

bWAPP

HTML Injection - Reflected (GET)

Tổng quan về HTML Injection:

- HTML là gì?

HTML là một ngôn ngữ đánh dấu mà tất cả các element của website đều được viết trong các thẻ. Nó hầu hết được sử dụng để tạo website. Các trang web sẽ được gửi tới trình duyệt dưới dạng các tài liệu HTML. Sau đó, các tài liệu HTML đó được convert sang website thông thường và hiển thị cho người dùng.

- HTML Injection là gì?

HTML Injection là một loại tấn công mà hacker sẽ tiêm code HTML vào website thông qua những lỗ hổng, với mục đích thay đổi thiết kế hoặc một số thông tin của website, rồi hiển thị cho user. Kết quả user có thể nhìn thấy những dữ liệu mà hacker đã gửi vào.

Những dữ liệu này sẽ khác nhau dựa vào loại tấn công. Nó có thể là 1 vài thẻ HTML, cũng có thể là 1 form hoặc 1 trang web fake. Khi tấn công xảy ra, trình duyệt sẽ hiển thị dữ liệu mà hacker đã tiêm vào.

Thay đổi hiển thị website không phải là rủi ro duy nhất khi cuộc tấn công này xảy ra. Nó cũng tương tự cuộc tấn công XSS, nên hacker có thể dễ dàng lấy cắp danh tính của người dùng.

- HTML Injection - Reflected (GET) xảy ra khi nào?

Reflected GET Injection xảy ra khi dữ liệu đầu vào hiển thị trên website. Giả sử, chúng ta có một trang đơn giản với form tìm kiếm là lỗ hổng cho cuộc tấn công này. Chúng ta sẽ nhập HTML code vào tìm kiếm, nó sẽ xuất hiện trên website cùng một thời điểm, và nó sẽ tiêm vào tài liệu HTML của web.



Hình ảnh minh họa

Và sau đây chúng ta sẽ sử dụng cách tấn công HTML Injection - Reflected (GET) với bWAPP với 2 mức độ Low và Medium

- Level Low

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

Choose your bug: bWAPP v2.2 Hack

Set your security level: low Set Current: low

Bugs Change Password Create User Set Security Level Reset Credits Blog Logout Welcome Bee

/ HTML Injection - Reflected (GET) /

Enter your first and last name:

First name:

Last name:

Go

Twitter LinkedIn Facebook Email

bWAPP is licensed under [CC BY-NC-SA] © 2014 MME BVBA / Follow @MME_IT on Twitter and ask for our cheat sheet, containing all solutions! / Need an exclusive training?

ta có thể thấy được 2 ô để điền thông tin First name và Last name

Giờ ta sẽ điền thử thông tin

Choose your bug: bWAPP v2.2 Hack

Set your security level: low Set Current: low

Bugs Change Password Create User Set Security Level Reset Credits Blog Logout Welcome Bee

/ HTML Injection - Reflected (GET) /

Enter your first and last name:

First name:

Last name:

Go

Twitter LinkedIn Facebook Email

Welcome NDX NDX

Giờ chúng ta sẽ tiêm lệnh HTML vào xem nó sẽ hiển thị gì

Với câu lệnh được tiêm vào là <h1> TEXT

bWAPP
an extremely buggy web app !

Choose your bug:
bWAPP v2.2 Hack

Set your security level:
low Set Current: low

Bugs Change Password Create User Set Security Level Reset Credits Blog Logout Welcome Bee

/ HTML Injection - Reflected (GET) /

Enter your first and last name:

First name:
NDX

Last name:
<h1> you have been hacked

Go

Welcome NDX NDX

Twitter LinkedIn Facebook Email

Và đây là kết quả chúng ta nhận được

bWAPP
an extremely buggy web app !

Choose your bug:
bWAPP v2.2 Hack

Set your security level:
low Set Current: low

Bugs Change Password Create User Set Security Level Reset Credits Blog Logout Welcome Bee

/ HTML Injection - Reflected (GET) /

Enter your first and last name:

First name:

Last name:

Go

Welcome NDX

/ you have been hacked /

Twitter LinkedIn Facebook Email

Vậy là ta đã thành công trong việc sử dụng HTML Injection-Reflected(GET) với level Low

- Level Medium

bWAPP
an extremely buggy web app !

Choose your bug:
bWAPP v2.2 Hack

Set your security level:
low Set Current: medium

Bugs Change Password Create User Set Security Level Reset Credits Blog Logout Welcome Bee

/ HTML Injection - Reflected (GET) /

Enter your first and last name:

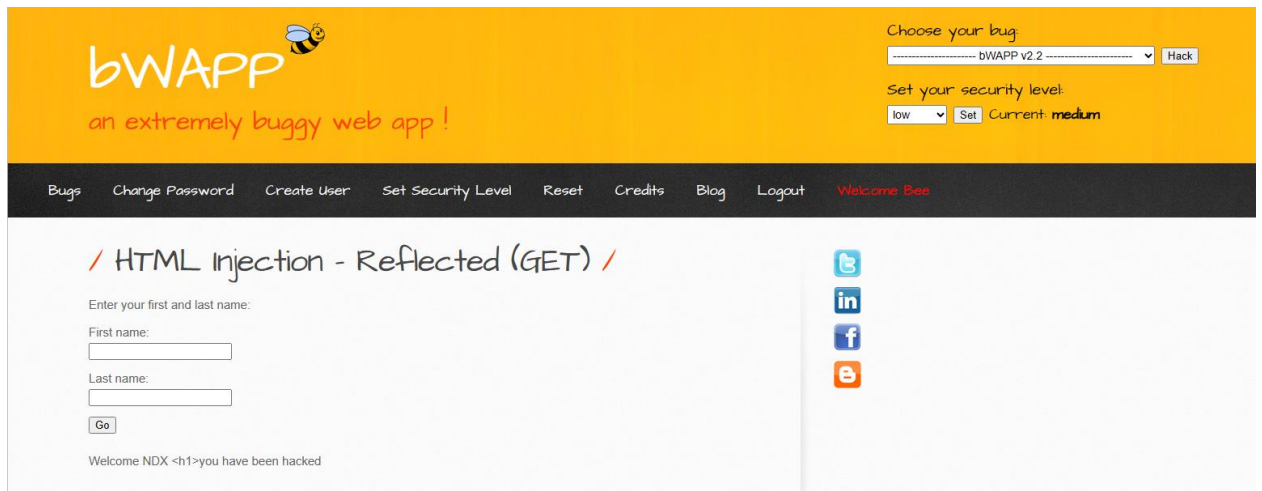
First name:

Last name:

Go

Twitter LinkedIn Facebook Email

Với level Medium chúng ta sẽ thử lại cách mà chúng ta đã dùng với low



The screenshot shows the bWAPP web application interface. The header is orange with the bWAPP logo and a bee icon. Below the logo, it says "an extremely buggy web app!". On the right, there's a "Choose your bug" dropdown menu set to "bWAPP v2.2" and a "Hack" button. Below that, there's a "Set your security level" section with a dropdown menu set to "low", a "Set" button, and "Current: medium". The navigation bar is dark grey with links: Bugs, Change Password, Create User, Set Security Level, Reset, Credits, Blog, Logout, and Welcome Bee. The main content area is light grey and titled "/ HTML Injection - Reflected (GET) /". It contains a form with the label "Enter your first and last name:", two input fields for "First name:" and "Last name:", and a "Go" button. Below the form, it says "Welcome NDX <h1>you have been hacked". On the right side of the main content area, there are social media icons for Twitter, LinkedIn, Facebook, and YouTube.

Nó đã không còn thanh công nữa và đã hiển thị lại câu lệnh chúng ta tiêm vào

Giờ chúng ta sẽ sử dụng công cụ Burp Suite để tiếp tục công việc khai thác

Và ta thấy được những gì chúng ta gõ vào trong trang web sẽ ra kết quả như này

Request

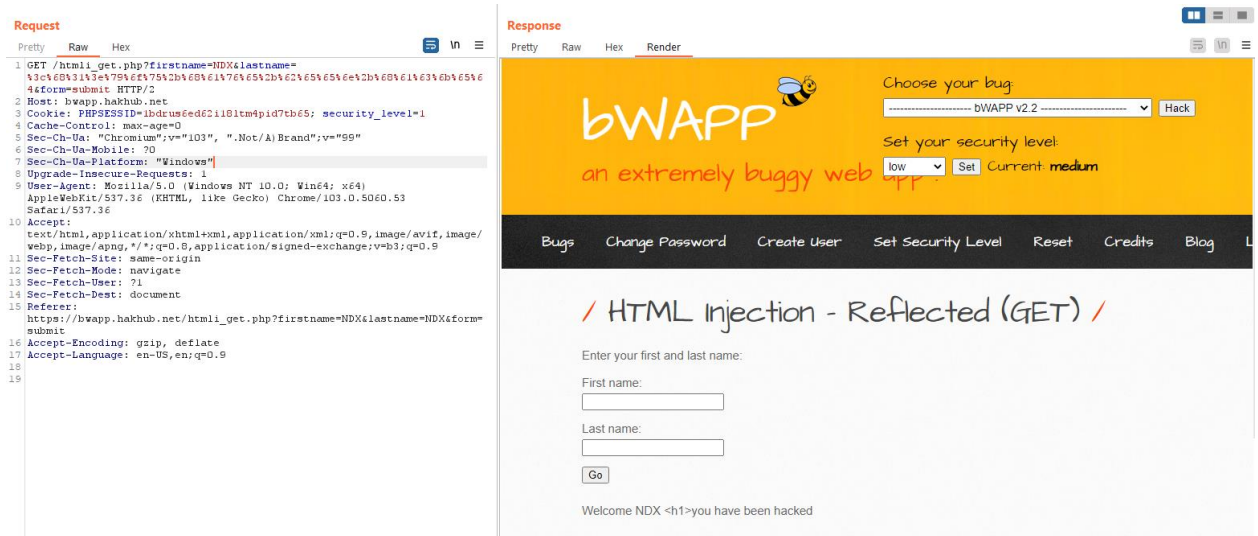
Pretty Raw Hex

```
1 GET /htmli_get.php?firstname=NDX&lastname=%3C%3Eyou+have+been+hacked&
  form=submit HTTP/2
2 Host: bwapp.hakhub.net
3 Cookie: PHPSESSID=1bdrus6ed62i18ltm4pid7tb65; security_level=1
4 Cache-Control: max-age=0
5 Sec-Ch-Ua: "Chromium";v="103", ".Not/A) Brand";v="99"
6 Sec-Ch-Ua-Mobile: ?0
7 Sec-Ch-Ua-Platform: "Windows"
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
  AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.5060.53
  Safari/537.36
10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/
  webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?1
14 Sec-Fetch-Dest: document
15 Referer: https://bwapp.hakhub.net/htmli_get.php?firstname=NDX&lastname=NDX&form=
  submit
16 Accept-Encoding: gzip, deflate
17 Accept-Language: en-US,en;q=0.9
18
19
```

Ta thấy được 2 dấu “<” “>” đã được chuyển thành %3C và %3E và ở đây 2 dấu này đã được mã hóa URL khi được chuyển vào vậy nên ta sẽ thử chuyển câu lệnh ta muốn tiêm vào thành encode của URL và ta được kết quả

<h1>you+have+been+hacked	<input checked="" type="radio"/> Text <input type="radio"/> Hex
	Decode as ...
	Encode as ...
	Hash ...
	Smart decode
%3C%68%31%3e%79%6f%75%2b%68%61%76%65%2b%62%65%65%6e%2b%68%61%63%6b%65%64	<input checked="" type="radio"/> Text <input type="radio"/> Hex
	Decode as ...
	Encode as ...
	Hash ...
	Smart decode

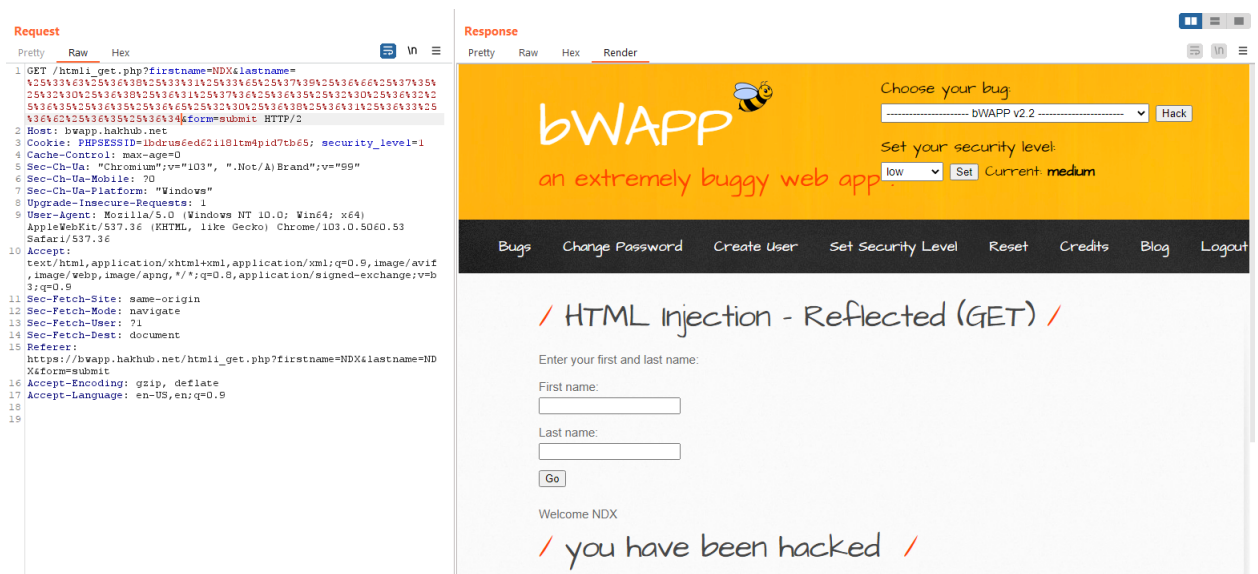
Sau khi chèn đoạn code đã được mã hóa vào ta sẽ có kết quả



Ở đây ta thấy được đoạn code đã được định ngược lại và không giống với những gì chúng ta đã tiêm vào chúng tỏ nó đã dịch mã mà chúng ta gửi vào, giờ ta sẽ thử encode một lần nữa vào tiêm vào xem kết quả chúng ta nhận được là gì



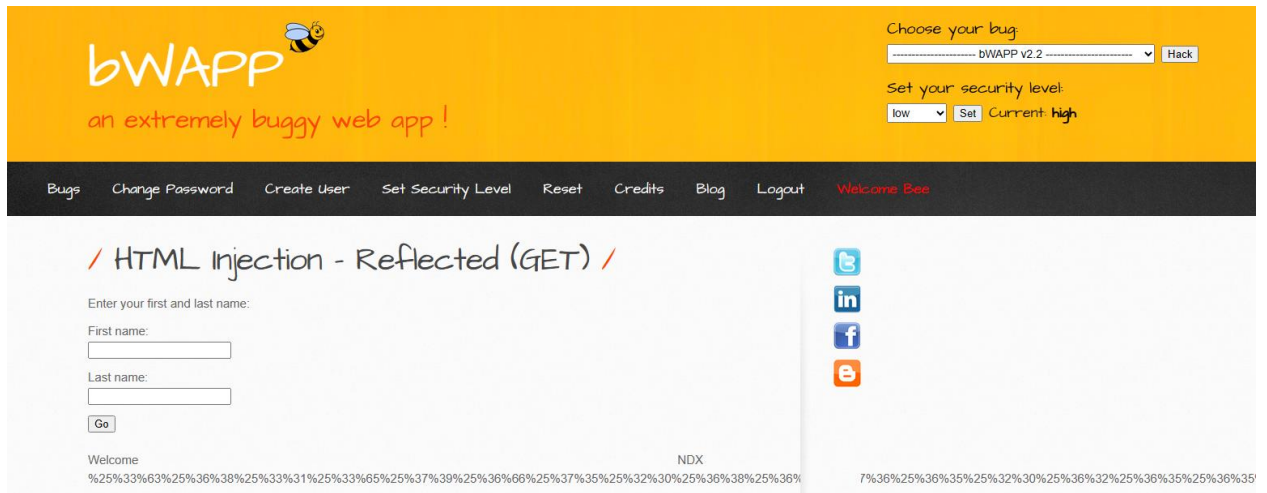
Và ta sẽ có kết quả thu được



Vậy là ta đã thành công qua 2 level của HTML Injection- Reflected (GET)

- Level High

ở level này chúng ta đã không thể dùng mã hóa để tấn công nữa



Giờ chúng ta sẽ phải đi xem source code của trang web



Sau khi xem source code ta đã thấy được

Ở level low không có một filter nào để check những gì chúng ta đã nhập vào

Ở level medium ta thấy được một hàm xss_check_1

Code của hàm xss_check_1

```
function xss_check_1($data)
{

    // Converts only "<" and ">" to HTLM entities
    $input = str_replace("<", "<", $data);
```

```

$input = str_replace(">", ">", $input);

// Failure is an option
// Bypasses double encoding attacks
// <script>alert(0)</script>
// %3Cscript%3Ealert%280%29%3C%2Fscript%3E
// %253Cscript%253Ealert%25280%2529%253C%252Fscript%253E
$input = urldecode($input);

return $input;

}

```

Ở đây ta đã thấy được web bắt đầu lọc đầu vào và đã chuyển những ký tự như “<” và “>” thành thực thể HTML, và chúng ta thấy thêm được web đã chặn những cuộc tấn công bằng double encoding

Ở level High ta thấy được hàm xss_check_3

Code của hàm xss_check_3

```

function xss_check_3($data, $encoding = "UTF-8")
{
    // htmlspecialchars - converts special characters to HTML entities
    // '&' (ampersand) becomes '&'
    // '"' (double quote) becomes '"' when ENT_NOQUOTES is not set
    // "'" (single quote) becomes "'" (or '"') only when ENT_QUOTES is set
    // '<' (less than) becomes '<'
    // '>' (greater than) becomes '>'

    return htmlspecialchars($data, ENT_QUOTES, $encoding);
}

```



```
}
```

Ở đây ta đã thấy được hàm `htmlspecialchars()` có tác dụng chuyển đổi toàn bộ những gì ta nhập vào thành thực thể HTML vì vậy chúng ta không thể tấn công một cách bình thường được. Nhưng nếu bạn ở trong hệ thống của trang web và bạn có thể vào được file `.htaccess` và thêm dòng mã `AddDefaultCharset UTF-7` và thì trang web sẽ được chuyển sang mã hóa UTF-7 vì những kí tự “>”, “<”, “” có điểm mã khác với UTF – 8 nên có thể đi qua filter của trang web