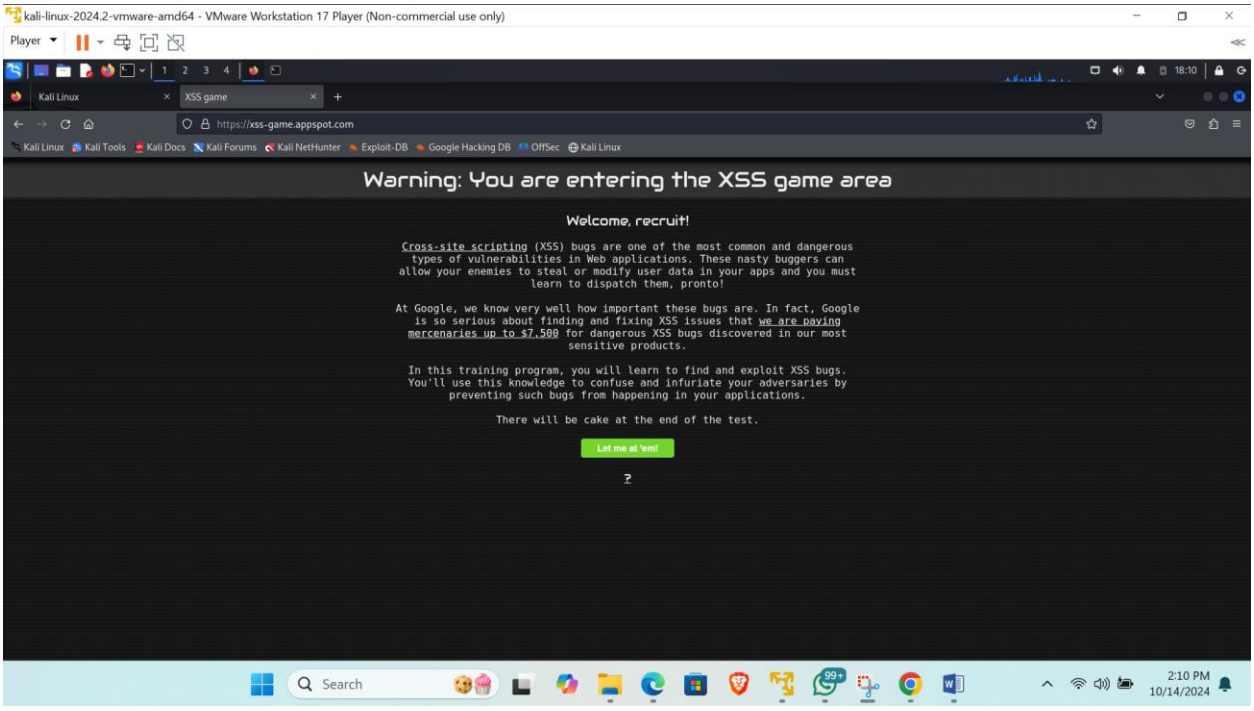
CROSS SITE SCRIPTING (XXS)

XSS (Cross-Site Scripting) is a type of security vulnerability typically found in web applications. It occurs when an attacker can inject malicious scripts (usually JavaScript) into web pages viewed by other users. These scripts can then run in the victim's browser, potentially leading to stolen session cookies, sensitive data, or other malicious actions.

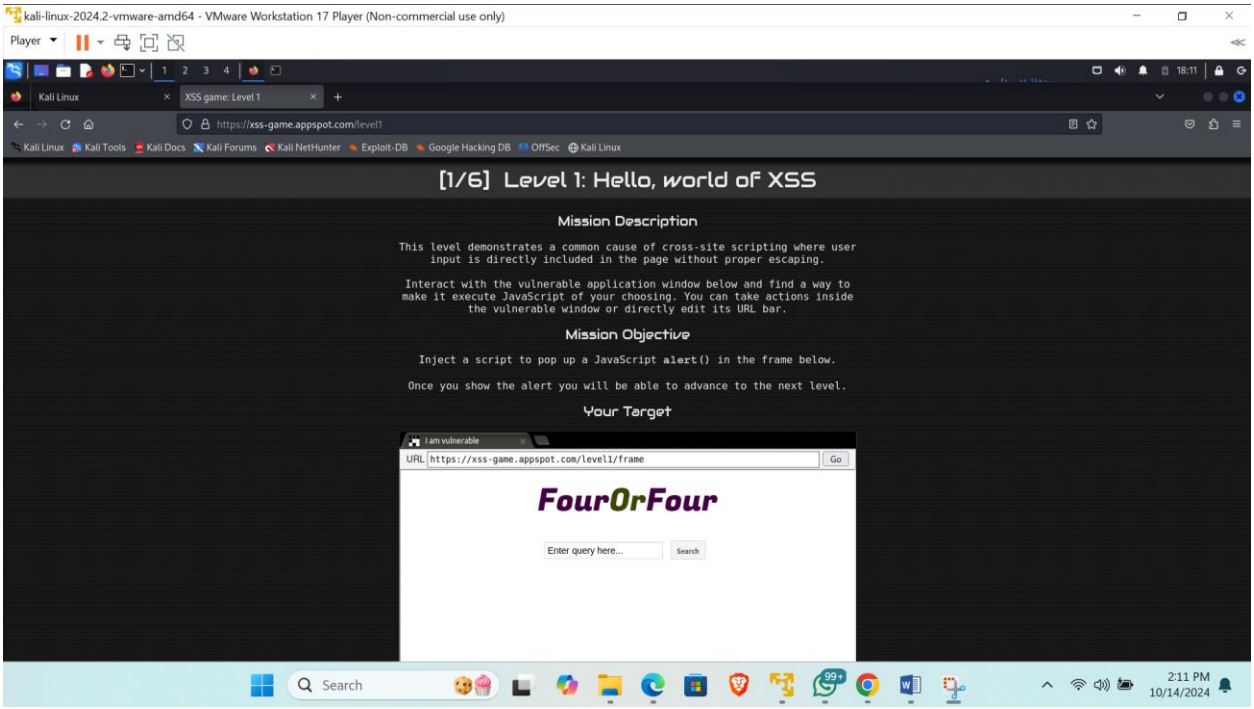
Tool: Web browser (FIREFOX)

Task 1

Start by typing this.. https://xss-game.appspot.com and when loaded click on **"let me at 'em!**



When you click on "let me at 'em!" an interface like this below will show

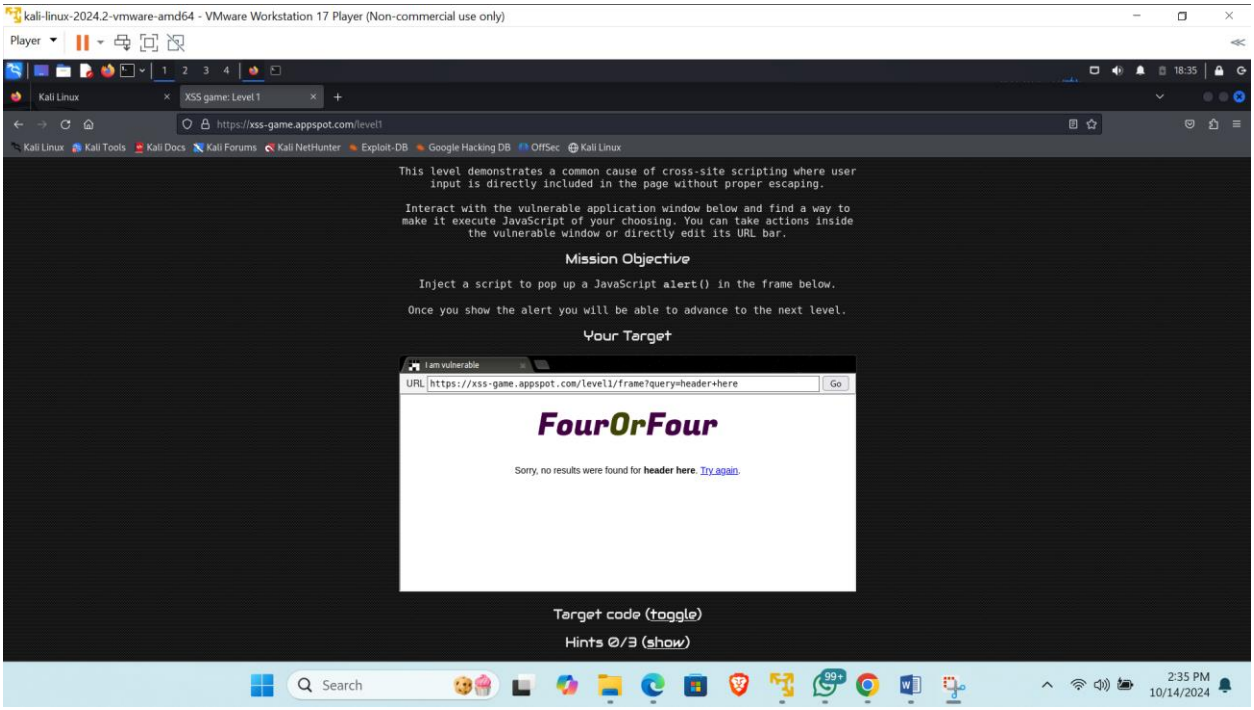


Task 2

In the search box for a web page presented for us, we will create a header……

To be able to execute JavaScript in a web application like this one, a basic understanding of the syntax for JavaScript and HTML is required.

FOR EXAMPLE: Enter this value **“Header here”** into the search box and see what result you get

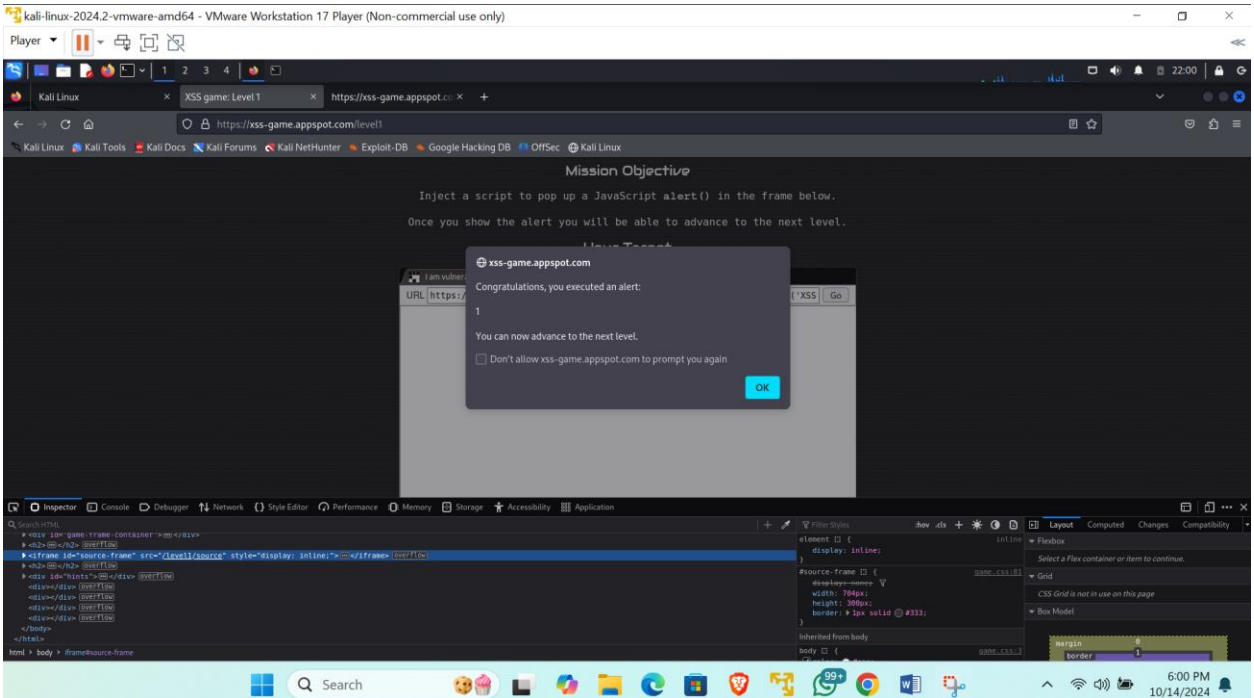


And the result was **“sorry no result were found for header here TRY AGAIN”**

Task 3

we executed the XXS attack successfully using command below:

<script>alert('XSS')</script>
<img src=x onerror=alert('XSS')>
"><script>alert(1)</script>



Task 4


I am vulnerable
URL
https://xss-game.appspot.com/level2/frame
Go
You
Mon Oct 14 2024 22:13:44 GMT-0400 (Eastern Daylight Time)
Welcome!
This is your personal stream. You can post anything you want here, especially madness.
You
Mon Oct 14 2024 22:15:33 GMT-0400 (Eastern Daylight Time)
FourOrFour