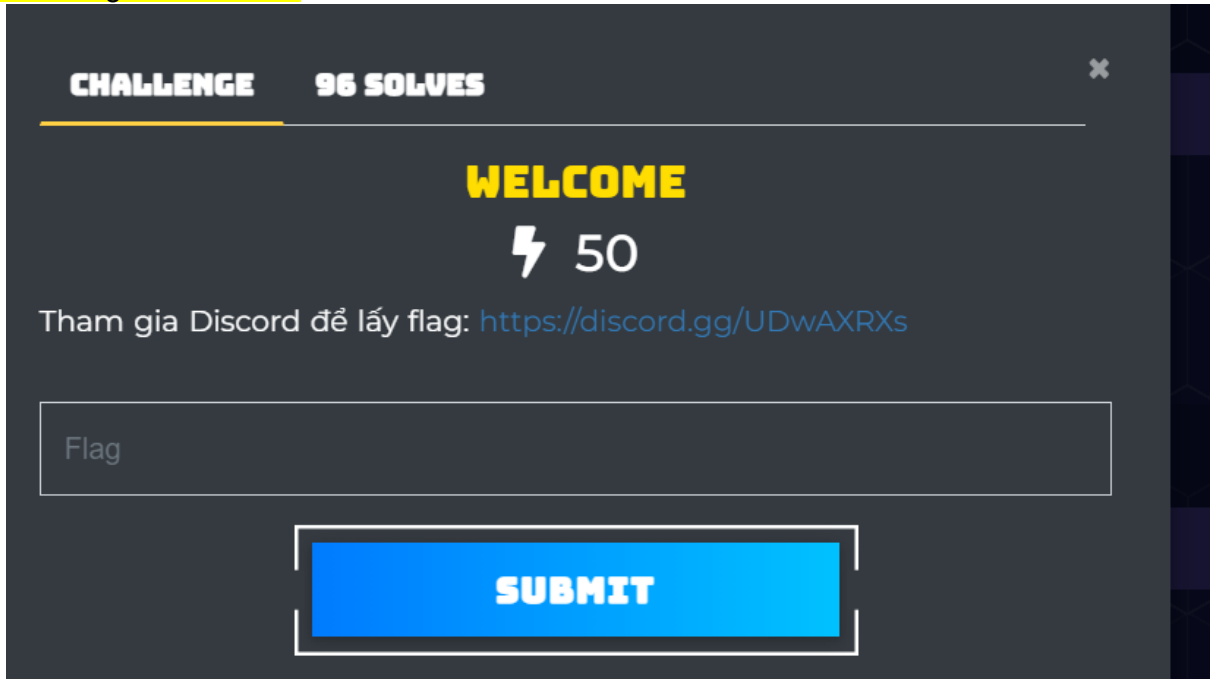


- Challenge 1: Welcome

The image shows a dark-themed web interface for a challenge. At the top, it says 'CHALLENGE' and '96 SOLVES'. Below this, the word 'WELCOME' is displayed in large yellow letters, followed by a lightning bolt icon and the number '50'. A text prompt in Vietnamese asks to join a Discord server to get a flag, with a link provided. Below the text is a text input field labeled 'Flag'. At the bottom, there is a prominent blue button with the word 'SUBMIT' in white capital letters.

CHALLENGE 96 SOLVES

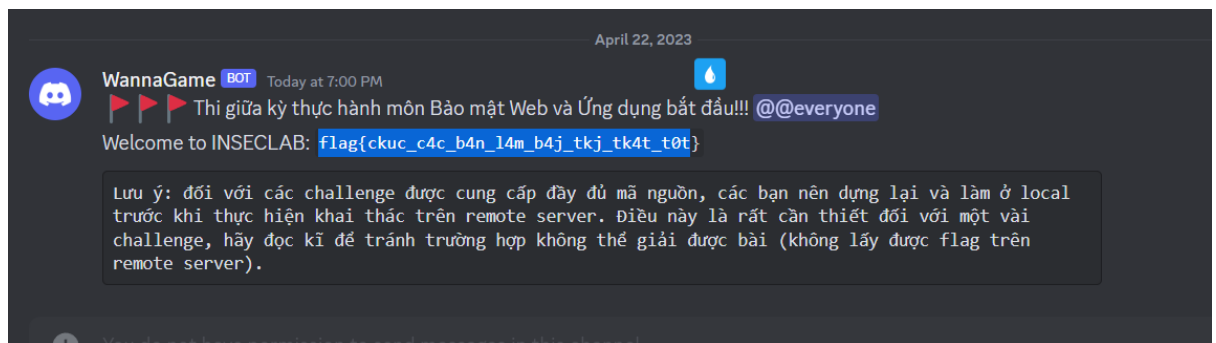
**WELCOME**  
⚡ 50

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

Flag

**SUBMIT**

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



→ `flag{ckuc_c4c_b4n_l4m_b4j_tkj_tk4t_t0t}`

- Challenge 2: Find Document

CHALLENGE

66 SOLVES

X

FIND DOCUMENT

⚡ 150

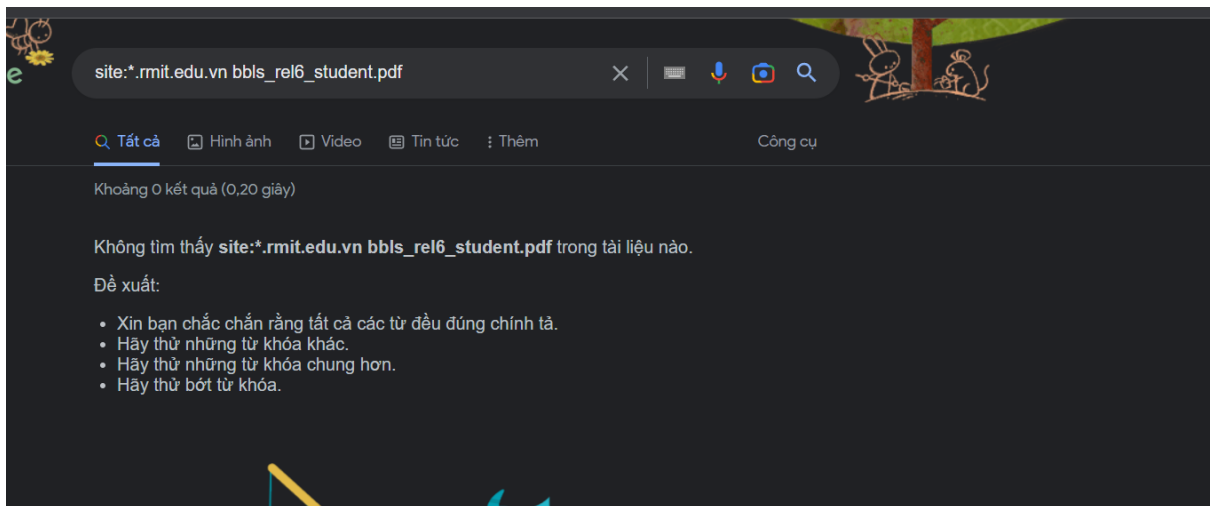
Tìm file **bbbs\_rel6\_student.pdf** trên **\*.rmit.edu.vn**

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

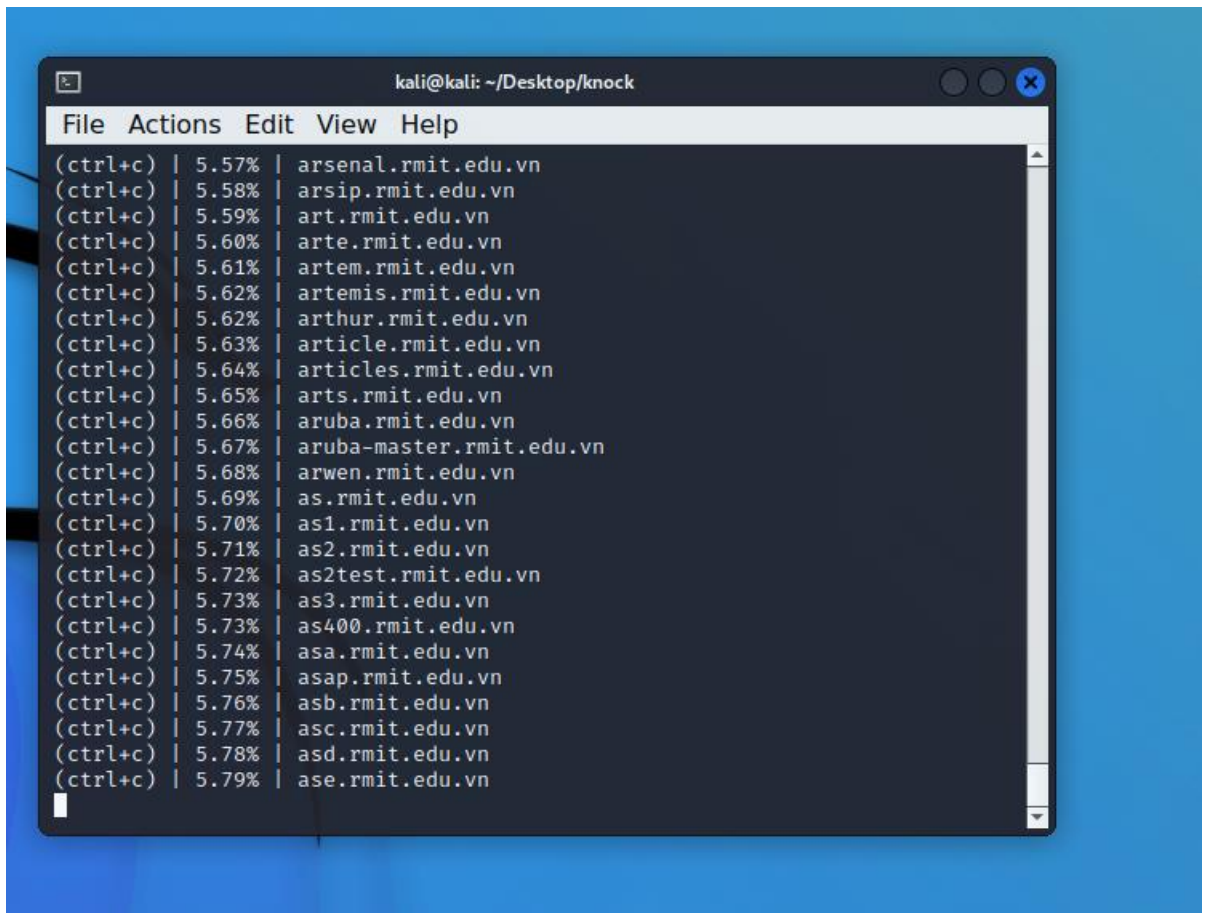
Flag

SUBMIT

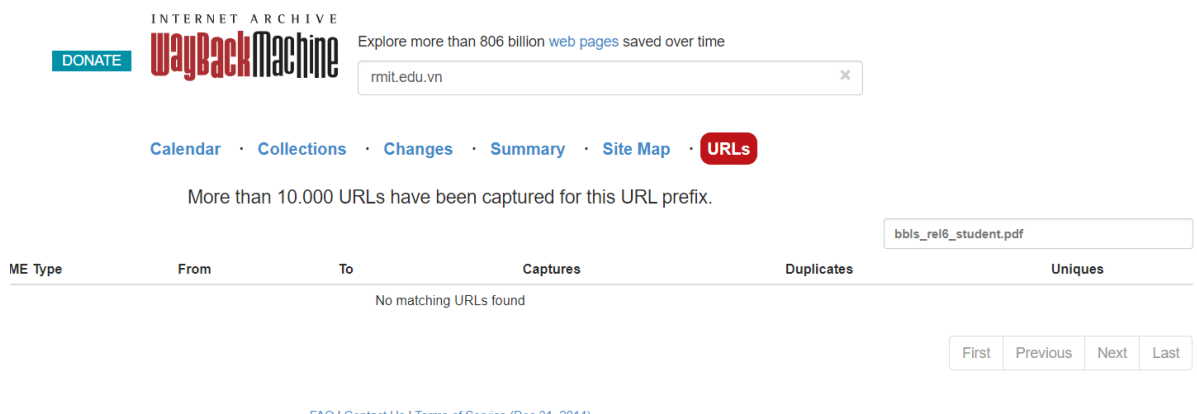
- Ở đây ta cần tìm 1 file tên là “bbbs\_rel6\_student.pdf” ở trên \*.rmit.edu.vn là top domain của rmit



- Tìm thử trên google thì không có



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



- 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

Bing

bbbs\_rel6\_student.pdf

TÌM KIẾM TRÒ CHUYỆN TRƯỜNG HỌC HÌNH ẢNH VIDEO BẢN ĐỒ XEM THÊM

Về 652,000 kết quả

**Behind the Blackboard!**  
[library.blackboard.com/docs/r6/student/bbbs\\_rel6\\_student.pdf](https://library.blackboard.com/docs/r6/student/bbbs_rel6_student.pdf)  
Web We would like to show you a description here but the site won't allow us.

Tìm kiếm

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

## MD5 File Checksum

MD5 online hash file checksum function

bbbs\_rel6\_student.pdf

Hash ☒ Auto Update

c769e47914ed6f3cd793d0b09e9acafe

- Đây là md5 của file

→ flag{c769e47914ed6f3cd793d0b09e9acafe}

Challenge 3: Whoisservice

# whois tool 2.0

host ▼

cat flag.txt

check

Attack detected!!!

- 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)

The image shows two side-by-side screenshots. The left screenshot is from Burp Suite Professional v2023.1.1, showing the 'Collaborator' tab. It displays a table of payloads and a description of a DNS query. The right screenshot is from the 'whois tool version 2.0' web application. It shows the same input fields as the top of the document, but the 'check' button has been clicked, and the output shows 'Done!!! Saved result to file'.

- 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.

The image shows two side-by-side screenshots from Burp Suite. The left screenshot shows the 'Generate Collaborator payloads' section, where a payload is generated and added to the 'Collaborator interactions' table. The right screenshot shows the 'Repeater' tab, displaying a list of requests. The selected request is a POST request to /index.php HTTP/1.1, with a body containing a command: 'command=hosttarget+...'. The 'Inspector' tab on the right shows the details of the request, including headers and body.

- Chuyển tên file dưới dạng mã hex về text:

Tùy chọn đầu vào

Dán văn bản bạn muốn hex giải mã ở đây:

```
2d7365637265743632343765362373566616635366265373239650a
```

Hex Decode!

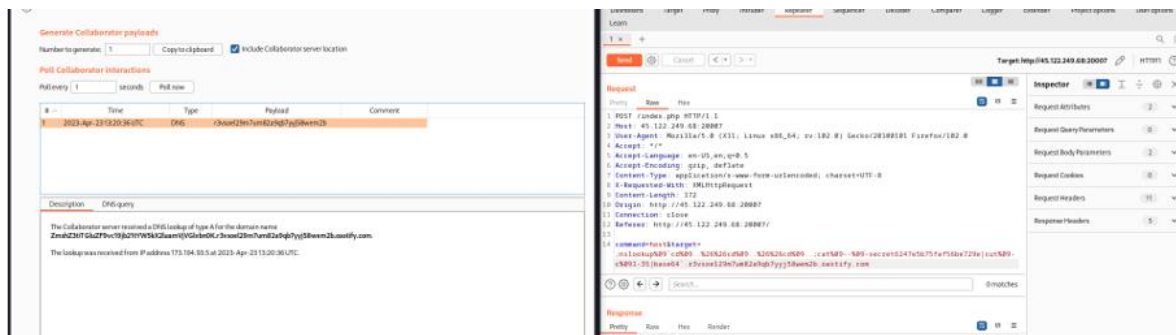
Hex vào văn bản

Download file

Sao chép văn bản giải mã hex của bạn ở đây:

```
-secret6247e5b75fa156be729e
```

- 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



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

Decode and Encode

Do you have to deal with Base64 format? Then this site is perfect for you! Use our super handy online tool to encode or decode your data.

Decode from Base64 format

Simply enter your data then push the decode button.

ZmxhZ29tTGluZF9vc19jb21tYW5kX2luamVjVGlnbnR0K

For encoded binaries (like images, documents, etc.) use the file upload form a little further down on this page.

Source character set: ASCII

Decode each line separately (useful for when you have multiple entries).

Live mode OFF

Decodes in real-time as you type or paste (supports only the UTF-8 character set).

DECODE

Decodes your data into the area below.

flag{bLind\_os\_command\_injection}

Language: English, Español, Français

Bonus tip: Bookmark us!

Other tools

- URL Decode
- URL Encode
- JSON Minify
- JSON Beautify
- JS Minify
- JS Beautify
- CSS Minify
- CSS Beautify

Partner sites

- Number System Converter
- TV Show and Movie Ratings
- Secure Group Chat

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

- `flag{bLind_os_command_injection}`

