WAPH - Web Application Programming and Hacking

Instructor: Dr. Phu Phung

Student

Name : Sai Krishna Barupai

Email : barupasa@mail.uc.edu

Profile Pic :

Repository information for HACKATHON 1

Repository

Repository URL: https://github.com/barupasa/waph-barupasa/tree/main/labs/hackathon1.

Hackathon 1: Cross-Site Scripting Attacks and Defenses

Overview

*** In the first Hackathon, it is to gain knowledge about threats by Xss attacks. I got to know about vulnerabilities in the code ,which i have written back in lab2.In this hackathon i learned about attacks and wrote code to prevent scripting attacks. The hackathon is divided into two distinct tasks. Task 1 is about attacks on url and It has six challenging levels of vulnerabilities where I need to inject the code and also guess the code. In Task 2 ,writing secure code to prevent attacks .At last I have documented every step in detail with corresponding code snippet images.

Task 1 : ATTACKS

Level 0

URL : http://waph-hackathon.eastus.cloudapp.azure.com/xss/level0/echo.php

attacking script :

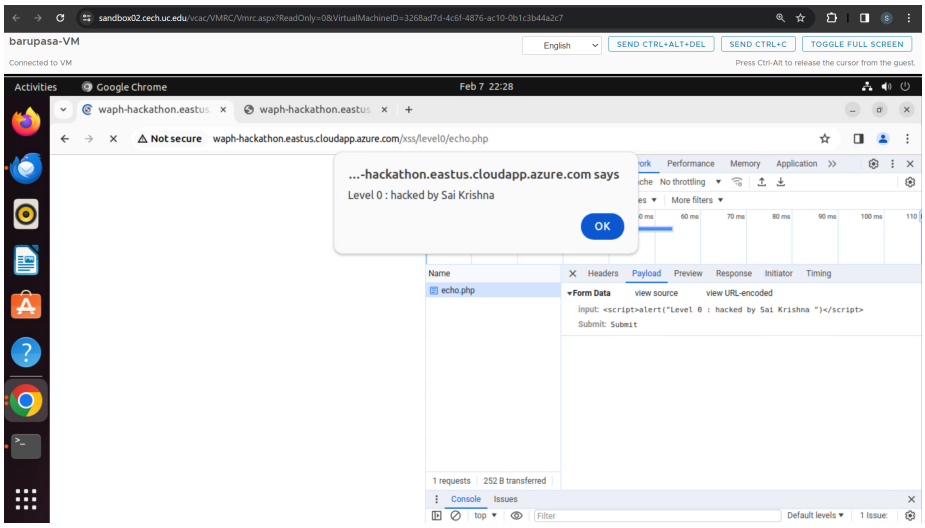


Figure 1: Level0

Level 1

In level 1 ,The assault script is injected like pathvariable and appended it to the end of URL. ?input=

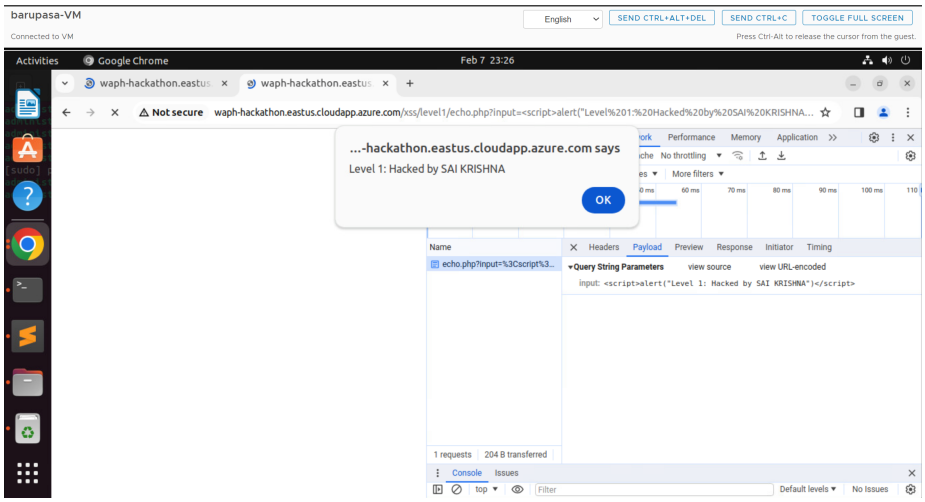


Figure 2: Level1

Level 2

The HTTP request doesnt have input feild and it is also not accepting the path variable , so i used HTML form element to link to the url .Then the script is sent through this form. Guess Code:

```
 if (isset($_POST['inputText’]))
    $input= $_POST['inputText'];
else
 echo "Error: 'input ' parameter is missing in the POST request.";
```

Level 3

In script tag is filtered in this level ,so i passed Script tag with combination of others. Guess code: `$output = preg_replace('/<script>|<\/script>/', '', $input);`

Level 4

The script tag is rejected completely,I utilized the onerror() segment of the tag to trigger an alert. Guess code:

```
 <?php
$inputText = "$_GET['input'];
$stringPattern = "/\bscript\b/i";
$resultString = preg_replace($stringPattern, '', $inputText);
echo $resultString;
?>
```

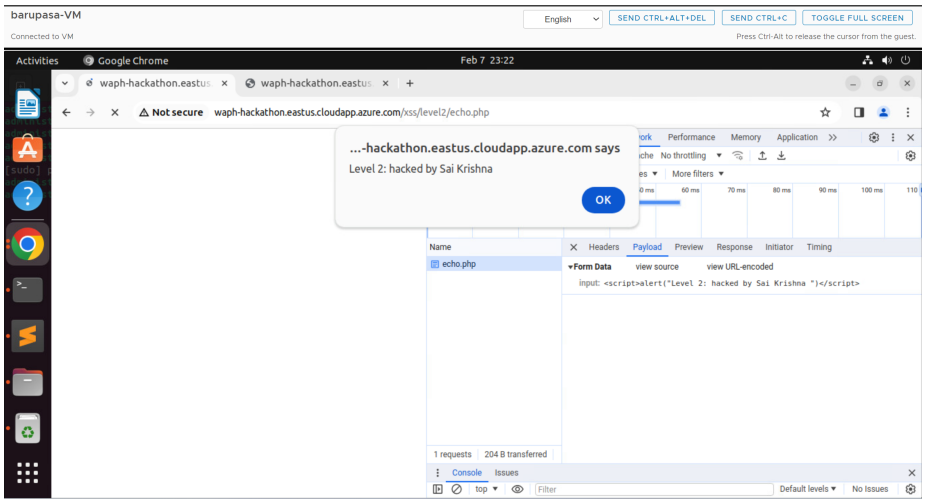


Figure 3: Level2

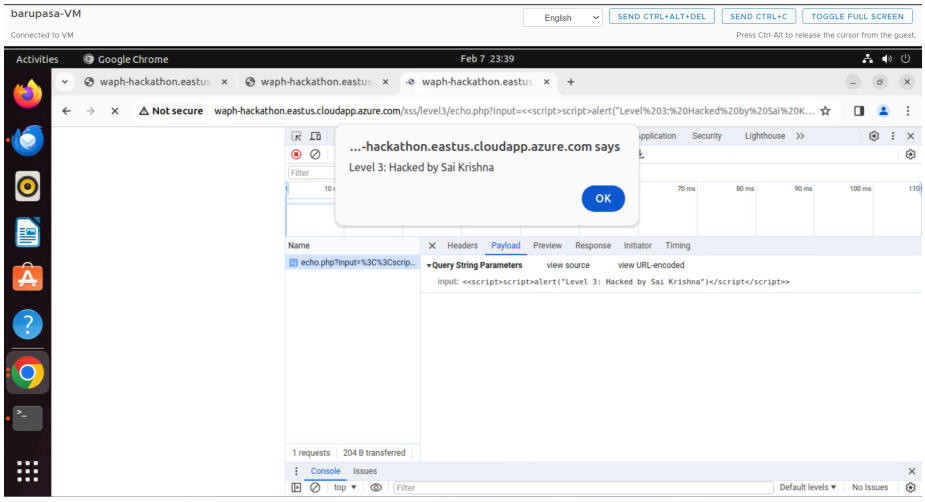


Figure 4: Level3

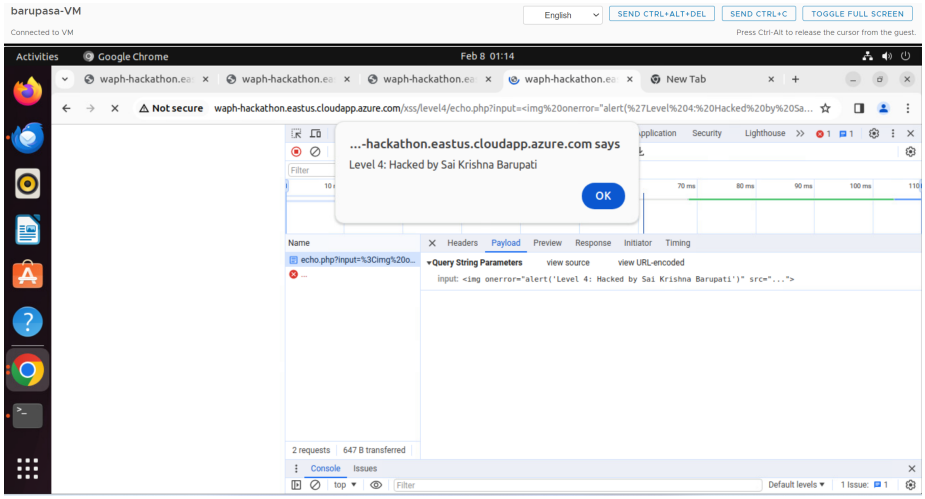


Figure 5: Level4

Level 5

In level 5, both the `<script>` tag and the `alert()` methods are not allowed. so to get popup alert, I employed a combination of unicode encoding and the `onerror()` function within the `<img>` tag. Guess code:

```
<?php
$data = $_REQUEST["inputText"];

if (str_contains($data, ["script", "alert"])) {
    echo "Both alerst and script tag not allowed";
} else {
    echo $data;
}
?>
```

Level 6

I tried for long time ,but i couldn't crack the logic here Guess code :

```
echo htmlentities($_REQUEST["data"])
```

Task 2 : DEFENCE

A Echo.php

I updated echo.php file from lab1. It now has code for checking input and defending against XSS. First it checks if input is empty ,if it is empty then thhis makes php files stop the execution .if not empty and input is valid ,htmlentities()

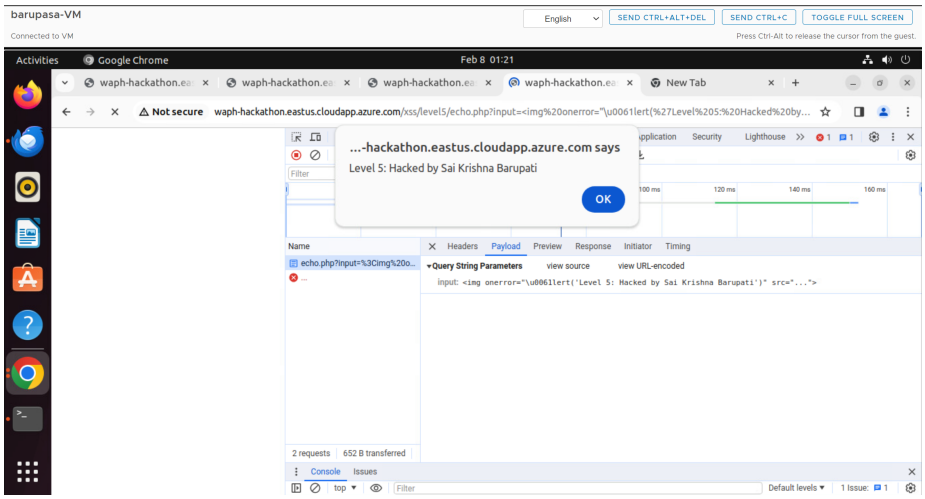


Figure 6: Level5

is called to sanitize the input. This method converts special characters to their HTML equivalents, ensuring that the text is displayed as plain text on the webpage.

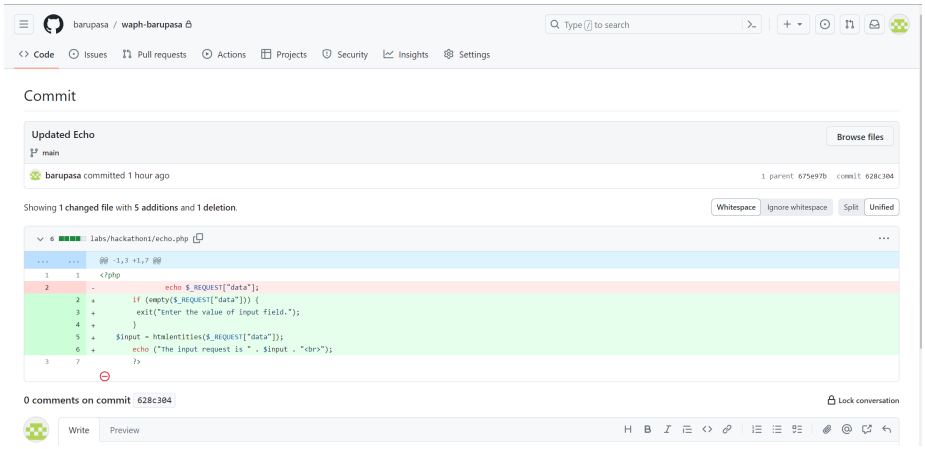


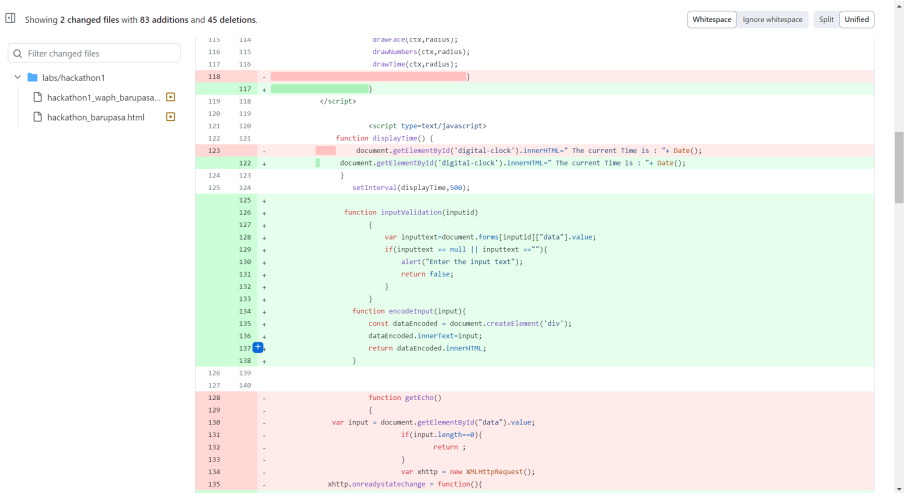
Figure 7: Task2A

B front-end prototype

The code in html file which is created in lab2 underwent a comprehensive review, leading to thorough revisions. External input points within the code were pinpointed and subjected to validation, ensuring their integrity. Moreover, output texts are sanitized to increase the security aspects.

1

The input data for both the HTTP GET and POST request forms now undergo validation. inputValidation() function is added and below is the code snippet of it.



2

inputValidation() method is written to valide the inputs from various elements ,an alert message is shown if the user enters empty string.I invoked this method in HTTPGET().HTTPPOST() and i have also added necessary null check and prompted alert message for these calls as well Ajax echo ,Jquery Get ,Jquery Post,Guess Age.

3

I have added necessary NULL checks and empty checks before appending the results to the response object.

4

A encodeInput(), befoe adding to html body ,the function encodeInput makes sure that the data is entered as plain text only. in this a div elememgt is created and content is added as innerText.it converts data as html ,ensuring its presentation as text and making it non-executable.

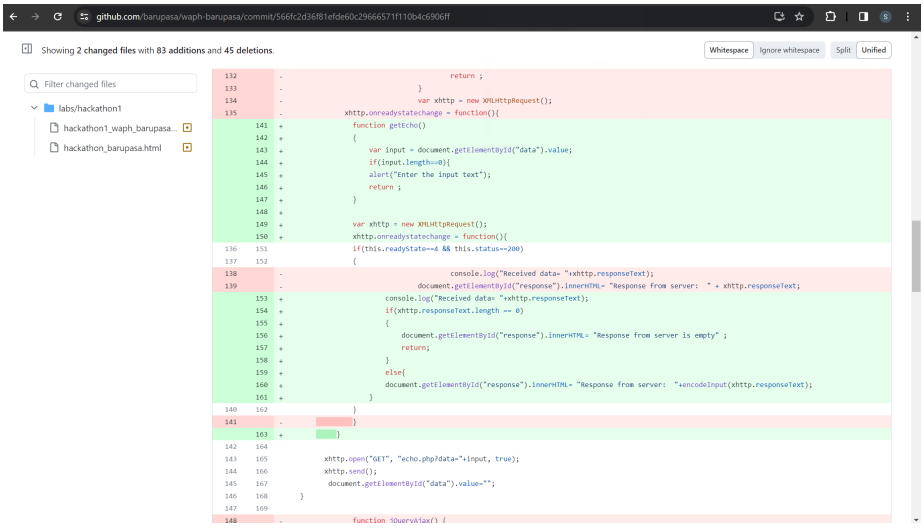


Figure 8: Task2B21

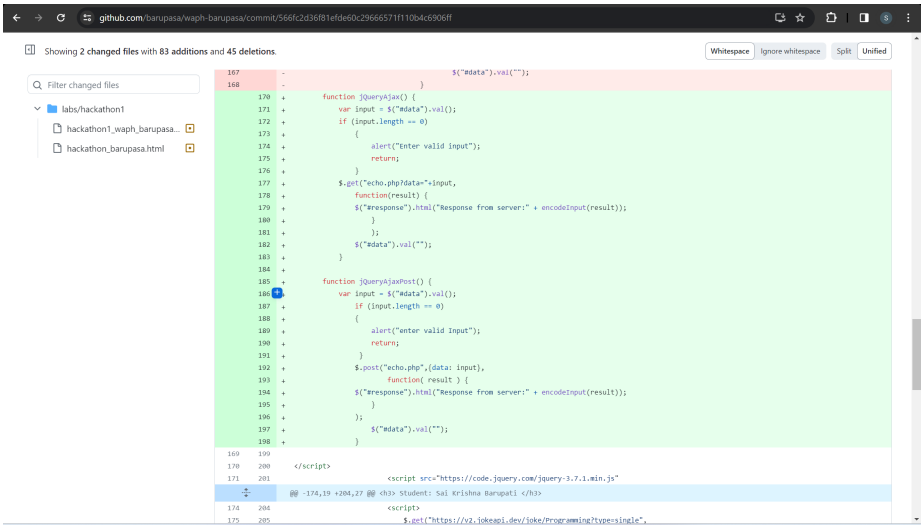


Figure 9: Task2B22

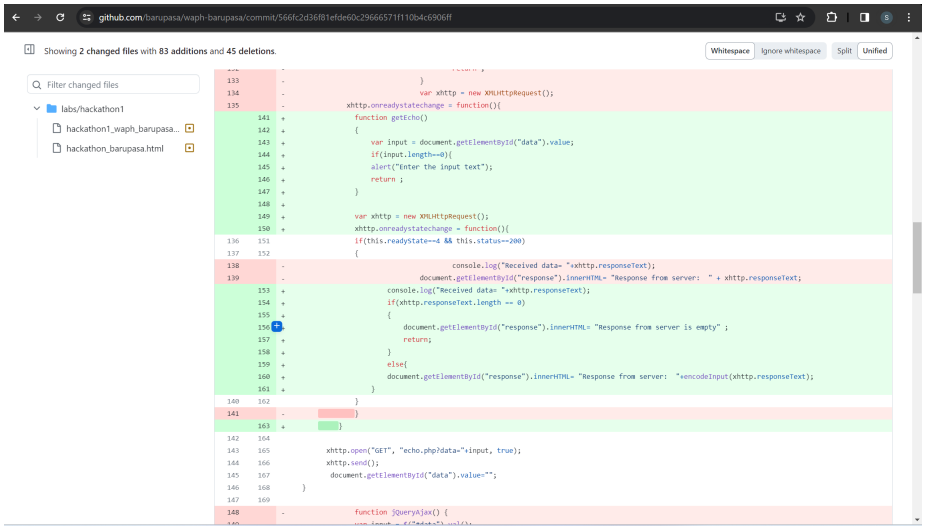


Figure 10: Task2B31

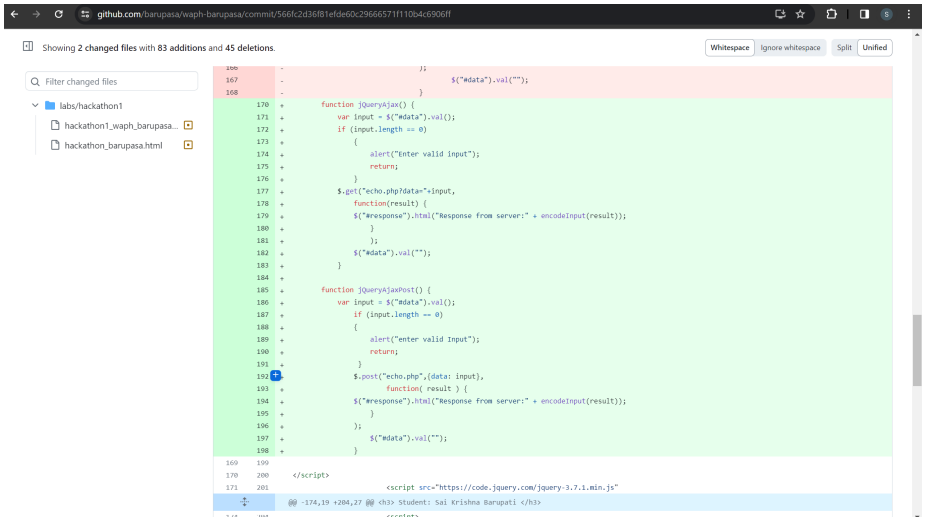


Figure 11: Task2B32

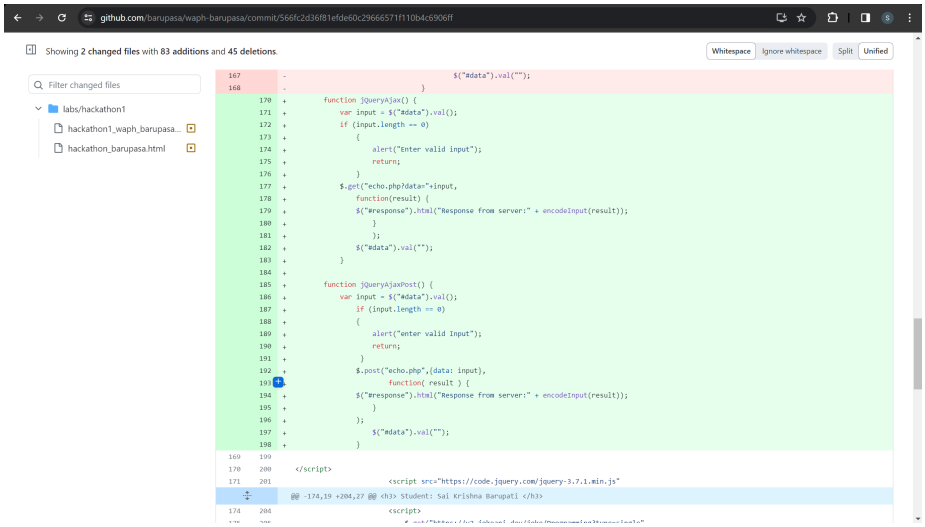


Figure 12: Task2B41

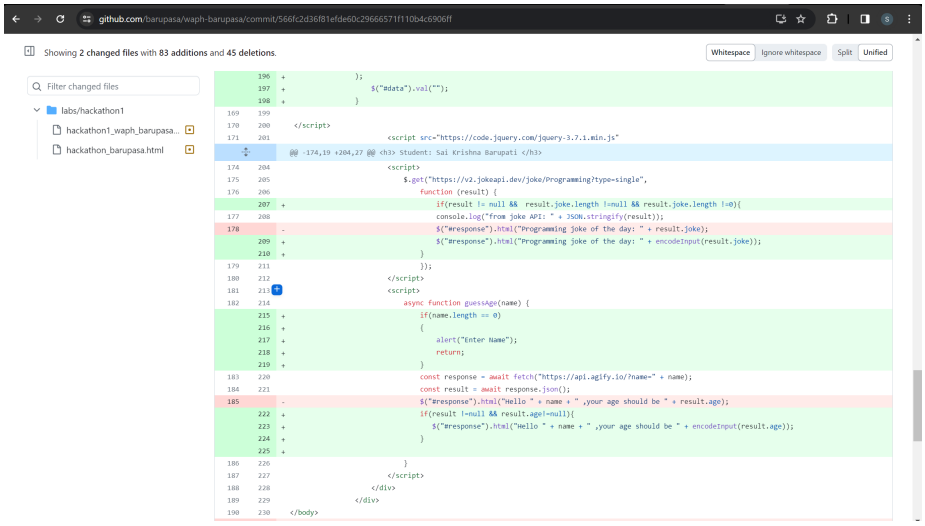


Figure 13: Task2B42