

www.itsecgames.com  
software: bee-box/bWAPP

Report type (1-2): **2**

**1** - problem

**2** - solution

GNU GPL

© 2014

Severity (1-4): **1**

**1** - Critical

**2** - Major

**3** - Minor

**4** - Cosmetic

Bug report # **1**

version: **2.2**

Additions (y/n): **y**

If yes, which ones?

**screenshots**

**descriptions**

## FEATURE:

A1 HTML injection reflected (GET/POST) security level: low

## PROBLEM:

Mismatch between actual behavior of the application and its expected behavior.

## CAN YOU REPRODUCE THE PROBLEM SITUATION? (y/n):

Yes

## PROBLEM DESCRIPTION:

Text input form does not support HTML tag validation.

## TEST CASE:

1. Get the url: [http://192.168.0.104/bWAPP/htmli\\_get.php](http://192.168.0.104/bWAPP/htmli_get.php)
2. Enter data:  
First name: "<h1>Hacked</h1>";  
Last name: "<p></p>";
3. Submit the form;
4. Check the actual behavior - html tag h1 was added into the page source.

## SUGGESTED CORRECTION (OPTIONAL):

Data that has been entered into the form must be validate.

provided by: **Prytula Nick**

date: **28.01.2019**

## A1 injection: HTML injection - reflected(GET/POST)

### Bug report #1 additions;

#### Actual behavior:

/ HTML Injection - Reflected (POST) /

Enter your first and last name:

First name:

Last name:

Welcome

/ HACKED /

// hacked //

/ HTML Injection - Reflected (POST) /

Enter your first and last name:

First name:

Last name:

Welcome

/ fname /

// lname //

#### Expected behavior:

/ HTML Injection - Reflected (POST) /

Enter your first and last name:

First name:

Last name:

Welcome <h1>HACKED</h1> <p></p>

#### SUMMARY:

HTML injection is a type of injection issue that occurs when a user is able to control an input point and is able to inject arbitrary HTML code into a vulnerable web page. This vulnerability can have many consequences, like disclosure of a user's session cookies that could be used to impersonate the victim, or, more generally, it can allow the attacker to modify the page content seen by the victims.