**bWAPP**

**Server-Side Includes (SSI) Injection**

Tổng quan về Server-Side Includes (SSI) Injection:

**- Server-Side Includes (SSI) Injection là gì?**

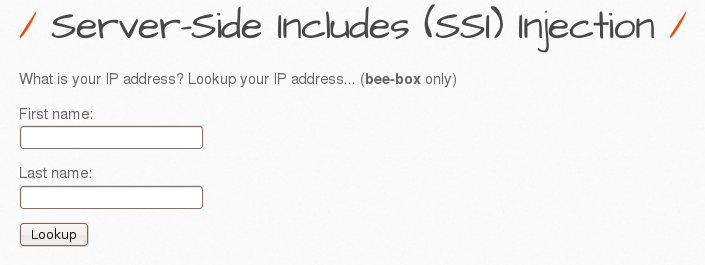
Server-Side Includes (SSI) Injection là một lỗ hổng xảy ra khi kẻ tấn công có thể đưa mã độc hại vào các tập lệnh hoặc trang phía máy chủ được xử lý bởi cơ chế bao gồm phía máy chủ. SSI là công nghệ phía máy chủ cho phép các nhà phát triển bao gồm các tệp bên ngoài hoặc thực thi các quy trình phía máy chủ trong các trang web.

Khi một ứng dụng dễ bị tấn công bởi SSI Injection, kẻ tấn công có thể khai thác lỗ hổng này bằng cách đưa lệnh hoặc lệnh SSI vào các trường đầu vào do người dùng kiểm soát, chẳng hạn như tham số URL, đầu vào biểu mẫu hoặc cookie. Sau đó, các lệnh hoặc lệnh được đưa vào này sẽ được máy chủ xử lý và thực thi, cho phép kẻ tấn công thực hiện nhiều hành động độc hại khác nhau.

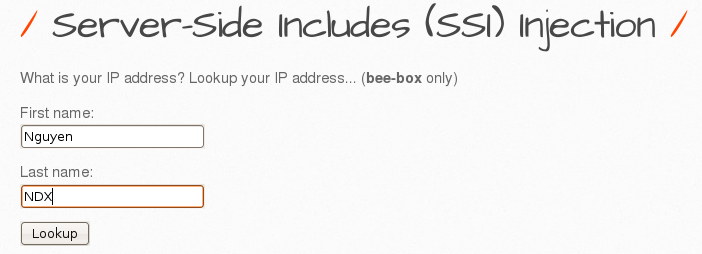
Và sau đây chúng ta sẽ tấn công Server-Side Includes (SSI) Injection với bWAPP

* **Level Low**

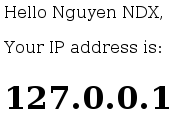
Đây là hình ảnh ban đầu của trang web chúng ta sẽ tấn công vào



Đầu tiên thì ta cứ làm những thao tác bình thường để xem trang web sẽ hoạt động như nào trước hết ta sẽ điền thông tin vào các text box



Và website sẽ trả lại cho ta những thông tin như IP của chúng ta

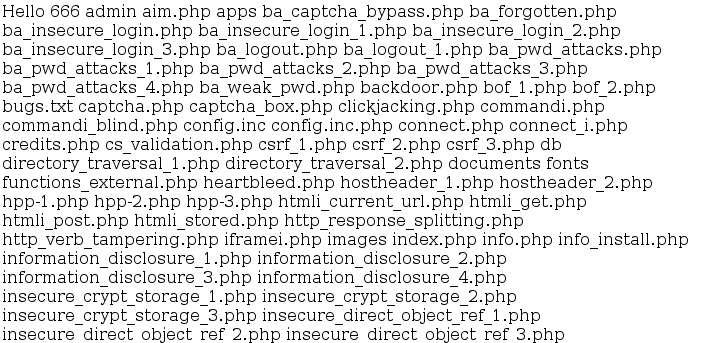


Giờ ta sẽ thử tiêm một vài câu lệnh SSI vào trang web này bằng các thử một vài câu lệnh như sau

<!--#exec cmd="ls" -->

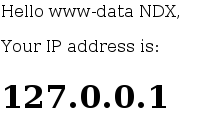


Và ta sẽ được trả lại toàn bộ file trong hệ thống này



Hay ta cũng có thể sử dụng câu lệnh này để biết chúng ta đang sử dụng user nào trong hệ thống

<!--#exec cmd="whoami" -->

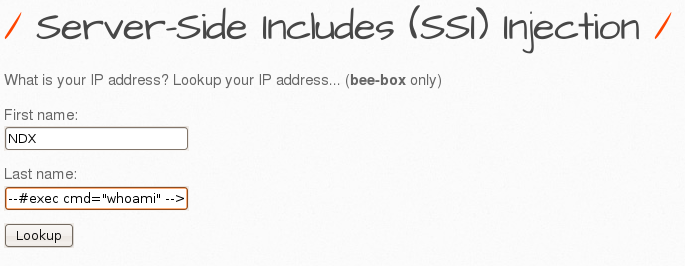


Ta thấy được ta đang ở user www-data

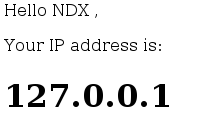
Từ những câu lệnh này chúng ta có thể lấy được dữ liệu của trang web này

* **Level Medium**

Giờ chúng ta sẽ chuyển sang level Medium và thử lại cách tiêm cũ



Và nó đã không còn hoạt động nữa



Và chúng ta sẽ xem qua hàm fiter của trang web đã sử dụng cho level này

switch($\_COOKIE["security\_level"]) {

case "0" :

$data = no\_check($data);

break;

case "1" :

$data = xss\_check\_4($data);

Break;

case "2" :

$data = xss\_check\_3($data);

break;

default :

$data = no\_check($data);

break; }

return $data;}

Ở đây chúng ta thấy được trang web sử dụng hàm xss\_check\_4 để fiter đầu vào ở level Medium

function xss\_check\_4($data){

// addslashes - returns a string with backslashes before characters that need to be quoted in database queries etc.

// These characters are single quote ('), double quote ("), backslash (\) and NUL (the NULL byte).

// Do NOT use this for XSS or HTML validations!!!

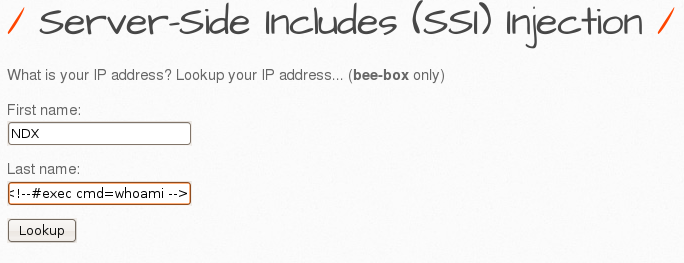
return addslashes($data);

}

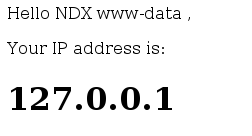
Ở đâu trang web đã sử dụng hàm addslashes() để fiter đầu vào và nó sẽ thêm vào trước những kí tự đặc biệt như “’”,’”’, “\”, và Null và đặt trước nó kí tự “\” và giờ ta sẽ phải tìm cách để đi qua nó.

Ở bài này thì cũng không quá phức tạp chúng ta chỉ cần bỏ đi những kí tự đặc biệt để có thể tiêm vào là được. Ở câu lệnh dưới đâu ta đã bỏ đi 2 ký tự ‘”’ ở whoami để có thể tiêm được SSI

<!--#exec cmd=whoami -->



Và đây là kết quả ta nhân được



Vậy là chúng ta đã thành công để đi qua level Medium Server-Side Includes (SSI) Injection của trang web bWAPP. Còn ở level High được filter bởi htmlspecialchars nên dường như trang web đã không còn lỗ hổng nào chúng ta có thể khai thác được nữa.