目標:

在頁面上注入”alert()”

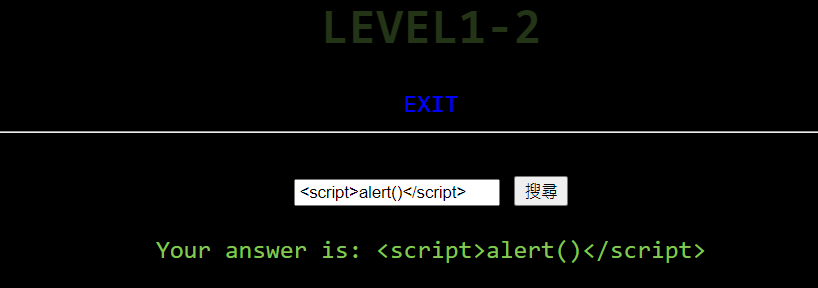
環境:

Windows

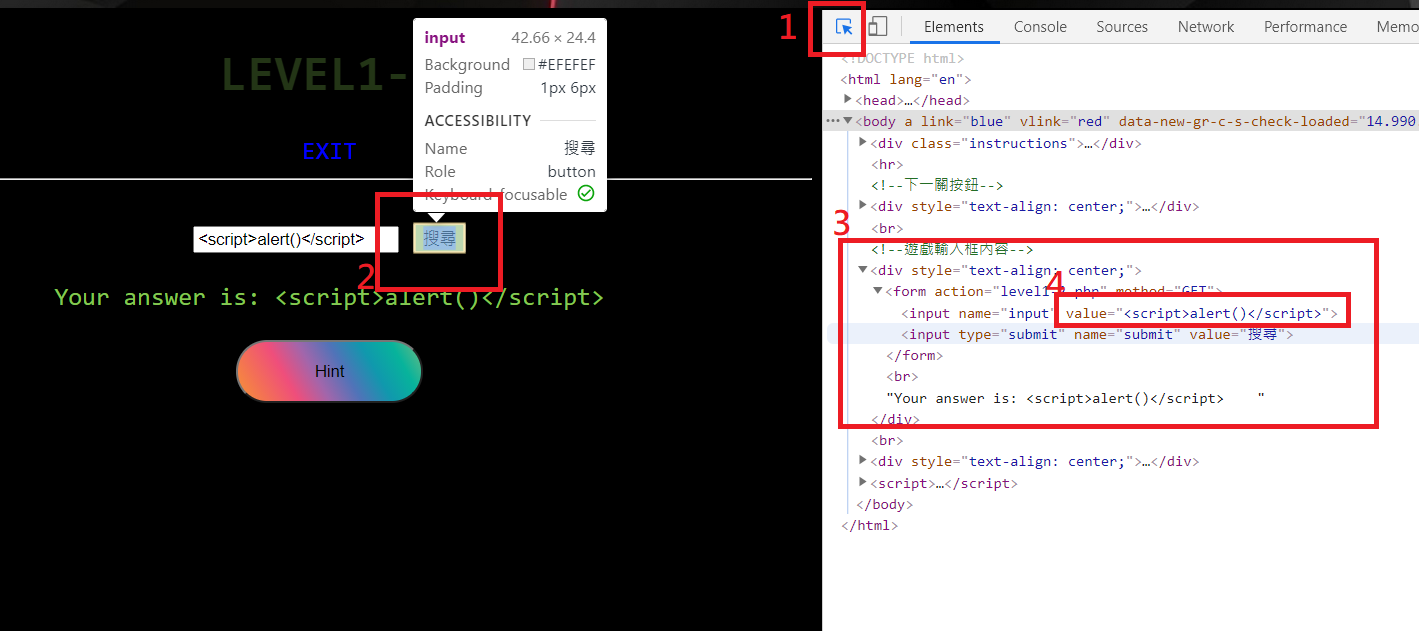
解題過程:



可以看到上面網址與第一關一樣有”name=test”，但輸入第一關的方式，會發現行不通。



在搜尋欄位內輸入也是一樣，此時可以按下F12，檢查原始碼。



按下F12查看網頁原始碼。

點選1,可以利用它快速找到想要查看的內容。

接著點選2按鈕或是搜尋欄。

接著3原始碼就會跳出。

再來4觀察”value”裡的直。

我們利用文字漏洞”><script>alert()</script>將Value的值強制為空，進而注入我們要的<script>