|  |  |
| --- | --- |
| Class & Module | IAW301  Lab 21: File Inclusion |
| Name | Nguyễn Đức Kiên |
| IC No. | HE141763 |
| Date & Time | October 29, 2020 |

**File Inclusion**

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

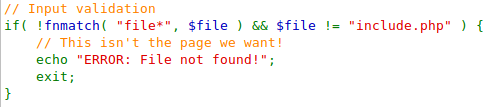
Là một loại lỗ hổng thường thấy ở web app, cho phép kẻ tấn công sử dụng đường dẫn có khả năng truy cập vào các file, thư mục nhạy cảm, từ đó có thể tạo ra các câu lệnh ảnh hưởng trực tiếp đến bề mặt, cơ sở dữ liệu của website.

**2, 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 ?**

Ở mức medium, filter được sử dụng là lọc ra kí tự ‘../’ tuy nhiên không thực sự hiểu quả, điển hình là nếu ta chỉ cần gấp đôi các kí tự trên khi truy cập vào đường dẫn thì vẫn được đưa đến thư mục mong muốn (ví dụ …./…./etc/passwd)

**3, 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 ?**

Ở mức high, DVWA chống file inclusion bằng cách thêm function input validation như sau



Nếu file khác file\*, ta có thể hiểu \* là số file, ví dụ như file1 file2 file3, và file khác file có tên “include.php” thì print ra ERROR như trên, nhưng cách này vẫn chưa thực sự tối ưu, ví dụ khi truy cập vào một file tên là file4.php thì ta vẫn được đưa đến một trang web cụ thể, sau khi xem các write up, để tối ưu code ta có thể dùng cách sau

