**SSCBS**

**MAYANK CHOPRA**

**ROLLNO -23719**

**CROSS SITE SCRIPTING -**

**XSS - it is a web security vulnerability that allows attacker to compromise the data present on the website**

**It allows attacker to carry out any action that user is able to perform and to access any user data**

**Impersonate as a user**

**Carry out any action**

**Read out any data that the user is able to access**

**Capture the user’s login credentials**

**Perform virtual defacement of the web site.**

**Inject Trojan functionality into web site.**

**Types of XSS attacks –**

**Reflected xxs- where the malicious script comes form the current HTTP request.**

**Stored xxs- where the malicious script comes from the website’s database.**

**Dom-based xxs- where the vulnerability exists in client-side code rather than server-side code.**

**LAB-REFLECTED XSS INTO HTML CONTENT WITH NOTHING ENCODED**

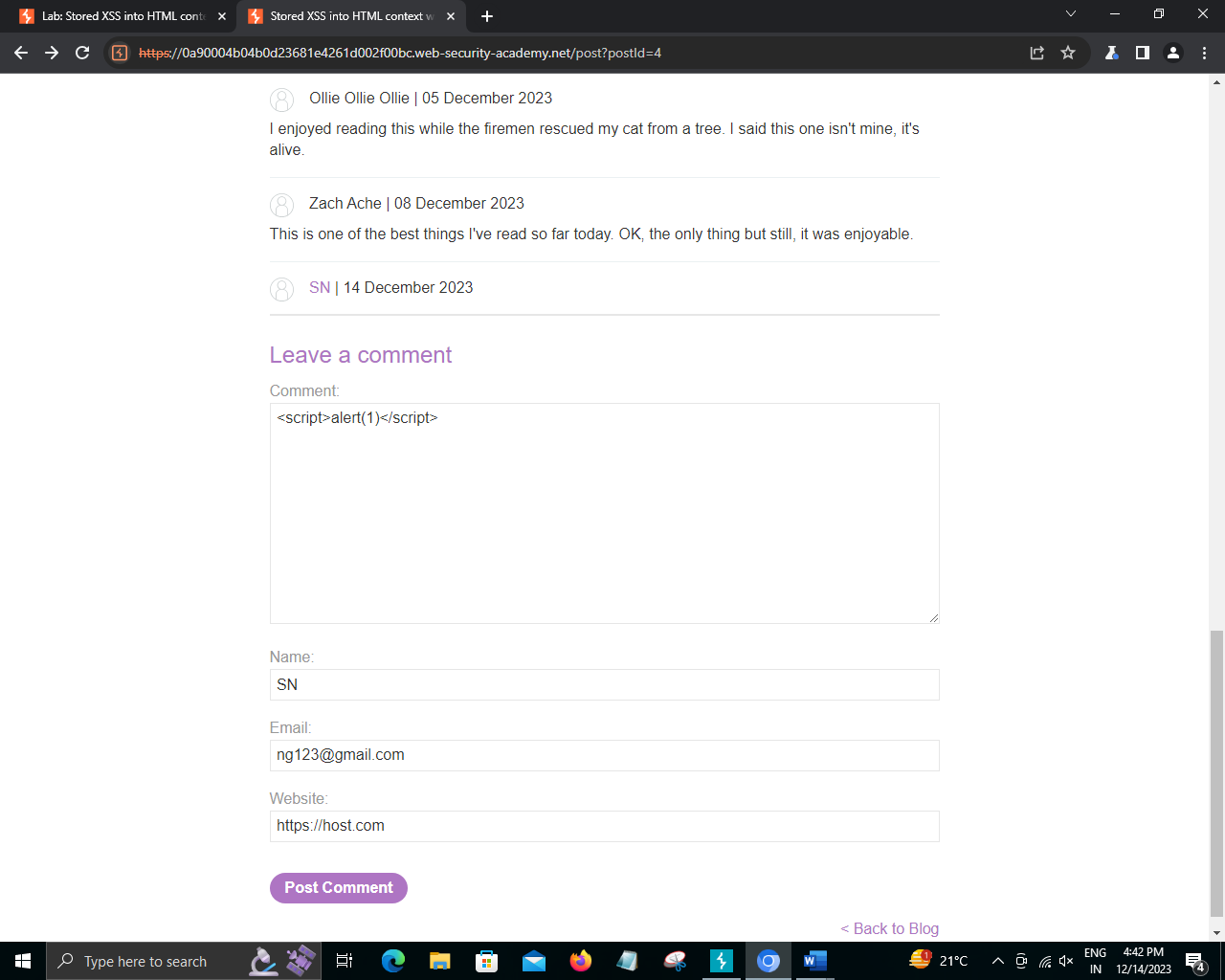
**Step1)-**open the lab->on the intercept->search<script>alert(1)</script> in the search bar->off the intercept->reload the website.

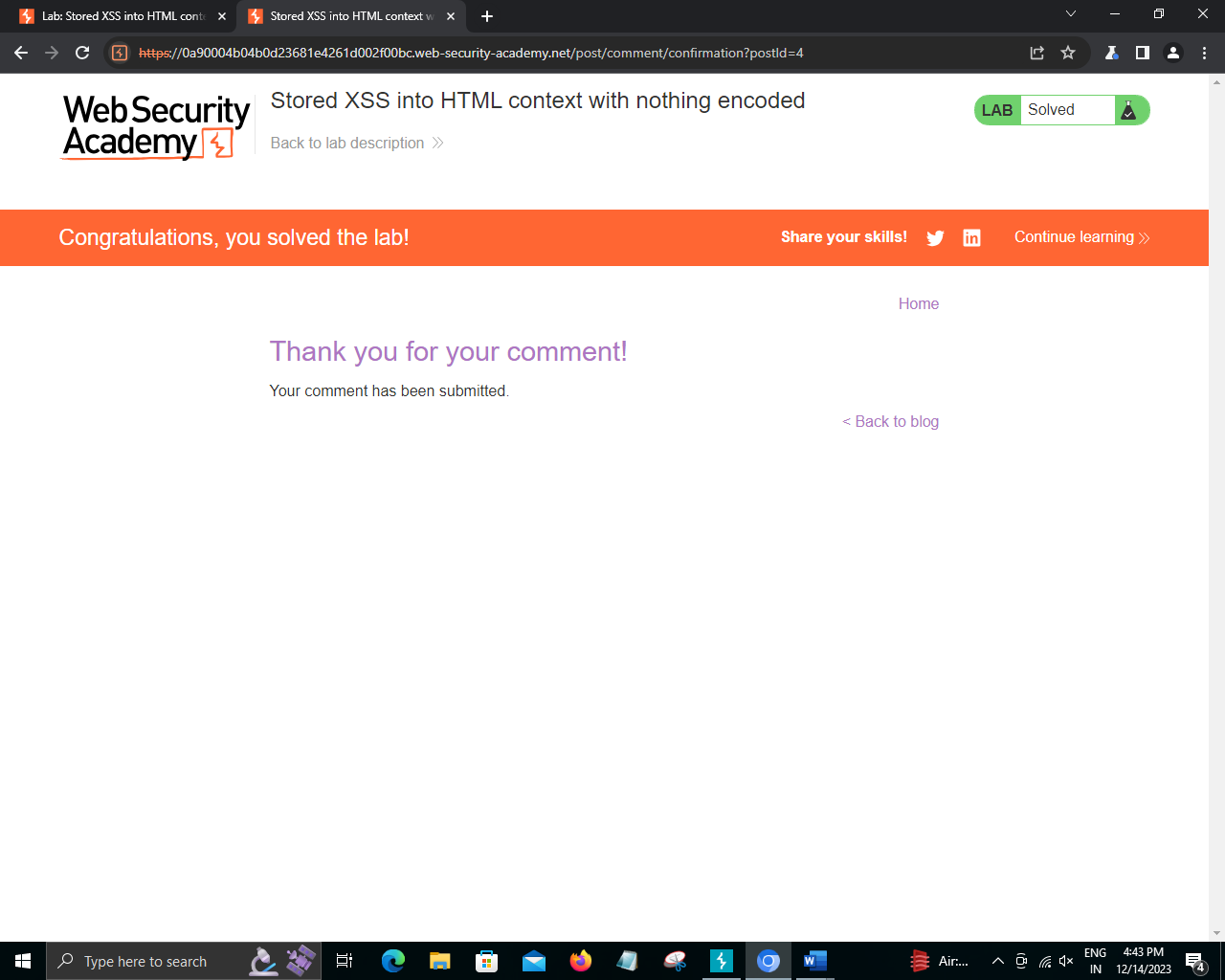


**LAB2-STORED XSS INTO HTML CONTENT WITH NOTHING ENCODED**

**POC-**

**Step1)-**open the lab->go to view post->type <script>alert(1)</script> in the comment section also provide name ,email,message and the post the comment->go back to blog->reload the website





**Lab:**[**DOM XSS**](https://portswigger.net/web-security/cross-site-scripting/dom-based)**in document.write sink using source location.search**

**POC-**

1. open the lab-> Enter a random alphanumeric string into the search box.
2. Right-click and inspect the element, and observe that your random string has been placed inside an img src attribute.
3. Break out of the img attribute by searching for:

"><svg onload=alert(1)>

