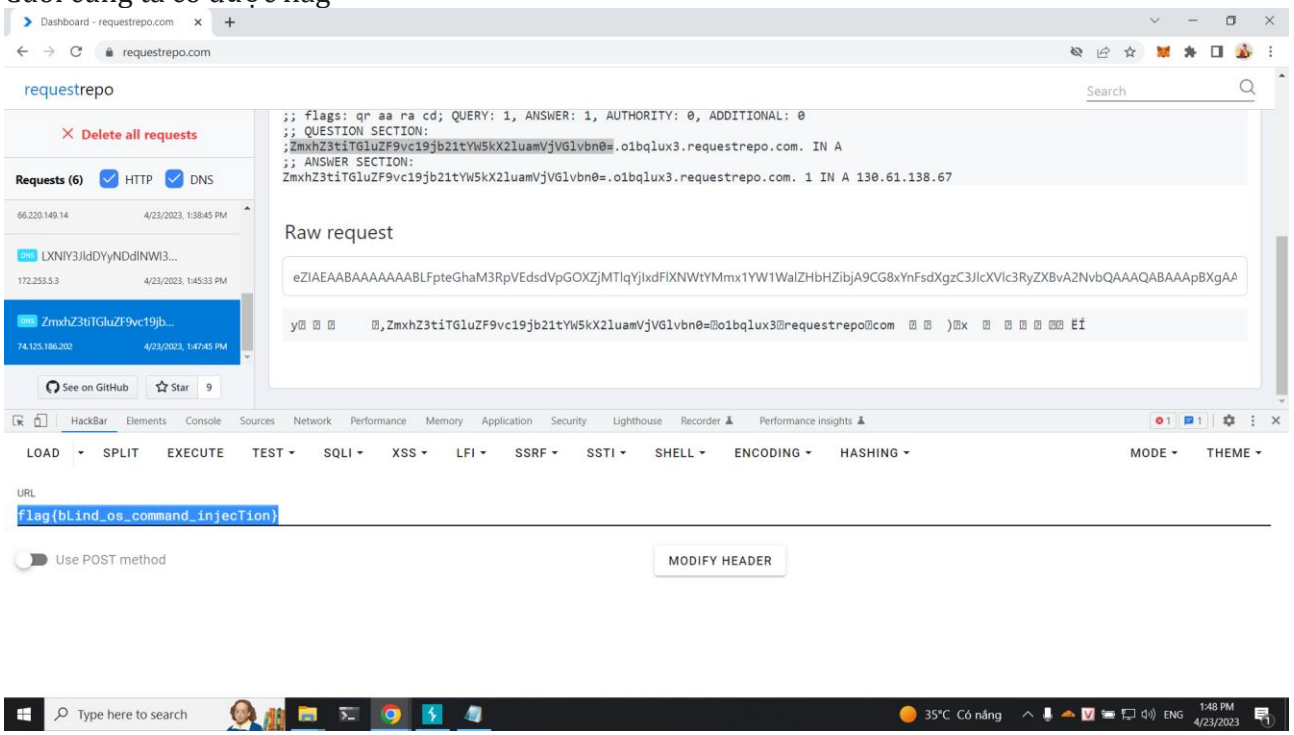
Gửi lên trang và ta có được thông tin file chứa flag -secret6247e5b75faf56be729e



Ta sẽ thực hiện cat /-secret6247e5b75faf56be729e để xem flag



Cuối cùng ta có được flag



Flag: flag{bLind_os_command_injecTion}

Sinh viên đọc kỹ yêu cầu trình bày bên dưới trang này

YÊU CẦU CHUNG

- Sinh viên tìm hiểu và thực hành theo hướng dẫn.
- Nộp báo cáo kết quả chi tiết những việc (**Report**) bạn đã thực hiện, quan sát thấy và kèm ảnh chụp màn hình kết quả (nếu có); giải thích cho quan sát (nếu có).
- Sinh viên báo cáo kết quả thực hiện và nộp bài.

Báo cáo:

- File .PDF. Tập trung vào nội dung, không mô tả lý thuyết.
- Nội dung trình bày bằng Font chữ Times New Romans/ hoặc font chữ của mẫu báo cáo này (UTM Neo Sans Intel/UTM Viet Sach)– cỡ chữ 13. Canh đều (Justify) cho văn bản. Canh giữa (Center) cho ảnh chụp.
- Đặt tên theo định dạng: [Mã lớp]-SessionX_GroupY. (trong đó X là Thứ tự buổi Thực hành, Y là số thứ tự Nhóm Thực hành/Tên Cá nhân đã đăng ký với GV).

  *Ví dụ: [*NT101.K11.ANTT*]-Session1_Group3.*
- Nếu báo cáo có nhiều file, nén tất cả file vào file .ZIP với cùng tên file báo cáo.
- Không đặt tên đúng định dạng – yêu cầu, sẽ **KHÔNG** chấm điểm.
- Nộp file báo cáo trên theo thời gian đã thống nhất tại courses.uit.edu.vn.

Đánh giá: Sinh viên hiểu và tự thực hiện. Khuyến khích:

- Chuẩn bị tốt.
- Có nội dung mở rộng, ứng dụng trong kịch bản/câu hỏi phức tạp hơn, có đóng góp xây dựng.

Bài sao chép, trễ, … sẽ được xử lý tùy mức độ vi phạm.

HẾT