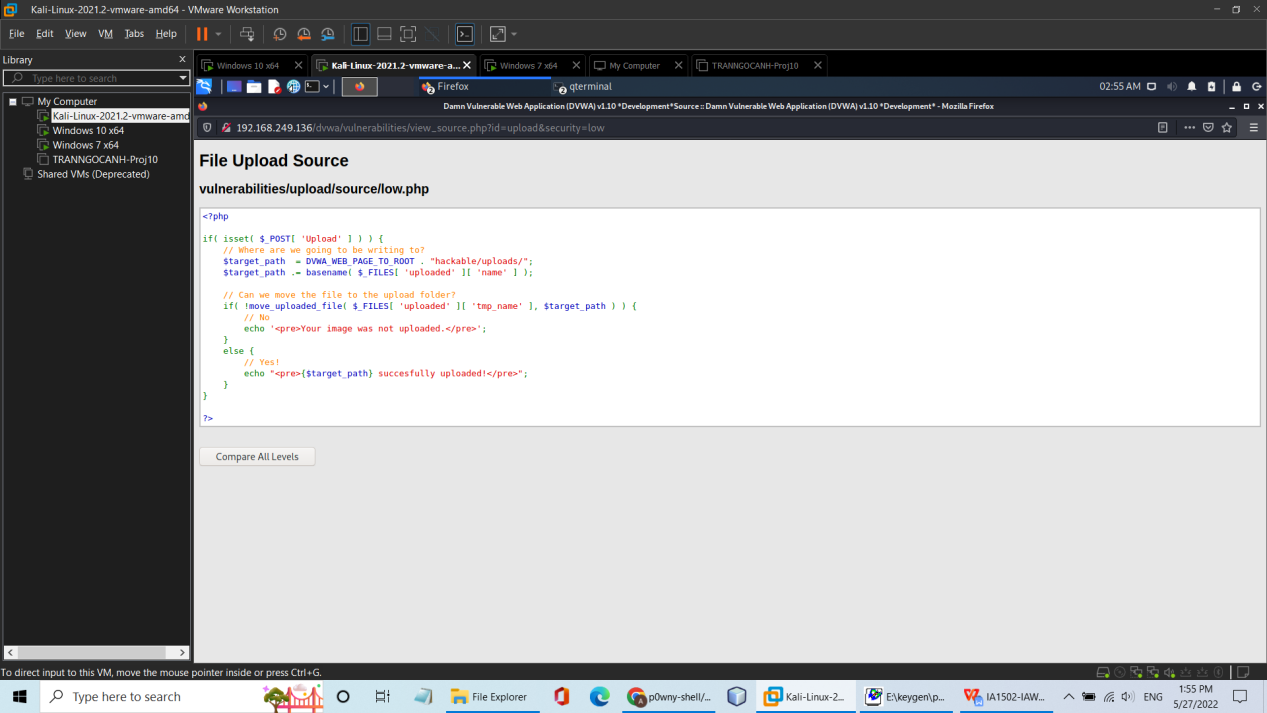
|  |  |
| --- | --- |
| Class | IAW301 |
| Name | Trần Ngọc Anh |
| IC No. | HE151461 |
| Date & Time | 27/5/2022 |

**LAB 9**

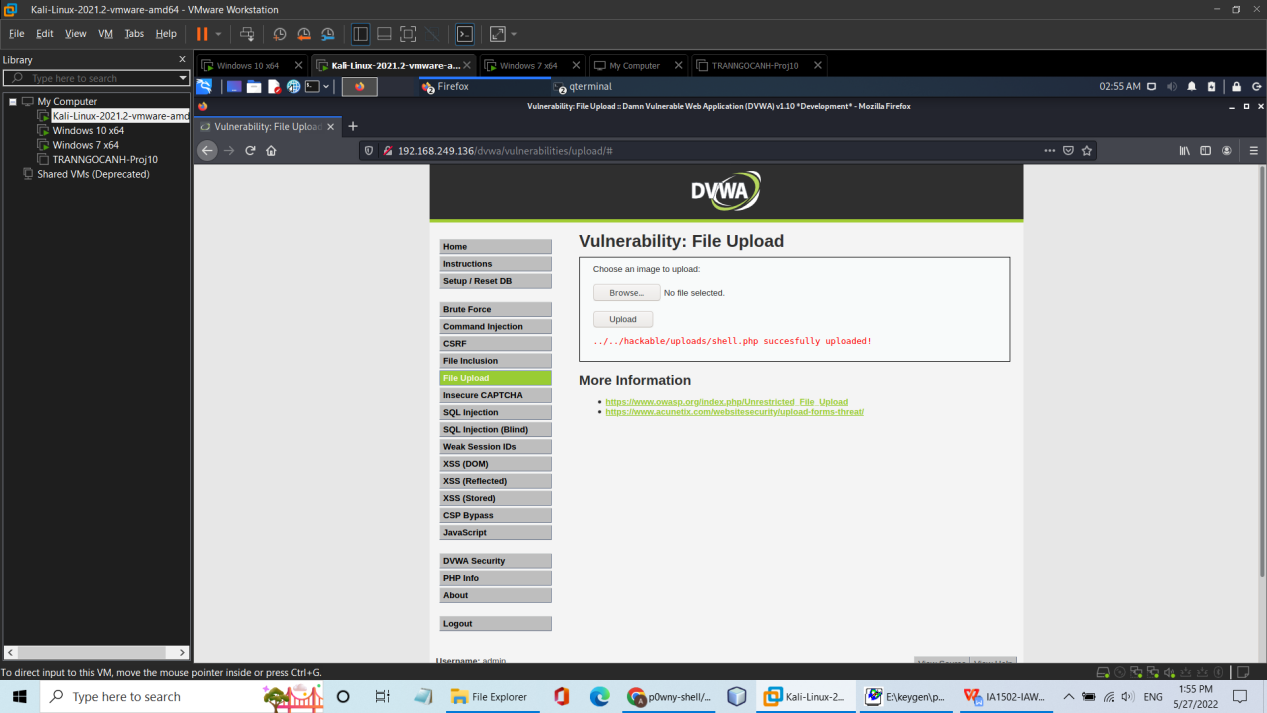
**Unrestricted File Upload**

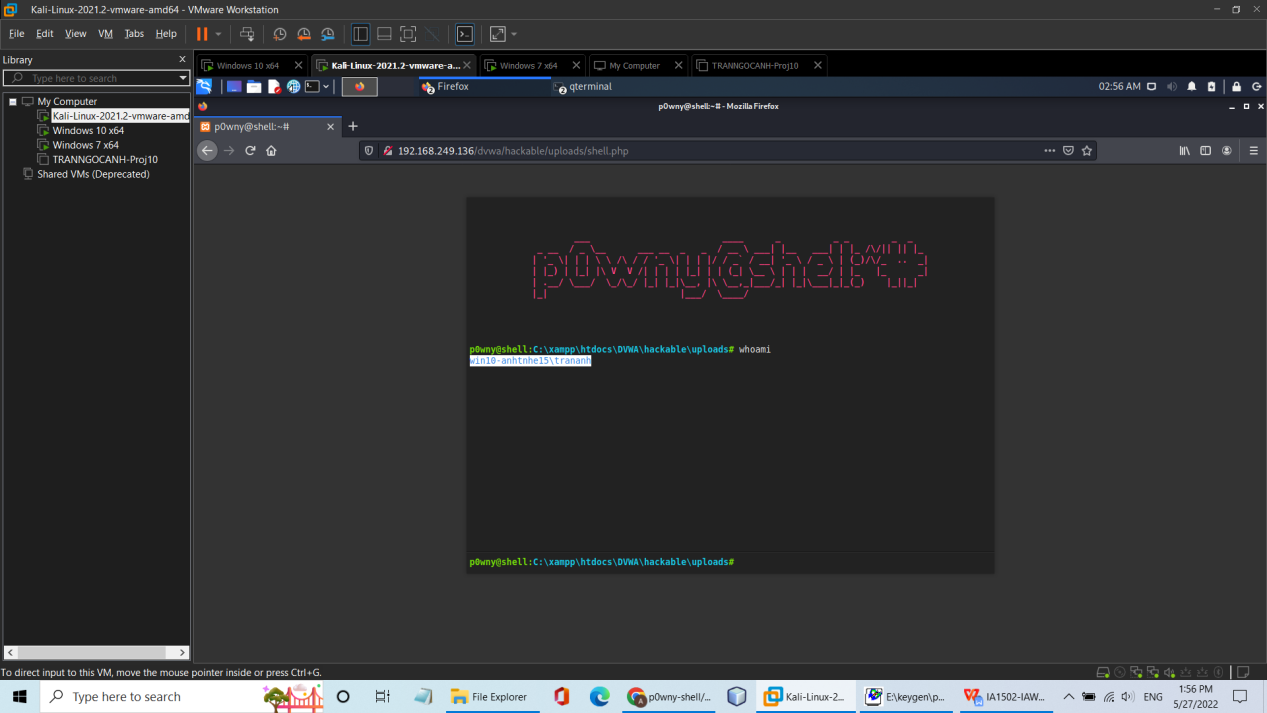
1. **Low**

- Ở mức này chúng ta xem source code và không thấy bất cứ việc check dữ liệu định dạng file được upload lên server.



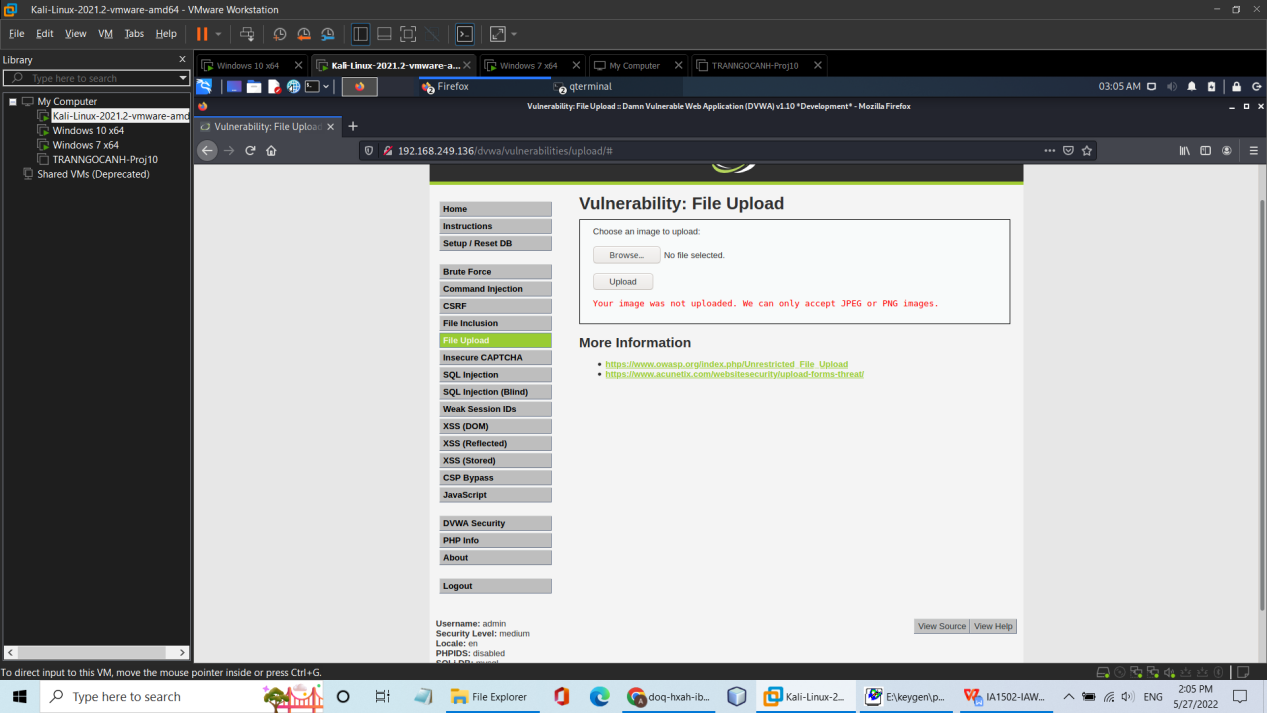
- Vì vậy chúng ta thử upload một file shell.php thành công và đã RCE được.



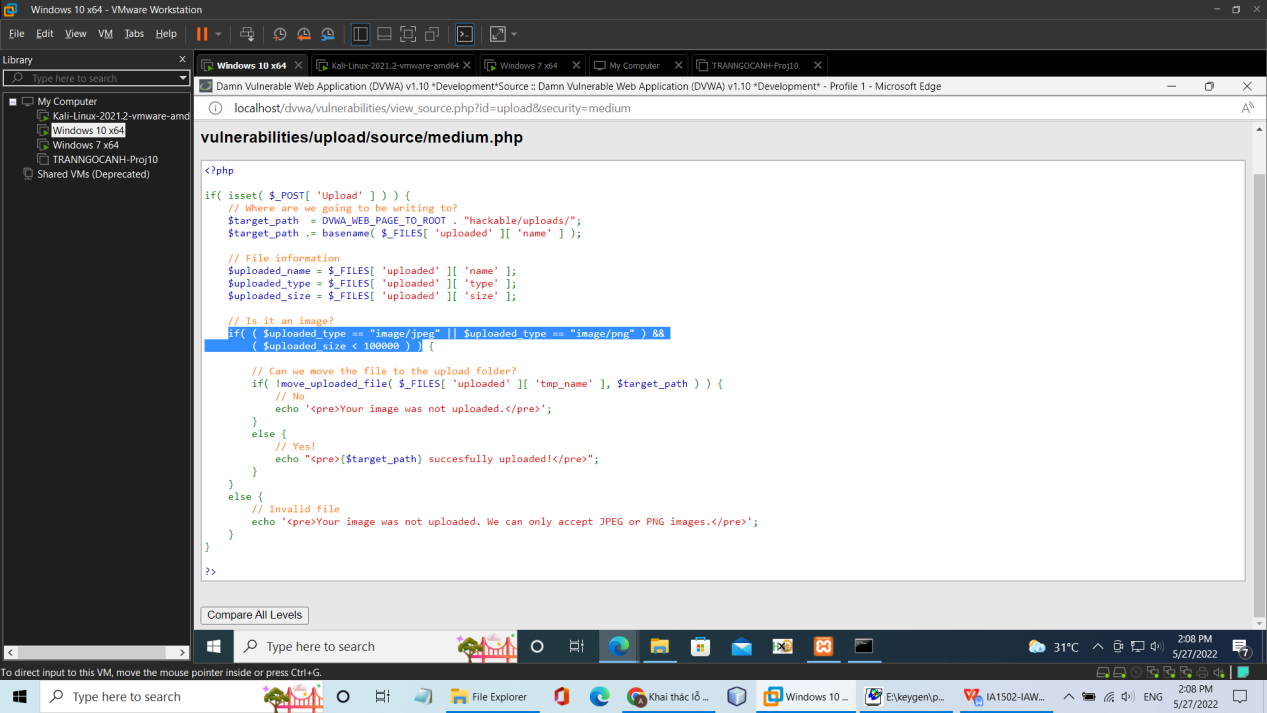


1. **Medium:**

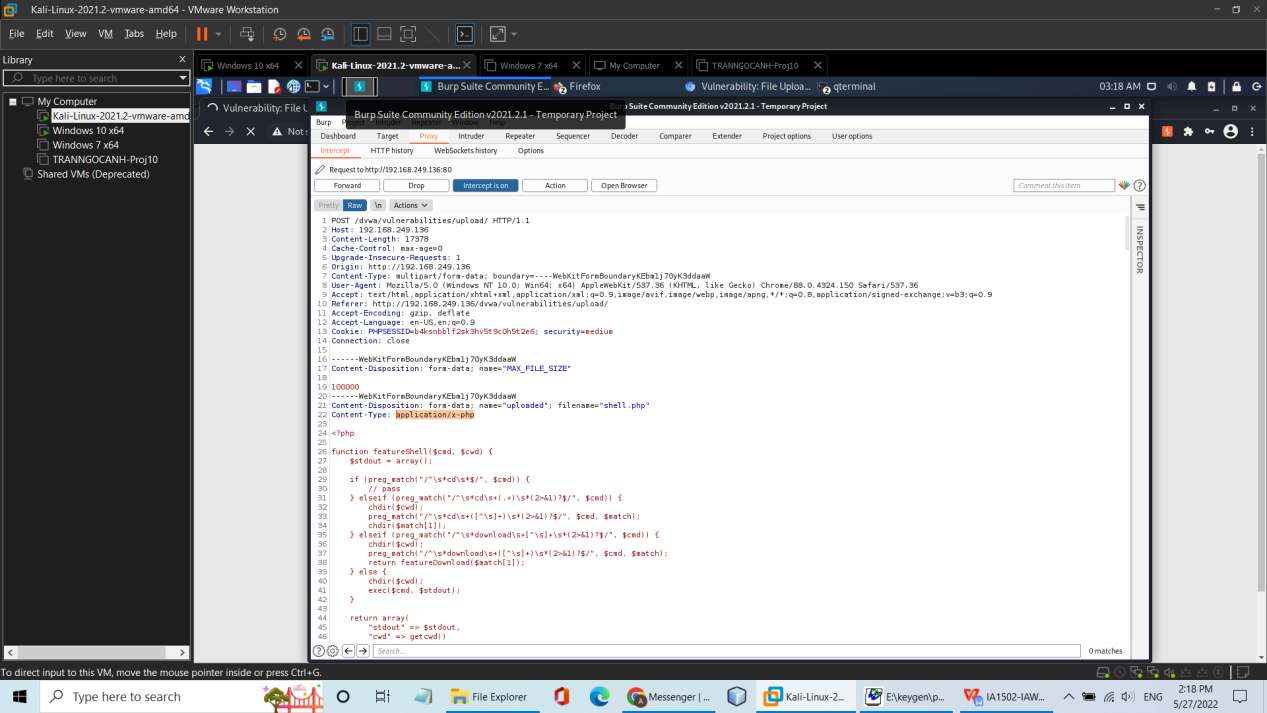
- Ở mức medium, chúng ta thử như ở mức Low nhưng không upload được file shell do nó chỉ chấp nhận file ảnh JPEG hoặc PNG.

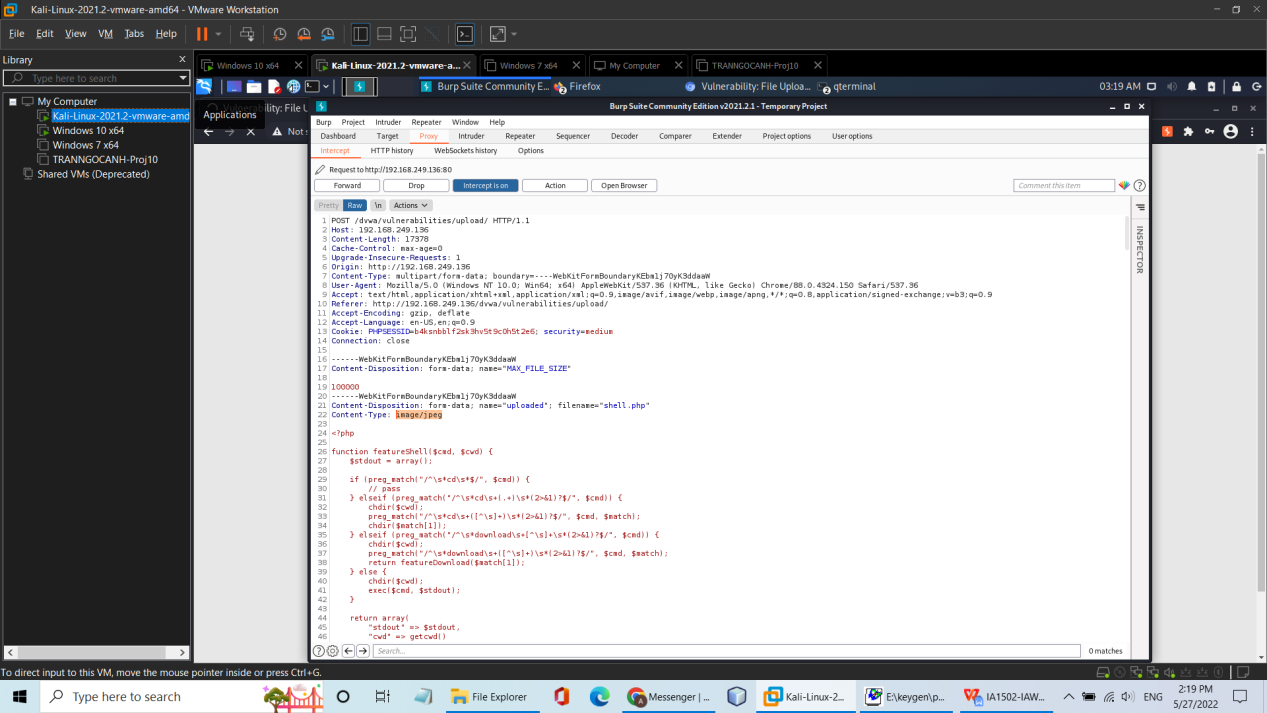


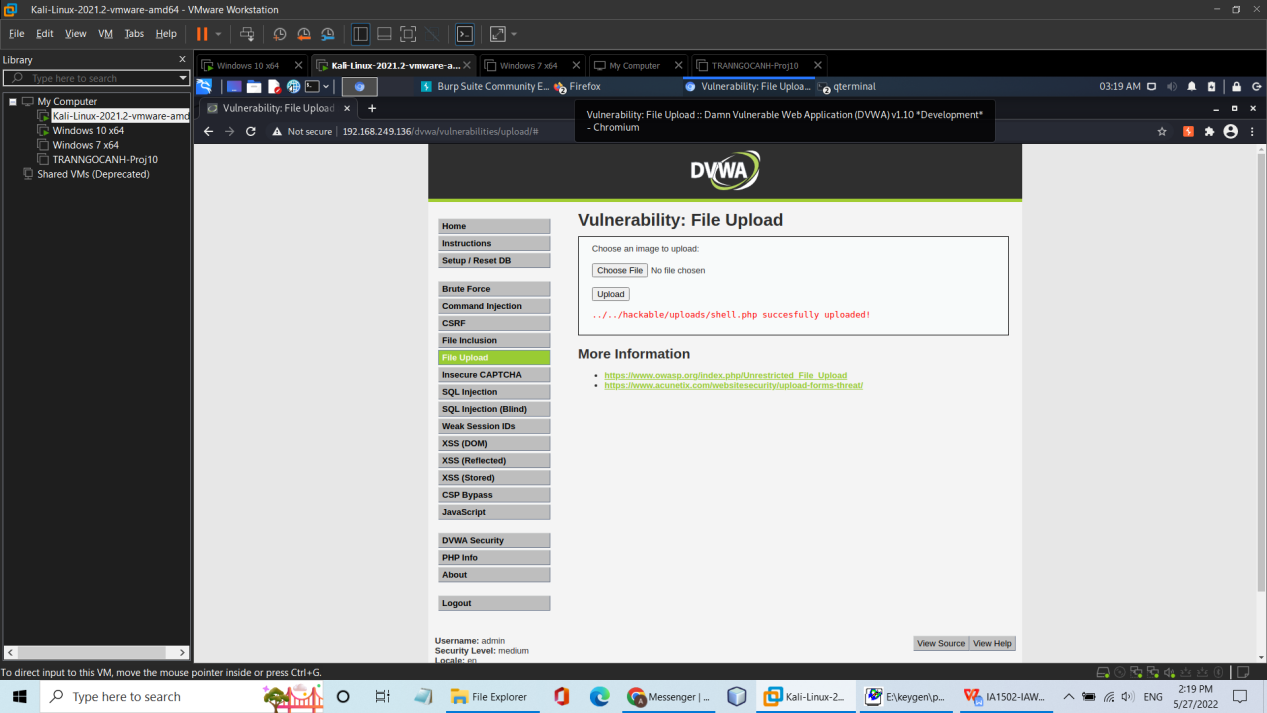
- Nhìn qua source code chúng ta thấy ở đây chỉ kiểm tra đầu vào Content-Type của file có đúng định dạng không chứ không kiểm tra nội dung bên trong.



- Chúng ta dùng Burp Suite để bắt lấy request upload file và tiến hành sửa Content-Type phù hợp để by pass đoạn code check trên.







1. **High:**

- Nhìn qua source code ở mức high , chúng ta thấy ngoài việc check các định dạng extension của file được upload theo mong muốn thì ở đây có một hàm cần lưu ý đó là hàm getimagesize().

- Hàm getimagesize () sẽ đọc 1 lượng byte ban đầu nhất định nhằm xác định xem về định dạng file, chiều rộng cũng như chiều cao của file.



- Để bypass được mức high thì ta sẽ kết hợp sử dụng cả mức medium để khai thác lỗi. Ta chỉ cần thêm đoạn GIF98 vào trước file shell.php để hàm getimagesize() sẽ check đây là 1 file gif. Sau đó, sử dụng burpsuite để bắt và thay đổi content-type là sẽ upload được file shell thành công.

