

HTML INJECTION – REFLECTED (GET)

As Observed the user input values has been reflected by the page.

The screenshot shows a web browser window for the bWAPP - HTML Injection application. The URL is https://bwapp.hakhub.net/html_get.php?firstname=abc&lastname=xyz&form=submit. The page title is "bWAPP - HTML Injection". The main content area displays the text "/ HTML Injection - Reflected (GET) /". Below it, there is a form with fields for "First name:" containing "abc" and "Last name:" containing "xyz". A "Go" button is present. To the right of the form are social media sharing icons for Twitter, LinkedIn, Facebook, and Email. The page footer includes a license notice: "bwAPP is licensed under [CC BY-NC-ND] © 2014 MME BVBA / Follow @MME_IT on Twitter and ask for our cheat sheet, containing all solutions! / Need an exclusive training?"

Hence, we can try to inject basic html code in any of the input field.

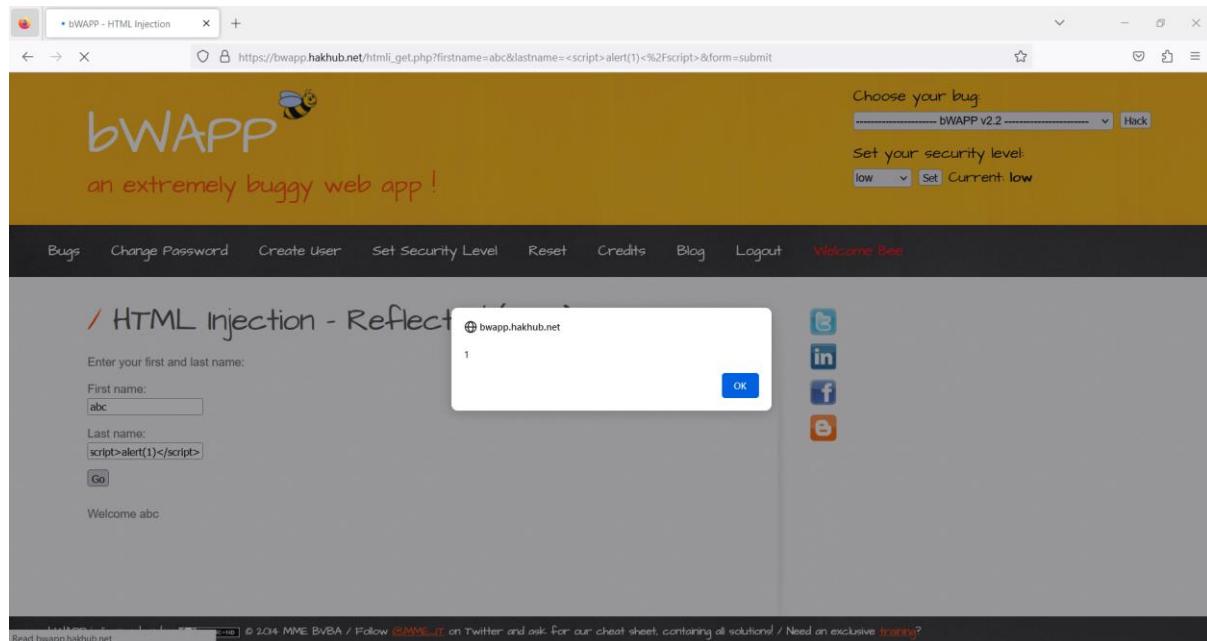
- - -> <h1> Hello </h1>

And here the injected request gets executed and is reflected on the page

The screenshot shows the same bWAPP - HTML Injection application. The URL is https://bwapp.hakhub.net/html_get.php?firstname=abc&lastname=<h1>Hello<%2Fh1>&form=submit. The page content and form fields are identical to the previous screenshot, but the output in the "Welcome abc" box now reflects the injected HTML: "/ Hello /". This demonstrates that the application is reflecting user input back to the user without proper sanitization.

Similarly, tried to inject a simple script for generating alert

---> <script> alert(1) </script>



CHALLENGE SOLVED...!!