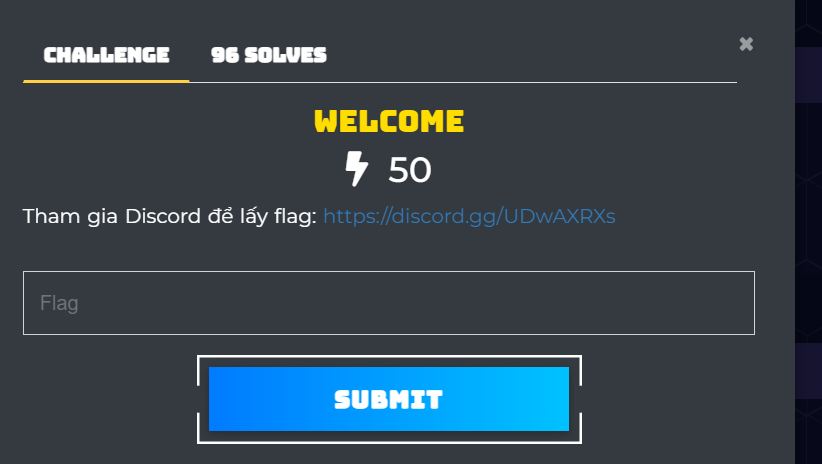
* Challenge 1: Welcome



* Ở challenge này ta chỉ cần vào link discord là sẽ có được flag

Ảnh có chứa văn bản, ảnh chụp màn hình, màu đen, bình phong

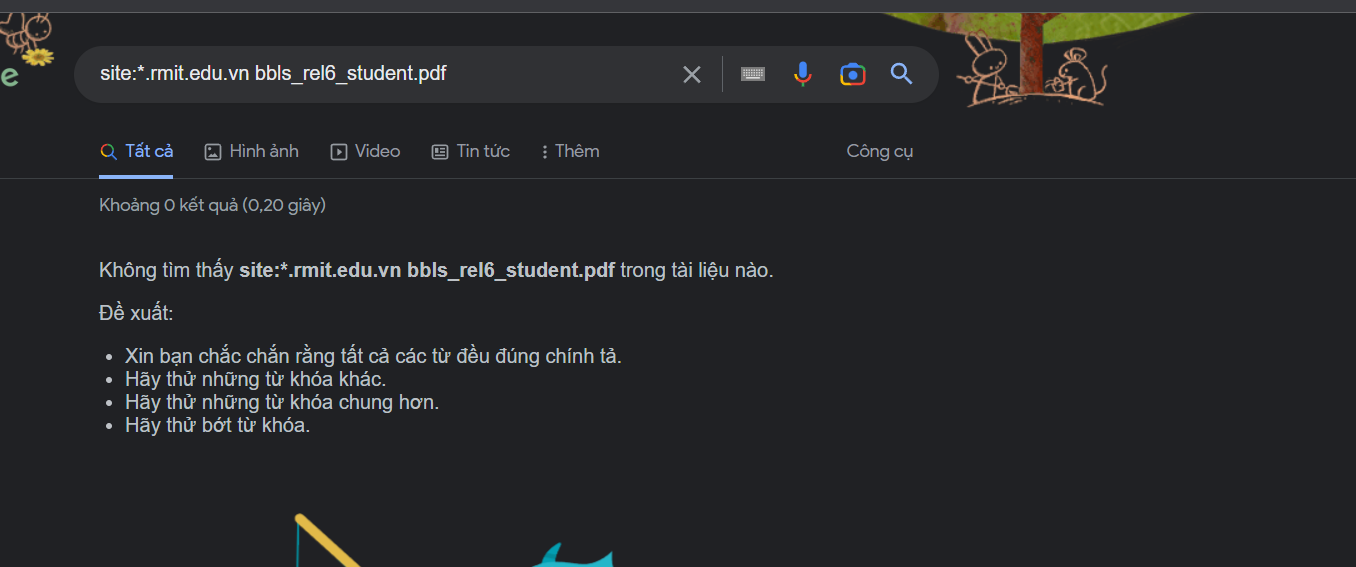
Mô tả được tạo tự động

* flag{ckuc\_c4c\_b4n\_l4m\_b4j\_tkj\_tk4t\_t0t}
* Challenge 2: Find Document

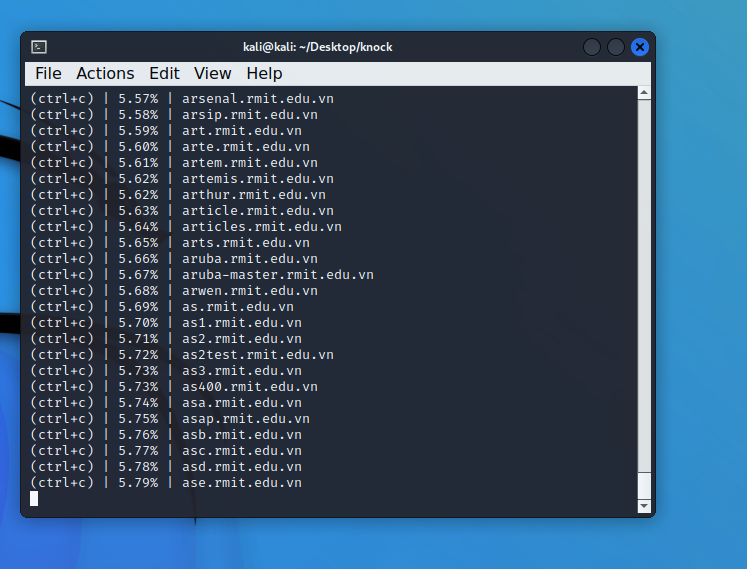
Ảnh có chứa Website

Mô tả được tạo tự động

* Ở đây ta cần tìm 1 file tên là “bbls\_rel6\_student.pdf” ở trên \*.rmit.edu.vn là top domain của rmit



* Tìm thử trên google thì không có



* Em sử dụng công cụ knock để kiếm xem các top domain của rmit.edu.vn xem sao
* Nhưng cũng không giúp ích gì nhiều

Ảnh có chứa văn bản

Mô tả được tạo tự động

* Em nảy ra ý tưởng sử dụng wayback machine để kiểm tra xem các domain ở công cụ duck search có ghi lại file đó không nhưng cũng không có ích
* Tới đây em nghĩ là do trang rmit nhúng link để down file ở một chỗ nào đó nên không thể search bình thường ra

Ảnh có chứa văn bản

Mô tả được tạo tự động

* Search google không được thì em chuyển qua bing thì lại thấy file sau đó tải về

Ảnh có chứa văn bản

Mô tả được tạo tự động

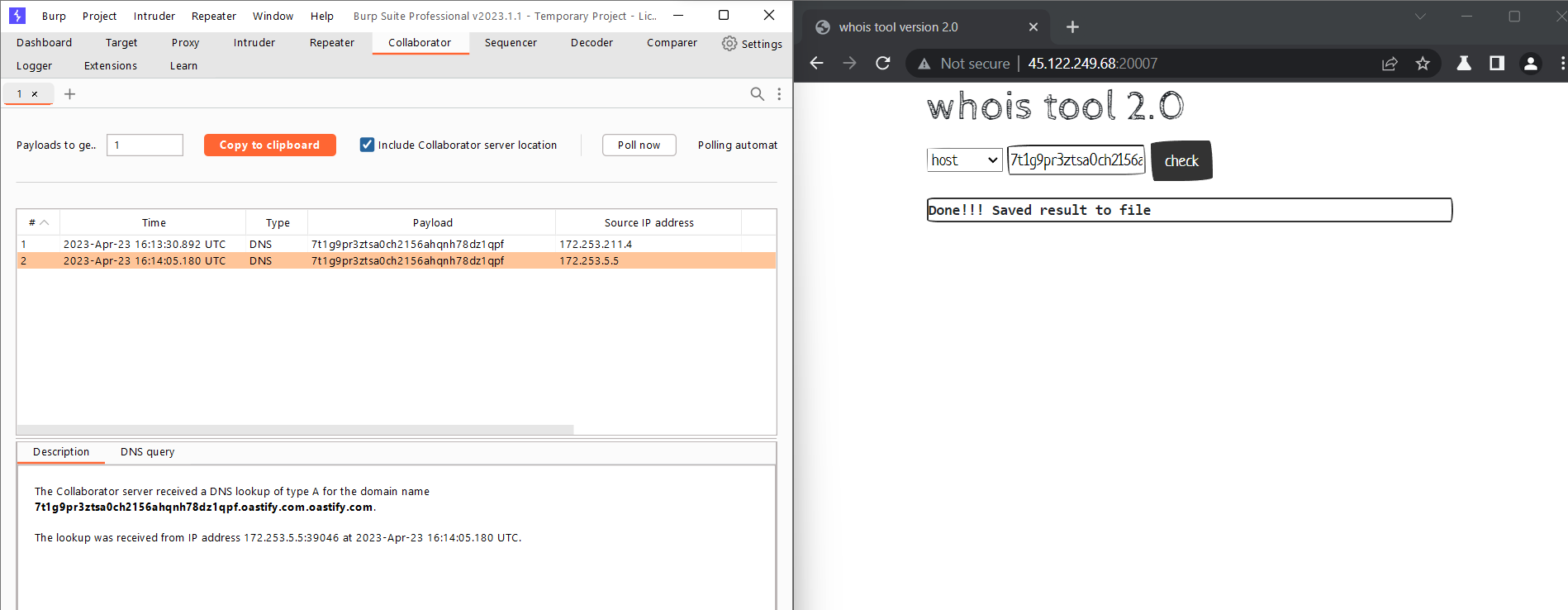
* Đây là md5 của file
* flag{c769e47914ed6f3cd793d0b09e9acafe}

Challege 3: Whoisservice

Ảnh có chứa văn bản

Mô tả được tạo tự động

* Khi qua thử các option thì ta thấy là service host có thể khai thác được
* - Khi sử dụng lệnh cd .. ta thấy thư mục hiện hành là html. Khả năng nó có đường dẫn là /var/www/html. Thực hiện tấn công Blind OS command như sau để tìm file secret ( Vì file bị mã hóa tên nên không thể trả về, nên ta sẽ sử dụng xxd để lấy mã hex và chuyển về text)



* Ta sử dụng chức năng collaborator của burpsuite pro
* Khi sử dụng chức năng Collaborator, Burp Suite Pro sẽ cung cấp cho bạn một địa chỉ email hoặc một địa chỉ IP, tùy thuộc vào cấu hình của bạn, để sử dụng trong các yêu cầu HTTP của bạn. Khi các yêu cầu này được gửi đến các ứng dụng web đang được kiểm thử, Burp Suite Pro sẽ theo dõi các phản hồi từ máy chủ phản hồi của Collaborator để phát hiện các lỗ hổng bảo mật.

Ảnh có chứa văn bản

Mô tả được tạo tự động

- Chuyển tên file dưới dạng mã hex về text:

Ảnh có chứa văn bản

Mô tả được tạo tự động

- Sau khi lấy được tên file thì thực hiện cat nội dung của file ra. Nội dung bị mã hóa nên ta đưa về dạng base64

Ảnh có chứa văn bản

Mô tả được tạo tự động

- Sau đó chuyển về lại text, ta nhận được flag

Ảnh có chứa văn bản

Mô tả được tạo tự động

- Do em nộp trễ quá đã quá thời gian nộp nên bài này em chỉ viết writeup

- flag{bLind\_os\_command\_injecTion}