A screenshot of a computer

Description automatically generated

XSS Reflected vulnerability can be found in the JavaScript code executed when the user enters the /dashboard html page. In lines 3,4 of greet.js file code gets the username from the URL without any sanitation , it just decodes it which doesn’t apply any filter for <script> and etc. The payload is sent to server as a request, server does not filter it as seen in the code and then sends it back to the client as a response resulting in a ‘Reflected Attack’.

Dom Xss vulnerability can be found in the next line of the same file (line5). Document.write is used and the input of this document.write is given again by the URL, (#..) which is treated as a fragment resulting in the browser to not forwarding it back to the server. The browser updates the DOM (the html body of the page) to contain Welcome <script> … </script> , then the browser finds the script and executes it.

http://139.91.71.5:11337/dashboard#%3Cscript%3Ealert(123)%3C/script%3E

A screenshot of a computer

Description automatically generated

<http://139.91.71.5:11337/dashboard#%3Cscript%3E%20var%20navAgt%20=%20navigator.userAgent;%20if%20(navAgt.indexOf(%22MSIE%22)!=-1)%20{%20document.write(%22DOM-XSS%20Vulnerabillity%20Detected%20%20:%20%22%20+%20document.location.href%20+%20%22.%22);%20}%20else%20{%20document.write(%22DOM-%20XSS%20Vulnerabillity%20Detected.%22);%20}%20%3C/script%3E>

The script was found online by searching