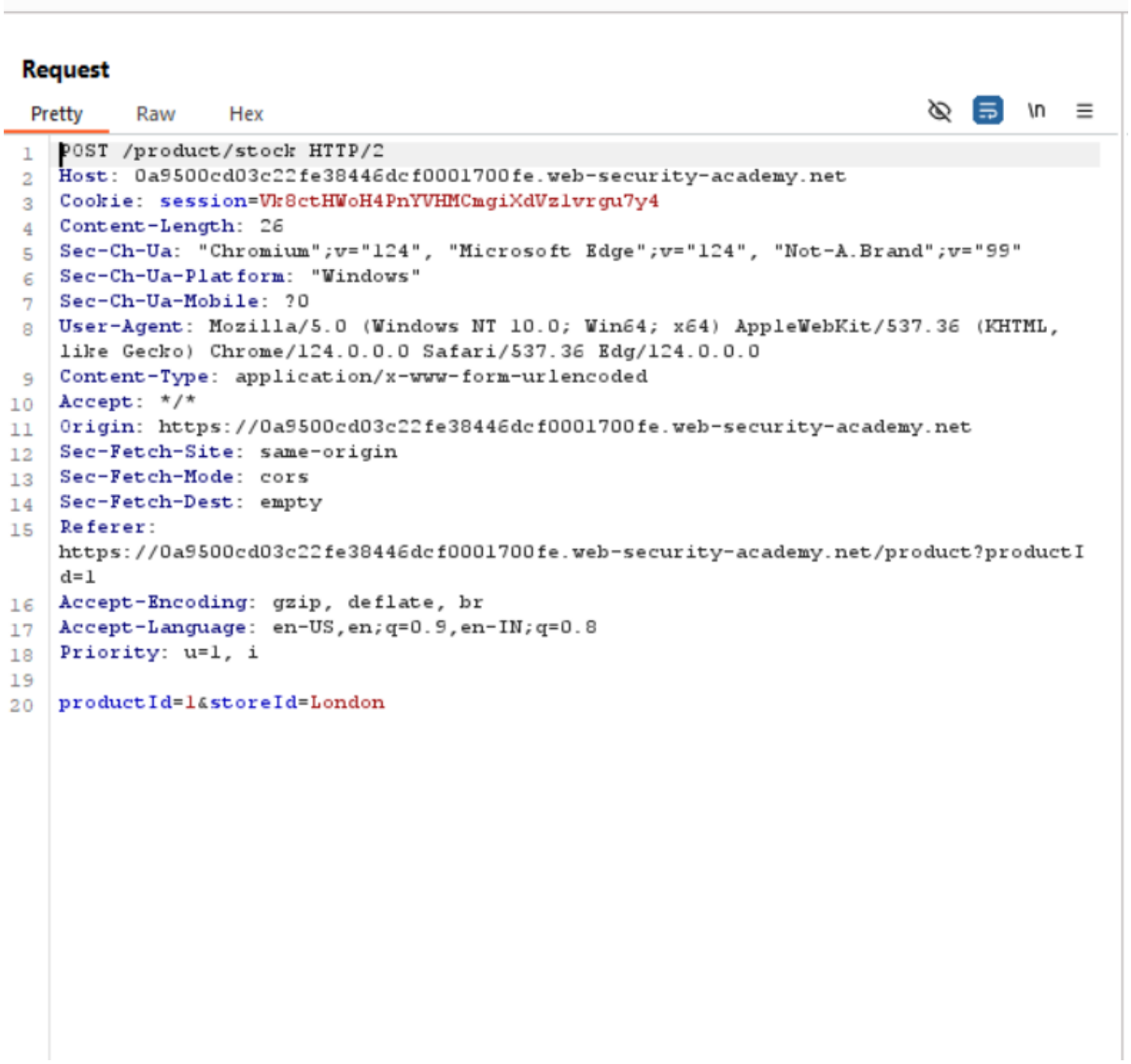
Lab: DOM XSS in document.write sink using source location.search inside a select element

S. Giridharan
CB.SC.P2CYS23006

This lab contains a DOM-based cross-site scripting vulnerability in the stock checker functionality. It uses the JavaScript document.write function, which writes data out to the page. The document.write function is called with data from location.search which you can control using the website URL. The data is enclosed within a select element.

To solve this lab, perform a cross-site scripting attack that breaks out of the select element and calls the alert function.

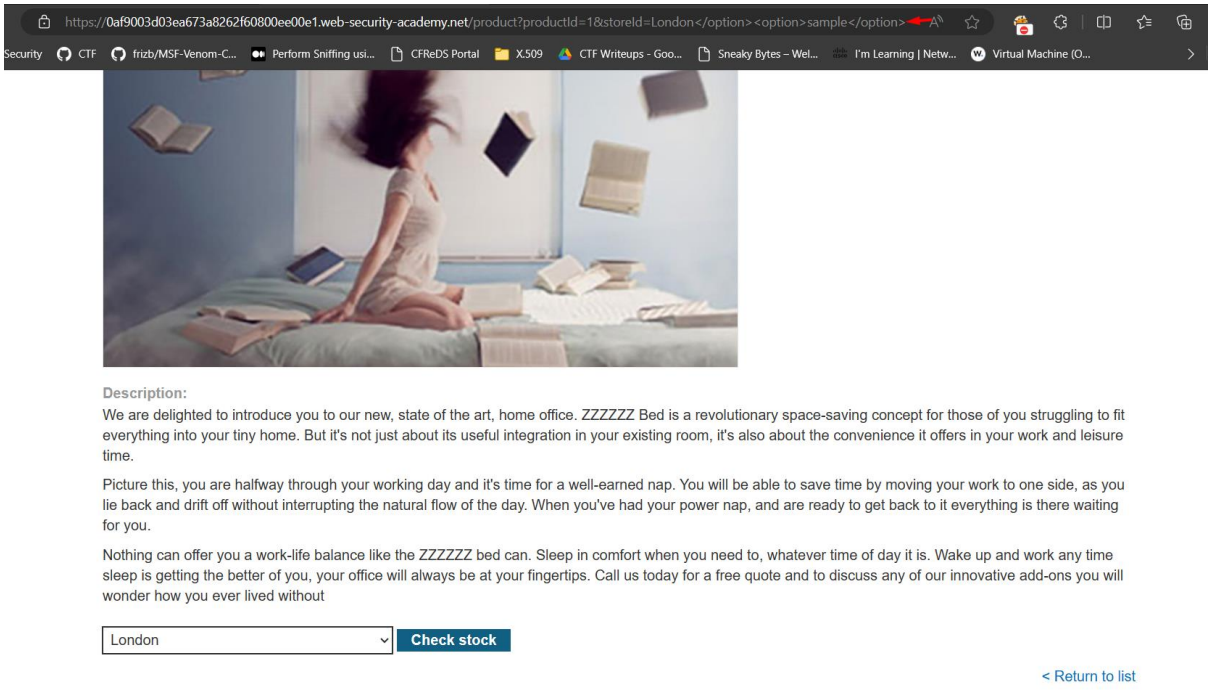
As stated in the lab description there is DOM based XSS Vulnerability in the Check Stock, Click the Check Stock and intercept the traffic in the Burpsuite.



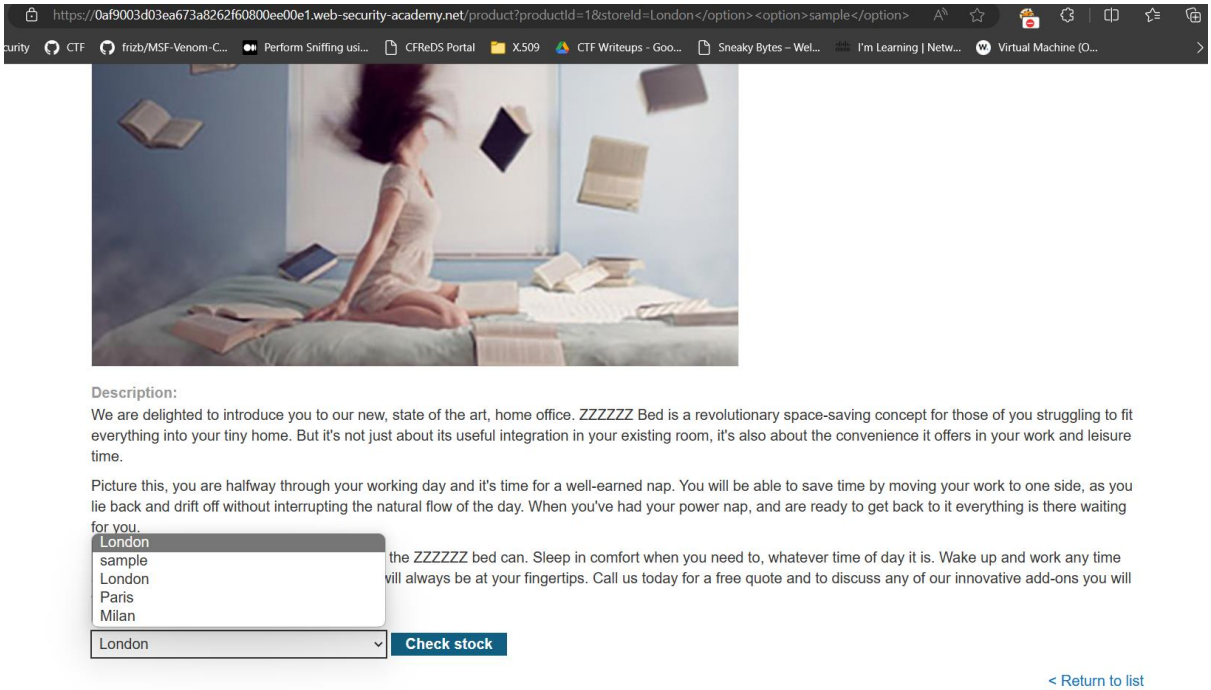
Enter a custom payload to check whether the payload is working fine.

Lab: DOM XSS in document.write sink using source location.search inside a select element

S. Giridharan
CB.SC.P2CYS23006

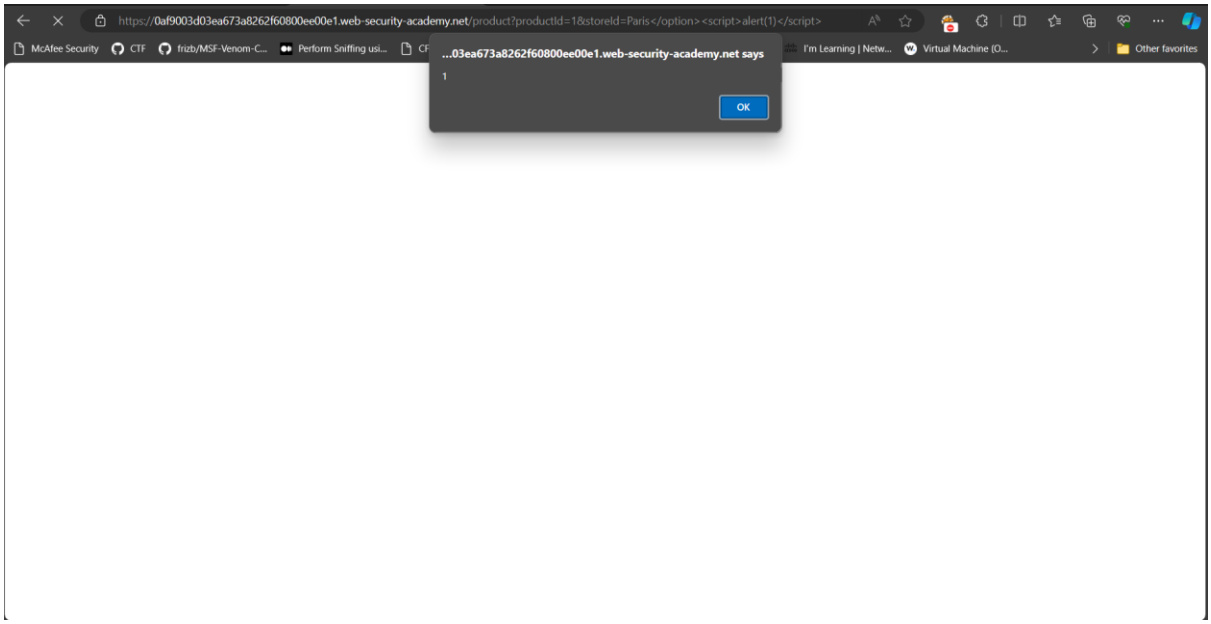
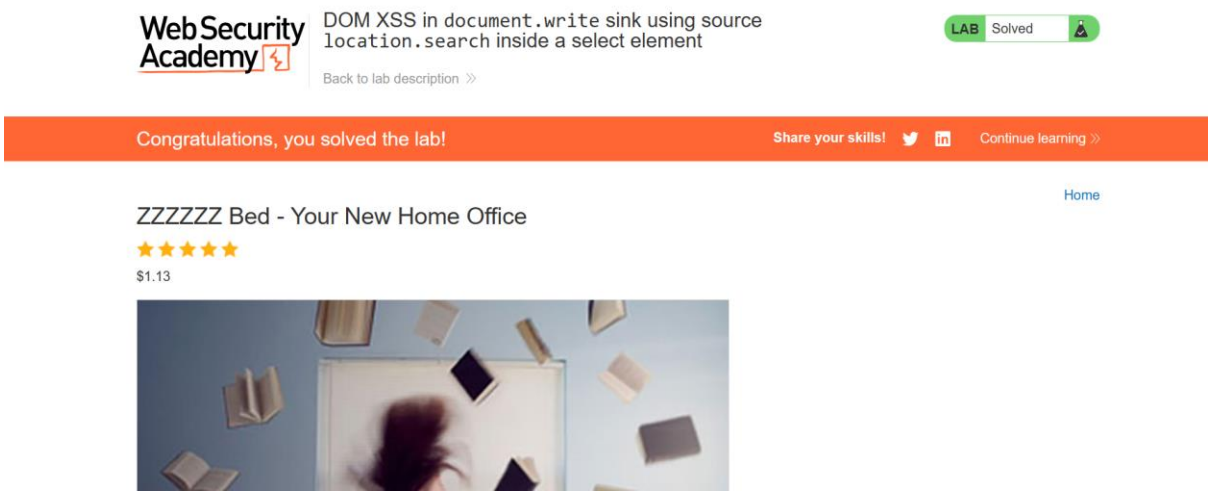


We can see that our sample is added as a option,



We can see that sample is added as a option we can use this to trigger an alert using the following script,

&storeId=Paris</option><script>alert(1)</script>

Lab: DOM XSS in document.write sink using source location.search inside a select element

S. Giridharan
CB.SC.P2CYS23006