Internship Studio

Ethical

Hacking

**Training + Internship**

TASK1: -To solve any 5 XSS labs from [**https://portswigger.net/web-security/all-labs**](https://portswigger.net/web-security/all-labs)**.**

Lab1: - Reflected XSS into HTML context with nothing encoded

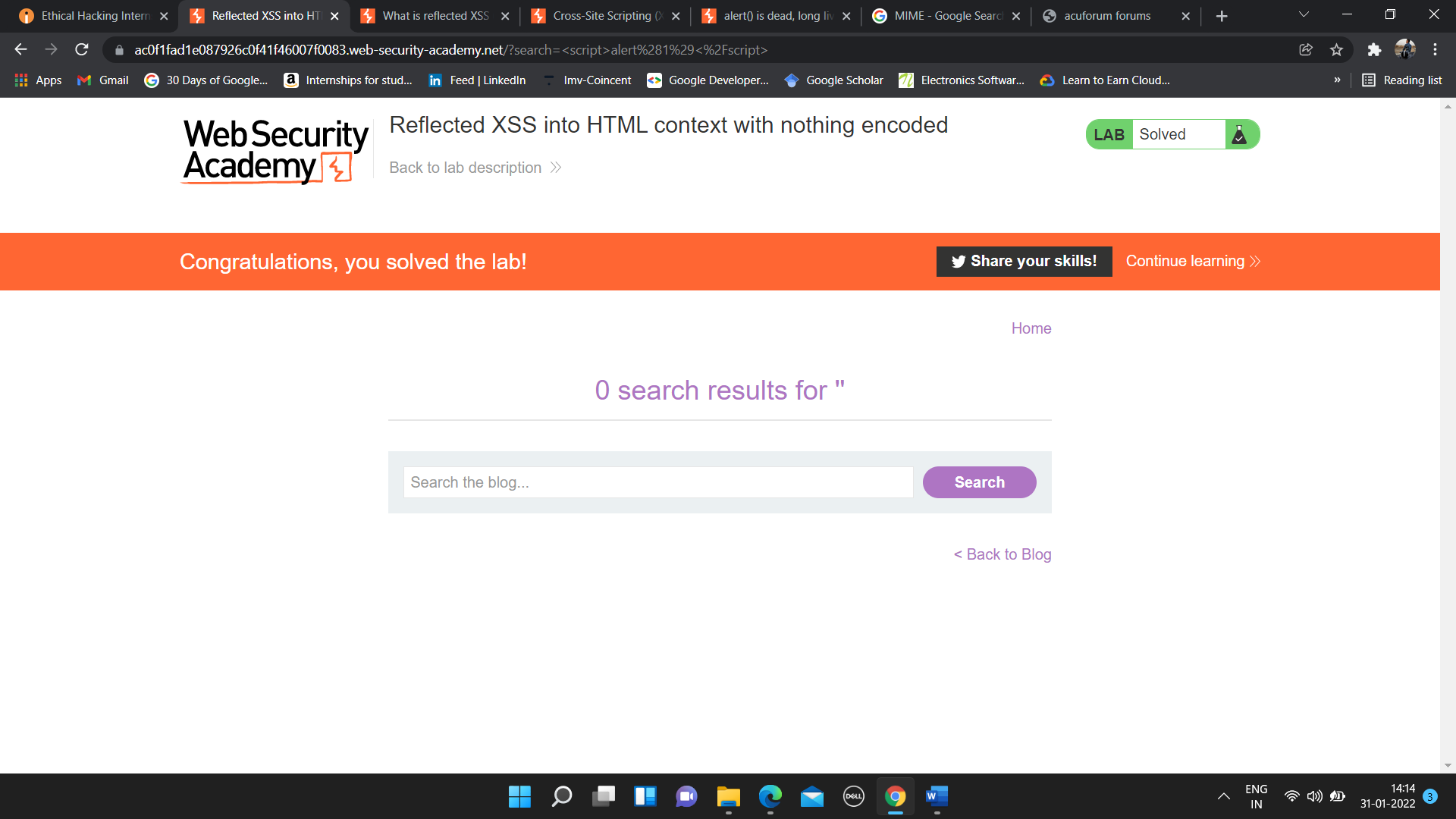
This lab contains a simple Reflected cross-site scripting Vulnerability. We can find this vulnerability in search functionality.

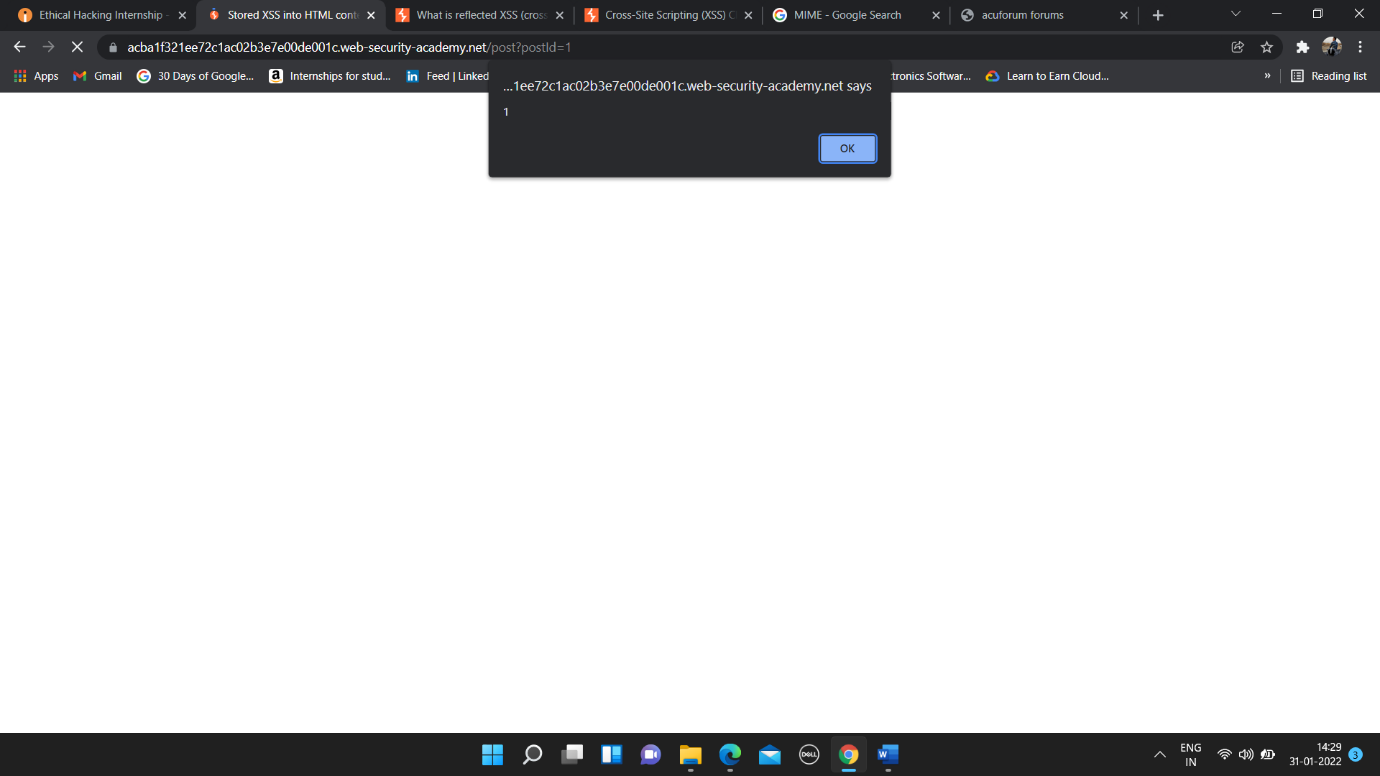
Procedure:

1. Click on access the lab tab
2. In search box type a cross-site script as <script>alert(1)</script>
3. Enter.

Cross-site script use in search box is:

<script>alert(1)</script>





**DEMO VIDEO**



Lab2: - Stored XSS into HTML context with nothing encoded

# This lab contains the stored cross-site scripting vulnerability. To find this vulnerability we need to write a cross-site script in comment with name, email-id and website name.

In comment box write below

Cross-site script is use: <script>alert(1)</script>

# Procedure:

# Click on tab access the lab.

# Go to any one of the posts and scroll down to end of the page.

# Here we want to enter the script in comment box as <script>alert(1)</script>

# Enter the name, email-id, and website name.

# Click on Post Comment.

# Go back to blog.

# 

# 

DEMO VIDEO

# 

# Lab3: - DOM XSS in document.write sink using source location.search

# This lab contains the DOM based cross-script scripting vulnerability in search of query tracking vulnerability. Here I use JavaScript document.write function, which write data out of page. Here in search box the cross-site script is written to find the vulnerability.

Write below cross-site script in search box

“><svg onload = alert(1)>

# Procedure: -

# Click on access the lab tab.

# In search box type cross-site script as

# “><svg onload=alert(1)>

# Click Enter.

# 

# 

# 

DEMO VIDEO

# Lab4: - DOM XSS in innerHTML sink using source location.search

# This lab contains the DOM based cross-site scripting vulnerability in the search box functionality. It uses an innerHTML assignment, which changes the HTML contents of a div element, using data from location.search.

Cross-site script use in search box is

<img src onerror=alert(1)>

# Procedure: -

# Click on tab access the lab

# In search box type <img src onerror=alert(1)> a cross-site script

# Enter.

# 

# 

# 

DEMO VIDEO

# 

# Lab5: - DOM XSS in jQuery anchor href attribute using location.search source

# This lab contains a [DOM-based cross-site scripting](https://portswigger.net/web-security/cross-site-scripting/dom-based) vulnerability in the submit feedback page. It uses the jQuery library's $ selector function to find an anchor element, and changes its href attribute using data from location.search.

# Procedure: -

# Click on access the lab tab.

# Click on Submit feedback icon.

# You will next page with URL as https://ac671fae1fec9f86c0634336007900ee.web-security-academy.net/feedback?returnPath=/

# Here cross-site scripting is done in url of the lab

# Click on URLs and after the returnPath= type javascript:alert(1). Final URL will be https://ac671fae1fec9f86c0634336007900ee.web-security-academy.net/feedback?returnPath=javascript:alert(1)

# Press Enter.

Cross-site script use in url is

javascript:alert(1)

# 

# 

DEMO VIDEO

