www.itsecgames.com	**GNU GPL**	**Bug report # 1**
software: bee-box/bWAPP	**© 2014**	**version: 2.2**
Report type (1-2): 2	**Severity (1-4): 1**	**Additions (y/n): y**
1 - problem	**1 - Critical**	**If yes, which ones?**
2 - solution	**2 - Major**	**screenshots**
	3 - Minor	**descriptions**
	4 - Cosmetic	

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
2. Fill in the form with data:
   First name: “<h1>Hacked</h1>”;
   Last name: “ ”;
3. Submit the form;
4. Check the actual behavior - html tag h1 was added into the page source.

SUGGESTED CORRECTION (OPTIONAL):

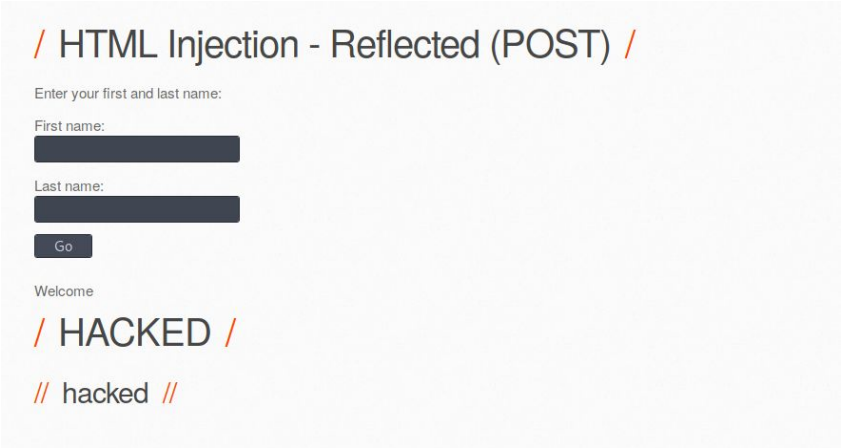
Data that has been entered into the form must be validate.

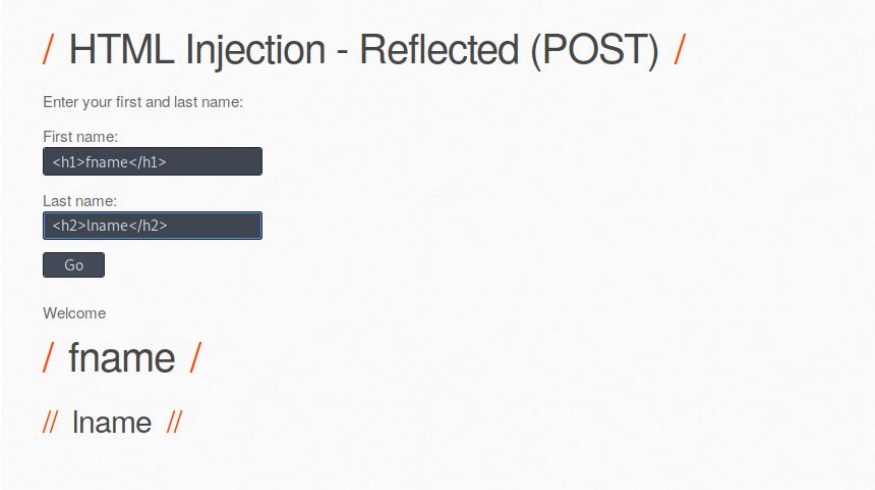
provided by: **Prytula Nick** **date:** **28.01.2019**

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

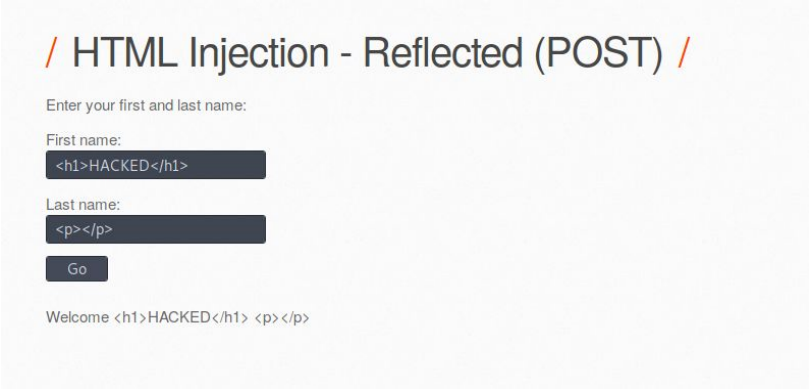
Bug report #1 additions;

Actual behavior:





Expected behavior:



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.