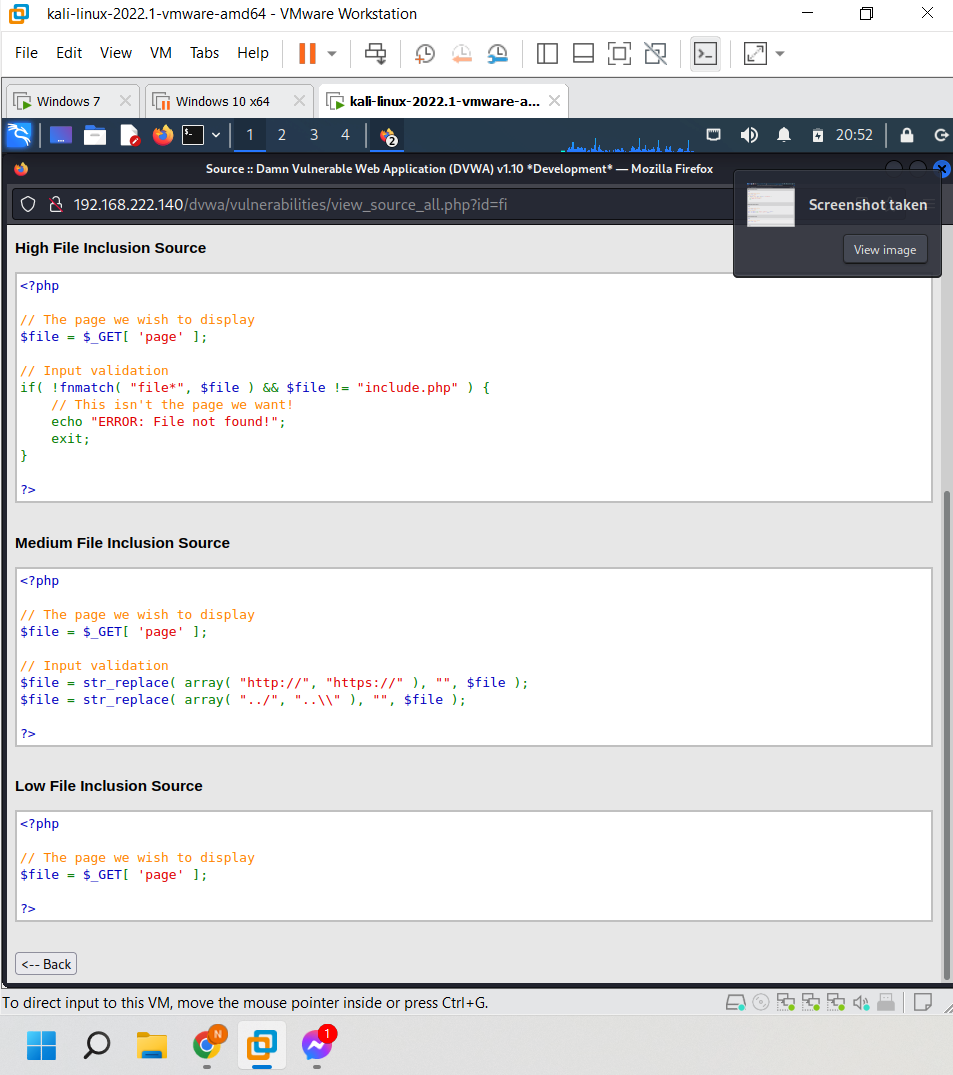
|  |  |
| --- | --- |
| Class | IAW301 |
| Name | Trần Ngọc Anh |
| IC No. | HE151461 |
| Date & Time | 24/6/2022 |

# Lab 21 - File Inclusion

1. **Theo em hiểu File Inclusion là gì?**

**- Lỗ hổng File Inclusion cho phép attacker truy cập trái phép vào những tập tin nhạy cảm trên máy chủ web hoặc thực thi các tệp tin độc hại.** Điều này xảy ra là do trong code php web , lập trình viên đã sử dụng các lệnh include(), require(), include\_once(), require\_once() , các lệnh này cho phép việc file hiện tại có thể gọi ra 1 file khác. **Đồng thời còn do cơ chế kiểm tra đầu vào không được thực hiện tốt, khiến attacker có thể khai thác và chèn các dữ liệu độc hại.**

1. ****Ở mức Medium DVWA phòng chống lại phương thức tấn công File Inclusion như thế nào. Có filter đc pay load sử dụng “..\” hay không và tại sao ?****

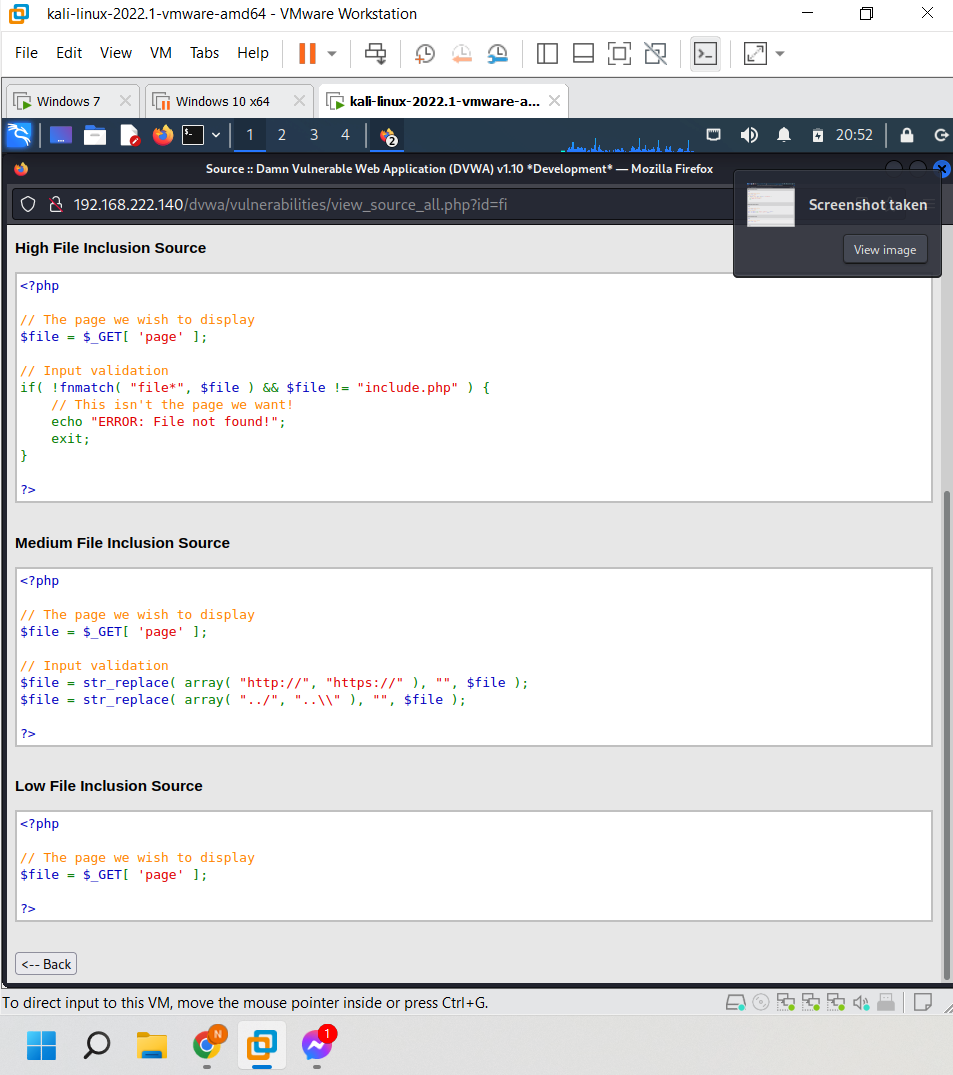
********

- Hàm **str\_replace()** sẽ xoá tất cả các giá trị được gán như là http:// , https:// và các kí tự như ../ , ..\ và thay thế bằng giá trị "" , và trả lại trang ban đầu cho người dùng.

- Không filter được payload “..\” vì nó không xuất hiện trong hàm check của hàm str\_replace() khi lập trình viên viết code.

1. **Ở mức High DVWA phòng chống lại File inclusion như nào. Function php mức này sử dụng là gì, giải thích chức năng của function đó ?**

- Trong hàm check ở mức high chỉ cho phép trỏ đến đúng file include.php , nếu khác file thì sẽ file not found.

********

- Funtion của php ở đây dùng là fnmatch() ở đây dùng để check bắt buộc dữ liệu mình nhập vào phải là một file.