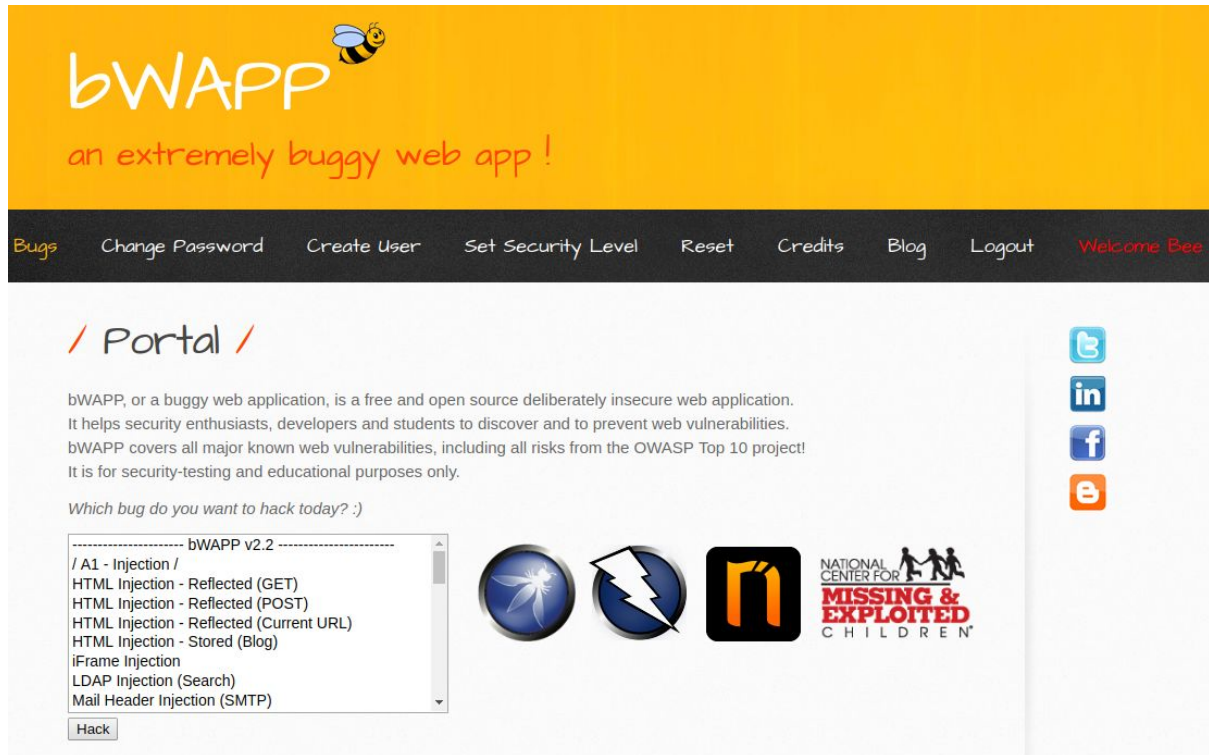


BEE-BOX bWAPP bugs description

by Prytula Nick



This error description is in addition to the automated testing cycle for this application. The test code is in the git repository.

https://github.com/Nickolazz1/OWASP_BWA_automation

A1 injection: HTML injection - reflected(POST)

hacked by: Prytula Nick

Id: 3

priority: several

Expected result:

<p>/ HTML Injection - Reflected (POST) /</p> <p>Enter your first and last name:</p> <p>First name: <input type="text" value="fname"/></p> <p>Last name: <input type="text" value="lname"/></p> <p><input type="button" value="Go"/></p> <p>Welcome fname lname</p>	<p>/ HTML Injection - Reflected (POST) /</p> <p>Enter your first and last name:</p> <p>First name: <input type="text" value="<h1>HACKED</h1>"/></p> <p>Last name: <input type="text" value="<p></p>"/></p> <p><input type="button" value="Go"/></p> <p>Welcome <h1>HACKED</h1> <p></p></p>
--	--

Actual result:

/ 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 //

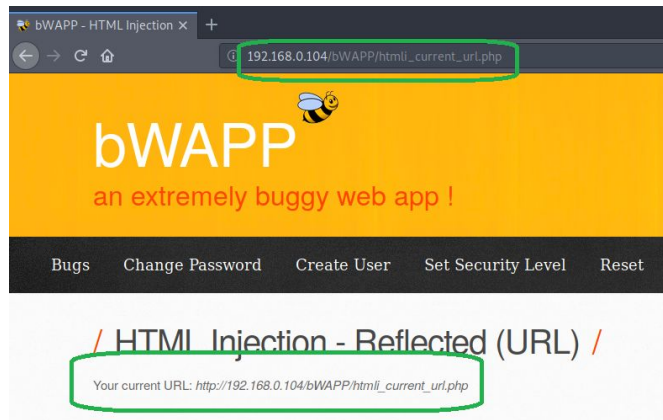
A1 injection: HTML injection - reflected(current url)

hacked by: Prytula Nick

Id: 4

priority: critical

Expected result:



Actual result:

intercept REST queries, change response data and forward link into user client:

