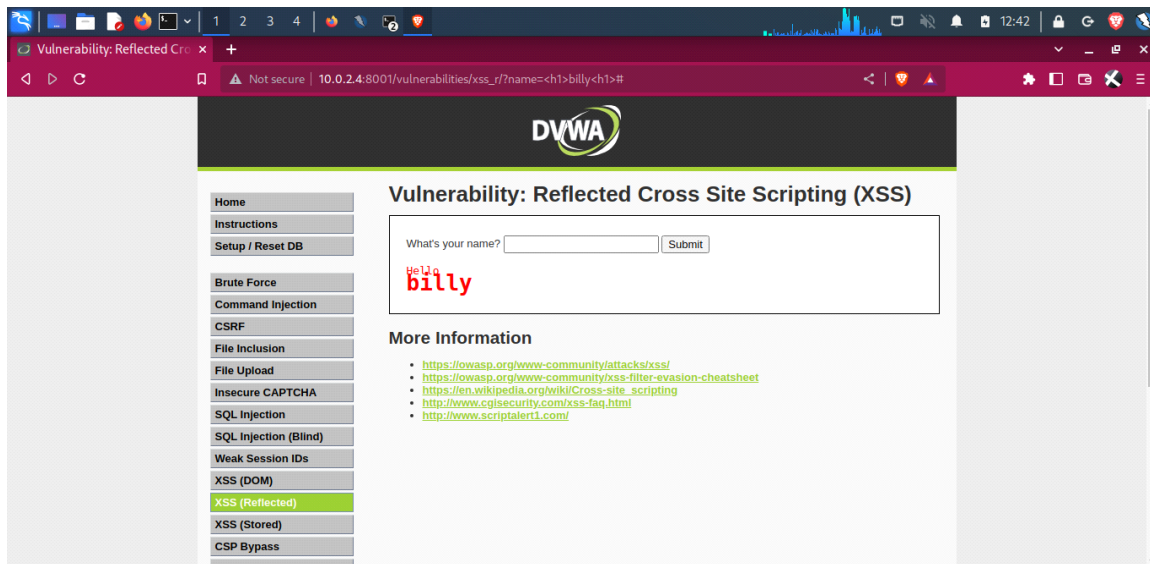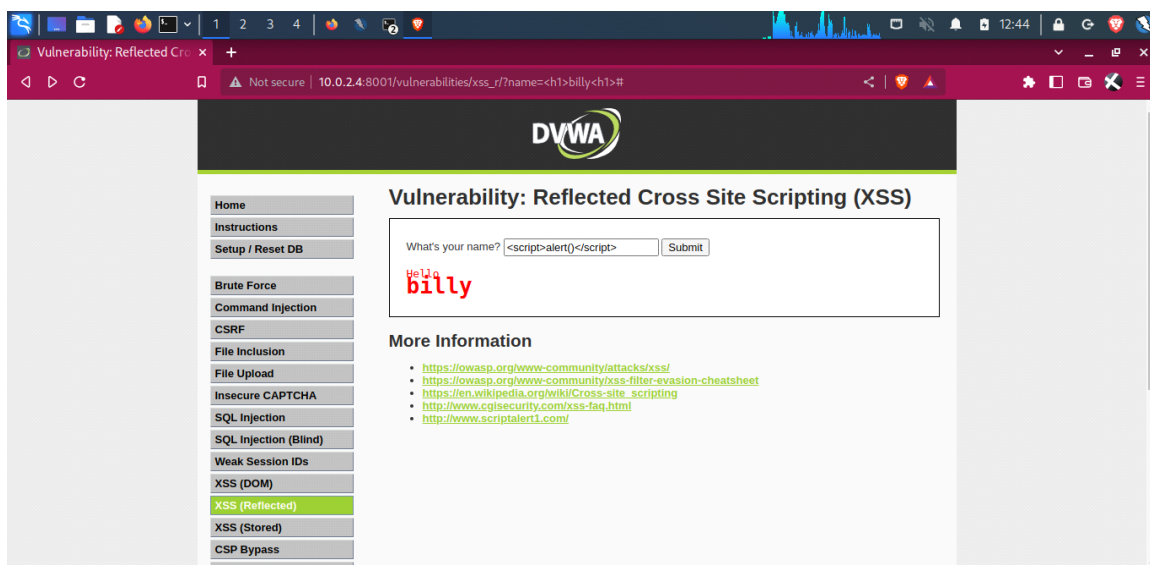Reflected Cross site scripting when URL parameters are passed to the application and are handled inside the page itself, causing the HTML to change

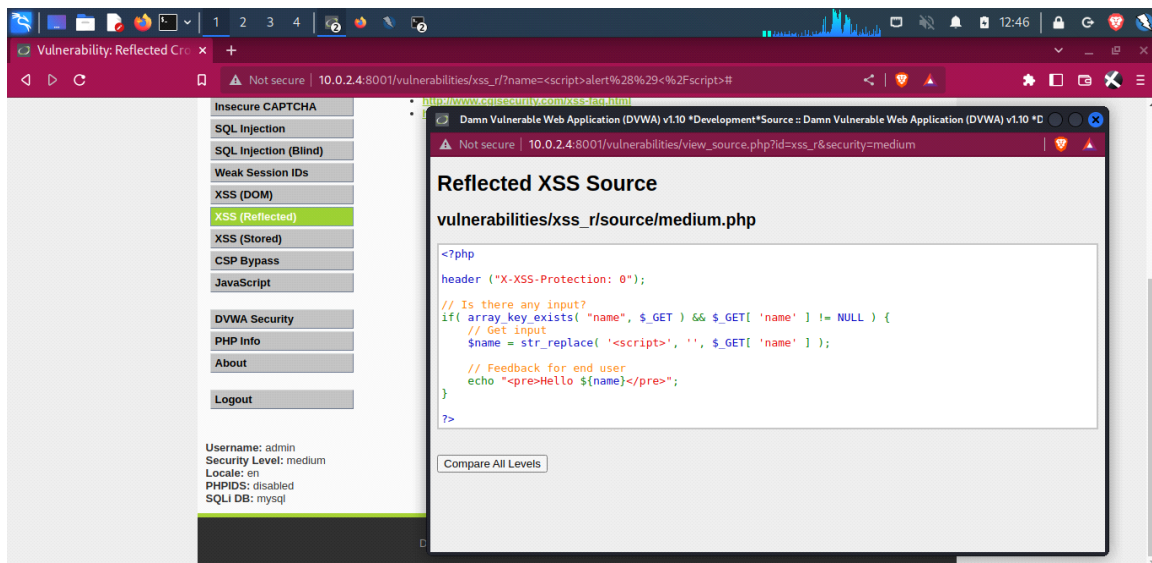We have an input here, so we test the action with complying , adding a name but I also added the arbitrary html <h1>billy</h2> . We see the input is 'reflected' onto the webpage with the arbitrary html code making the name bold.
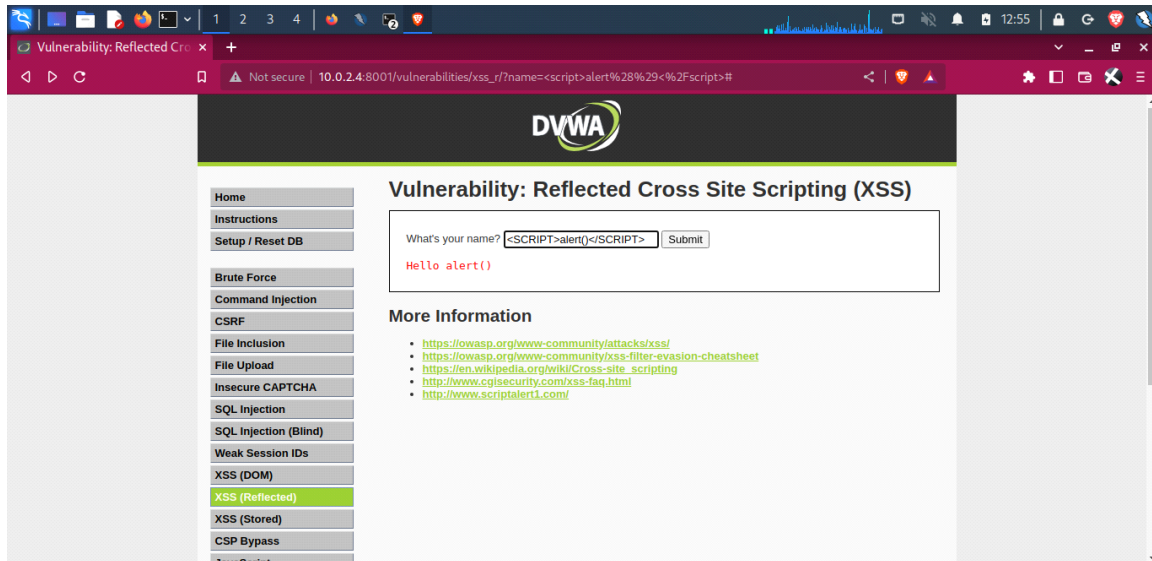

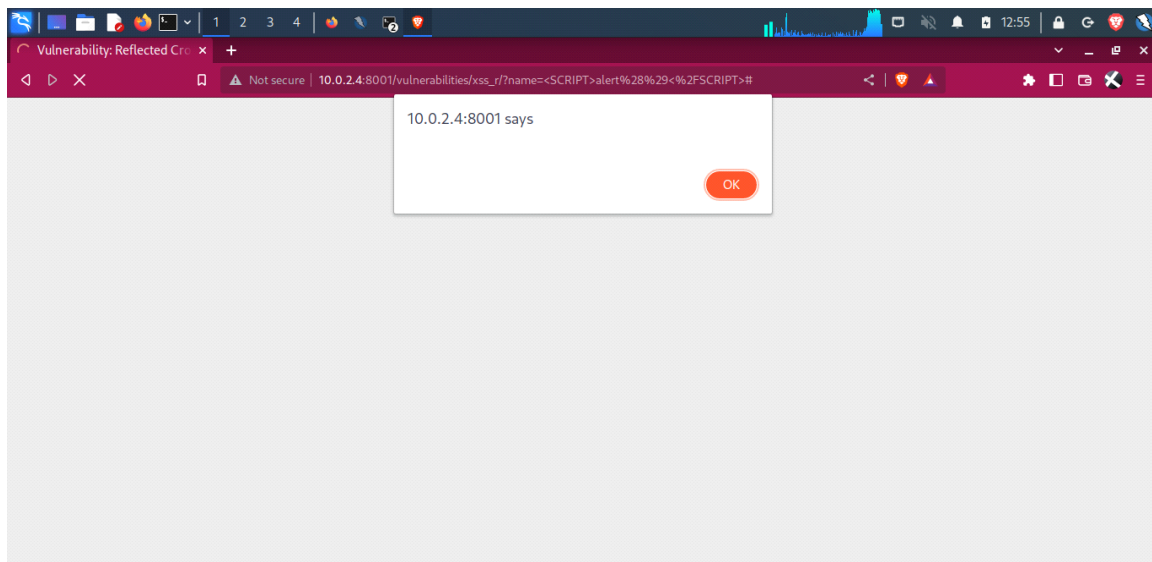The next step I try to add a <script>alter()</script> pop up
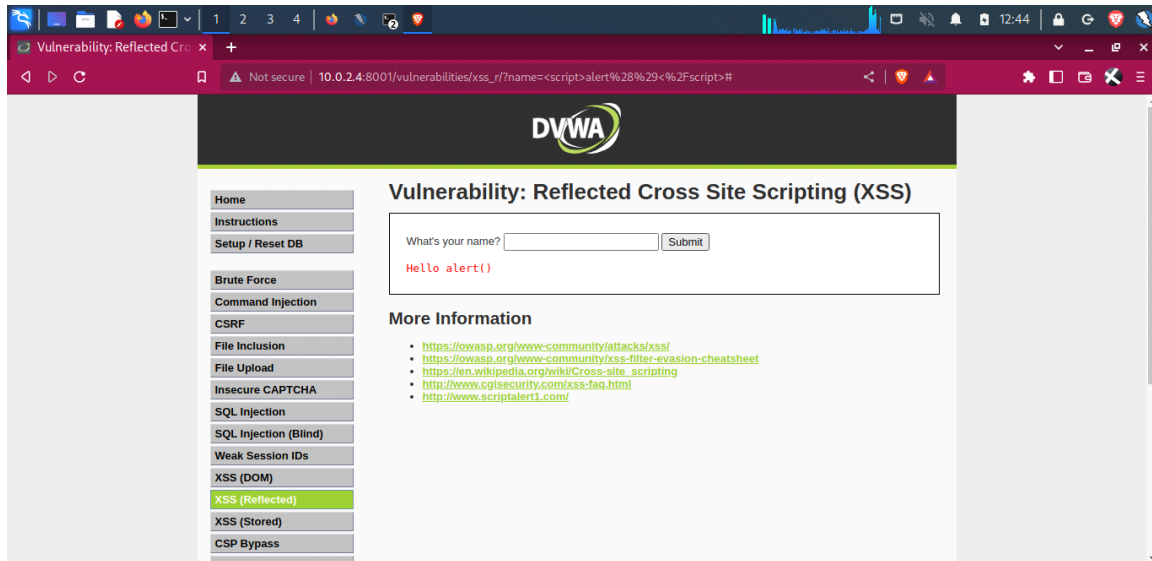
we see that script is being filtered

If we examine the source code we see that the specific word <script>is being filtered out

Because html does not care if the script is in uppercase or lower, but the filter does - as in it is case sensitive. I try writing the <script> but simply put it in uppercase

And it works fine.