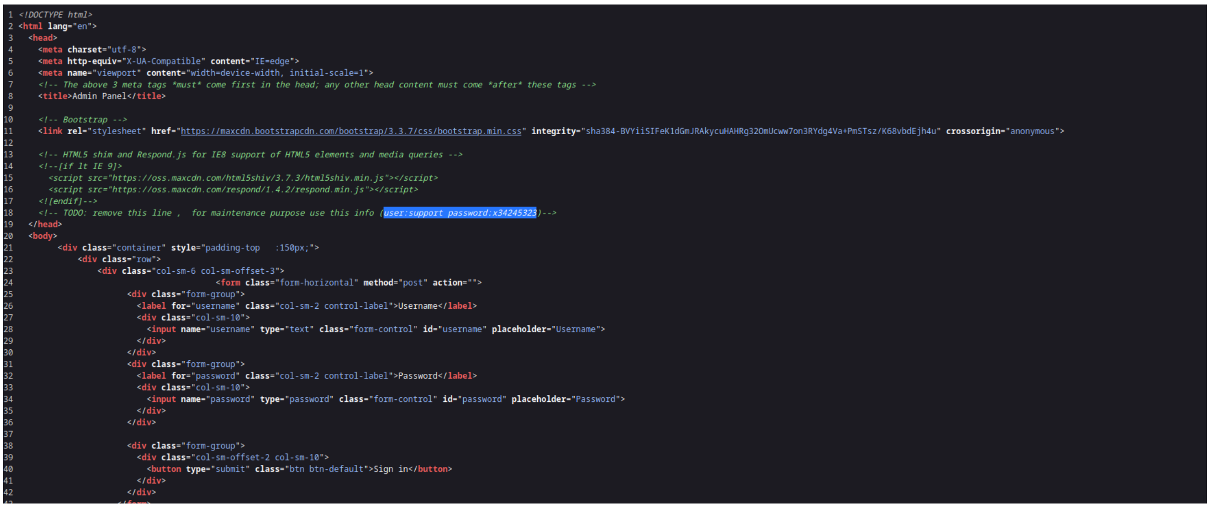
Cyber Talent - Web Security Solutions

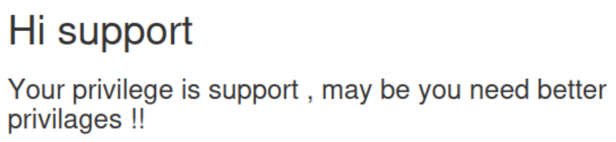
CHALLENGE 1 - AKA ADMIN HAS THE POWER



```
<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale=1">
    <!-- The above 3 meta tags *must* come first in the head; any other head content must come *after* these tags -->
    <title>Admin Panel</title>

    <!-- Bootstrap -->
    <link rel="stylesheet" href="https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/css/bootstrap.min.css" integrity="sha384-BVYiiSIFeK1dGmJRAkycuHAHRg32OmUcww7on3RYdg4Va+PmSTsz/K68vbdEjh4u" crossorigin="anonymous">

    <!-- HTML5 shim and Respond.js for IE8 support of HTML5 elements and media queries -->
    <!--[if lt IE 9]>
      <script src="https://oss.maxcdn.com/html5shiv/3.7.3/html5shiv.min.js"></script>
      <script src="https://oss.maxcdn.com/respond/1.4.2/respond.min.js"></script>
    <![endif]-->
    <!-- TODO: remove this line ,  for maintenance purpose use this info (user:support password:x34245323)-->
  </head>
  <body>
        <div class="container" style="padding-top   :150px;">
            <div class="row">
                <div class="col-sm-6 col-sm-offset-3">
                                        <form class="form-horizontal" method="post" action="">
                      <div class="form-group">
                        <label for="username" class="col-sm-2 control-label">Username</label>
                        <div class="col-sm-10">
                          <input name="username" type="text" class="form-control" id="username" placeholder="Username">
                        </div>
                      </div>
                      <div class="form-group">
                        <label for="password" class="col-sm-2 control-label">Password</label>
                        <div class="col-sm-10">
                          <input name="password" type="password" class="form-control" id="password" placeholder="Password">
                        </div>
                      </div>

                      <div class="form-group">
                        <div class="col-sm-offset-2 col-sm-10">
                          <button type="submit" class="btn btn-default">Sign in</button>
                        </div>
                      </div>
                    </form>
```

The HTML code for the Login Page of the Admin Has Power challenge

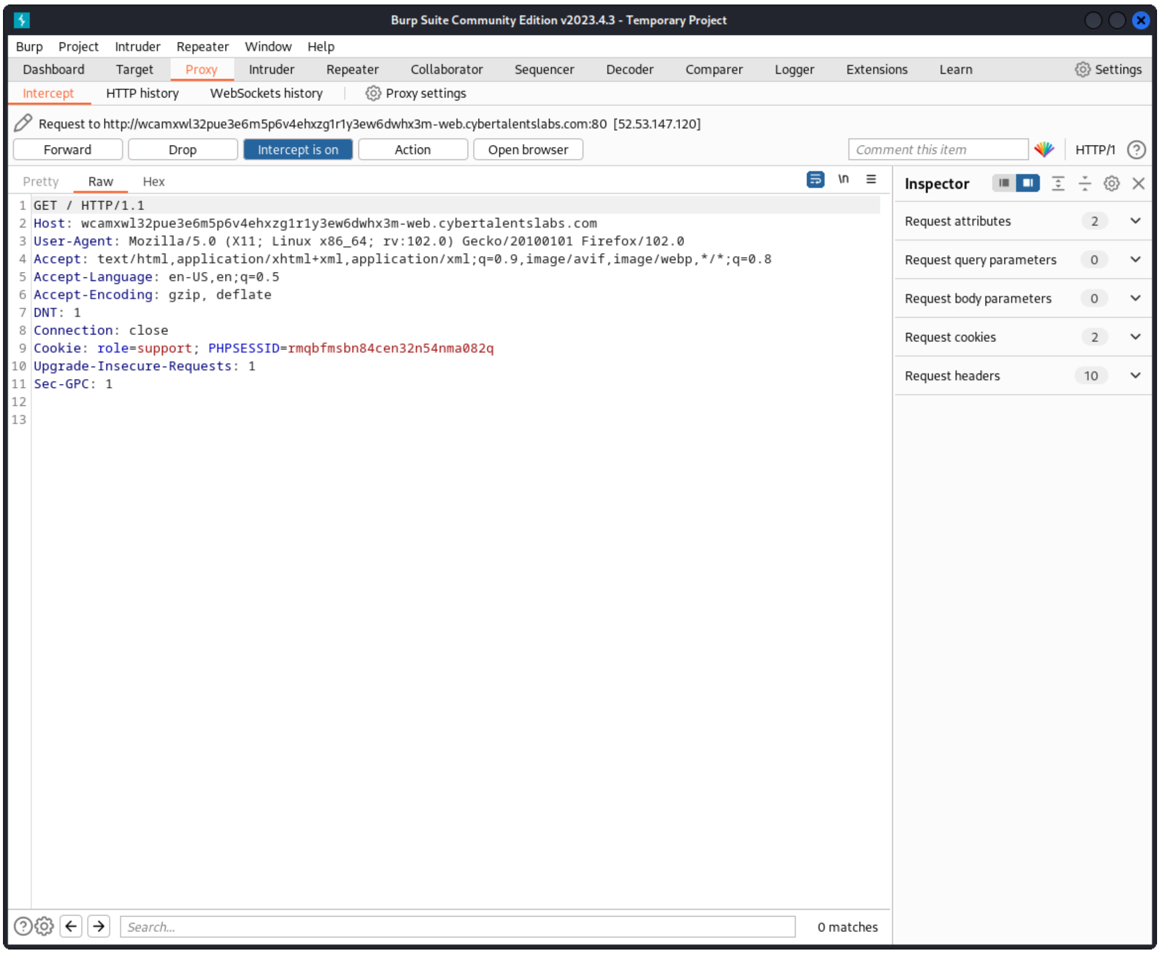
The code seems to have the username ‘support’ and the password as shown above.



Hi support

Your privilege is support , may be you need better privilages !!

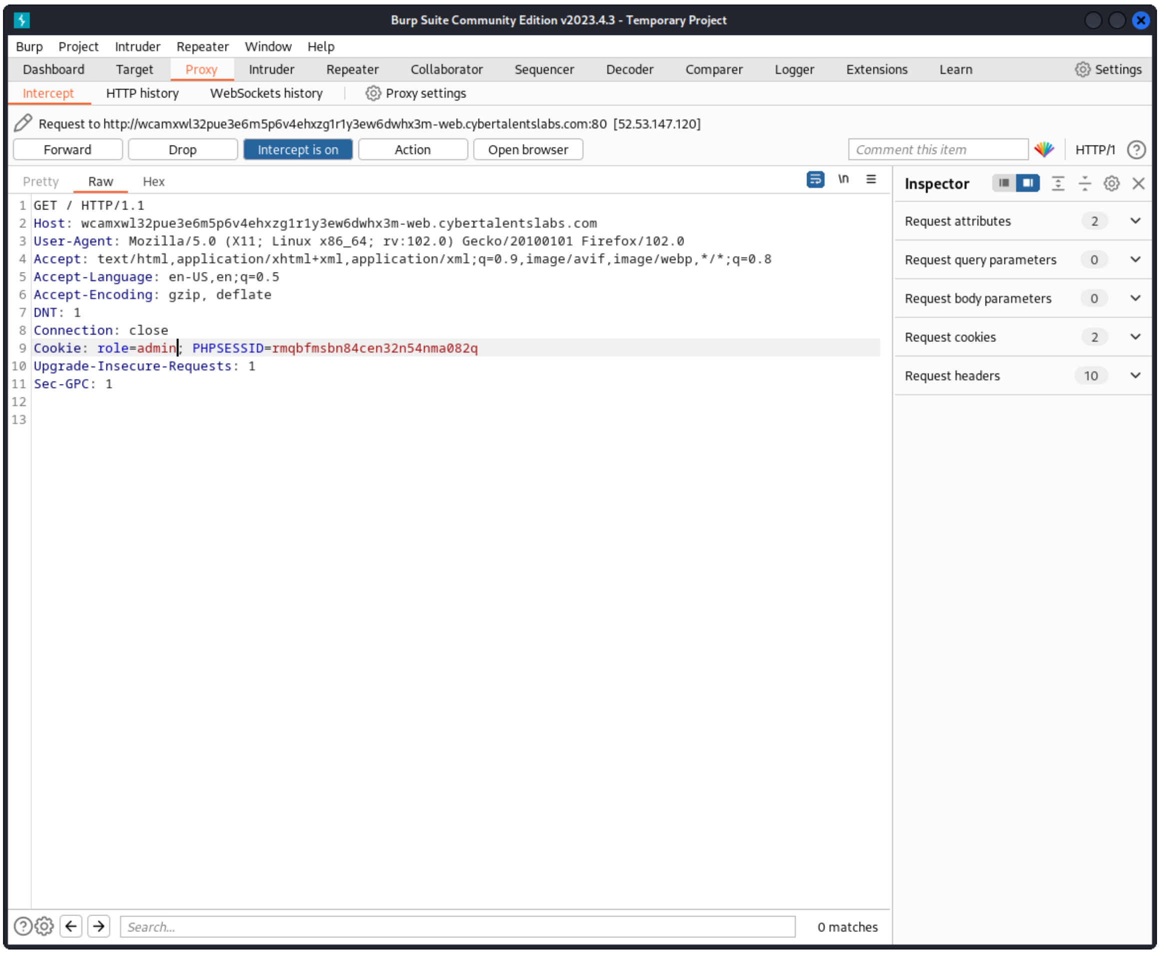
- Open burpsuite to see the Request and Response



Request to http://wcamxwl32pue3e6m5p6v4ehxzg1r1y3ew6dwhx3m-web.cybertalentslabs.com:80 [52.53.147.120]

```
GET / HTTP/1.1
Host: wcamxwl32pue3e6m5p6v4ehxzg1r1y3ew6dwhx3m-web.cybertalentslabs.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
DNT: 1
Connection: close
Cookie: role=support; PHPSESSID=rmqbfmsbn84cen32n54nma082q
Upgrade-Insecure-Requests: 1
Sec-GPC: 1


```

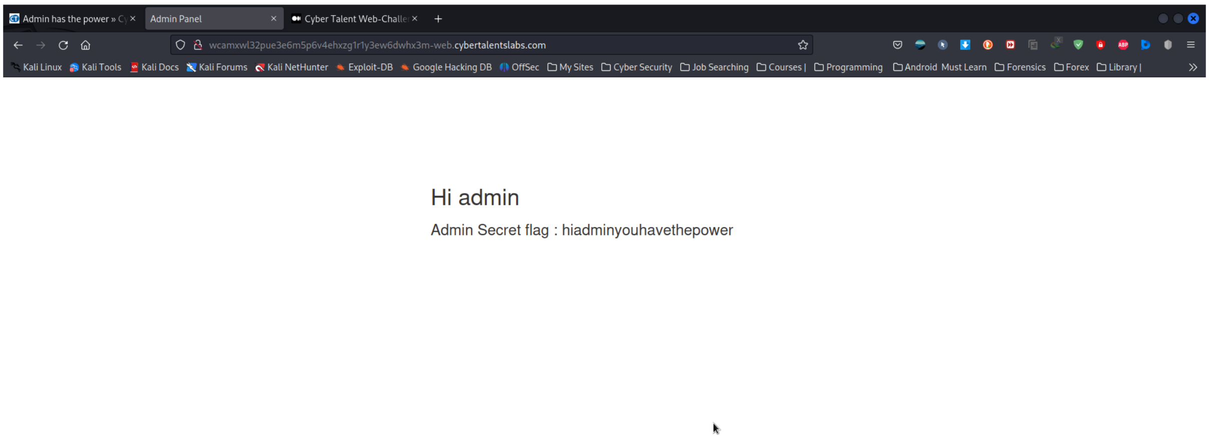
- Here in burpsuite you can change the Cookie role assigned and try it as admin to see what it can do.


Burp Suite Community Edition v2023.4.3 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Extensions Learn Settings
Intercept HTTP history WebSockets history Proxy settings
Forward Drop Intercept is on Action Open browser
Comment this item
HTTP/1
Pretty Raw Hex
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 0
Request cookies 2
Request headers 10
Search...
0 matches

Request to http://wcamxwl32pue3e6m5p6v4ehxzg1r1y3ew6dwhx3m-web.cybertalentslabs.com:80 [52.53.147.120]

```
GET / HTTP/1.1
Host: wcamxwl32pue3e6m5p6v4ehxzg1r1y3ew6dwhx3m-web.cybertalentslabs.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
DNT: 1
Connection: close
Cookie: role=admin; PHPSESSID=rmqbfmsbn84cen32n54nma082q
Upgrade-Insecure-Requests: 1
Sec-GPC: 1
```

- Forward the intercepted HTTP request and check on your browser.


Admin has the power » C
Admin Panel
Cyber Talent Web-Challe
wcamxwl32pue3e6m5p6v4ehxzg1r1y3ew6dwhx3m-web.cybertalentslabs.com
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec My Sites Cyber Security Job Searching Courses | Programming Android Must Learn Forensics Forex Library |

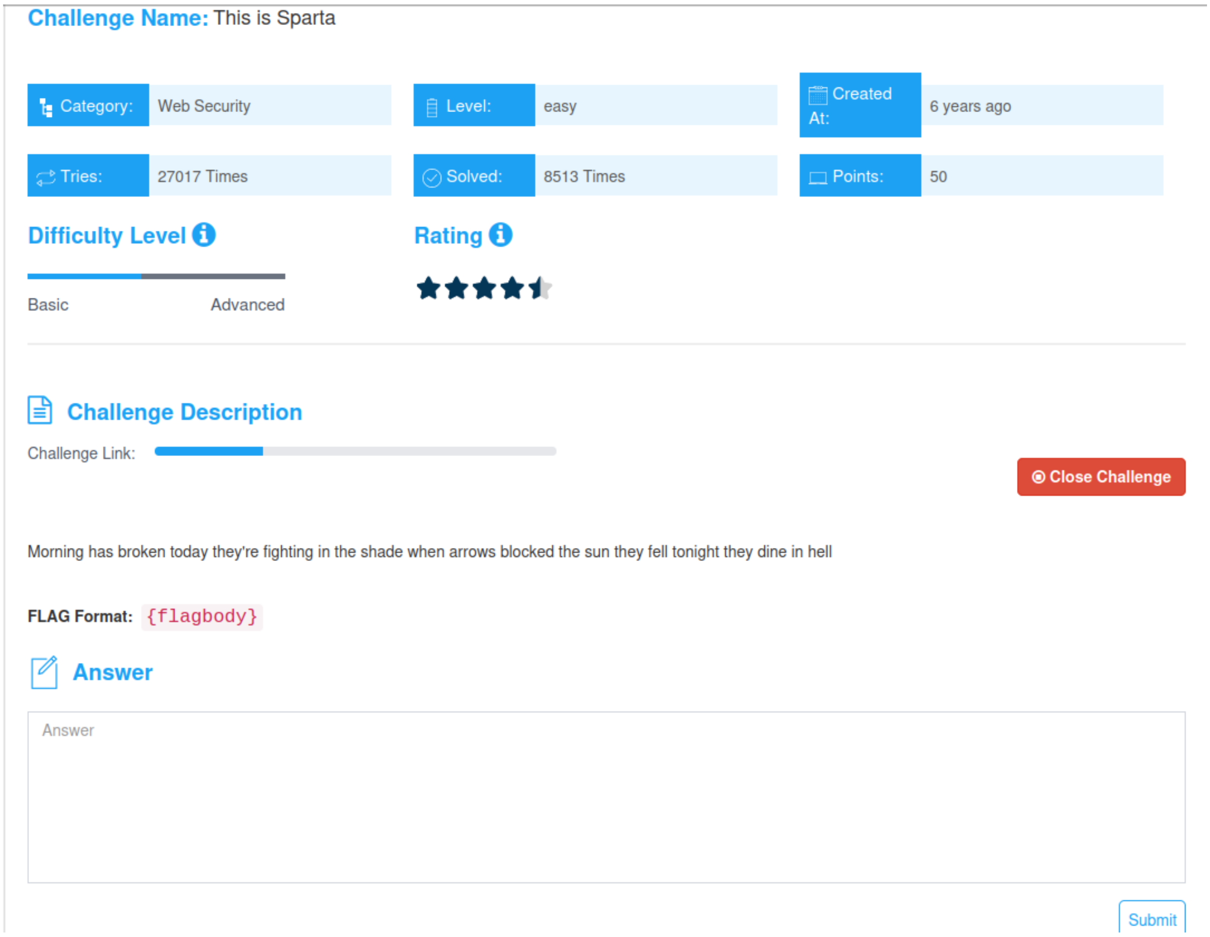
Hi admin

Admin Secret flag : hiadminyouhavethepower

💡 Well Done there is your flag. Thing learnt is :

```
1. Always check the html code of the given site you might see something intruiging.
2. Check the response and request of the web page you're tring to pentest
3. Always try something out.
```

CHALLENGE 2 - AKA THIS IS SPARTA



Challenge Name: This is Sparta

Category:	Web Security	Level:	easy	Created At:	6 years ago
Tries:	27017 Times	Solved:	8513 Times	Points:	50

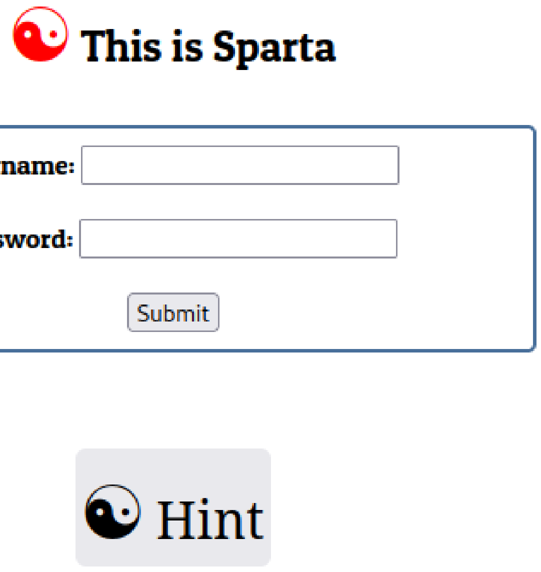
Challenge Description

Challenge Link:

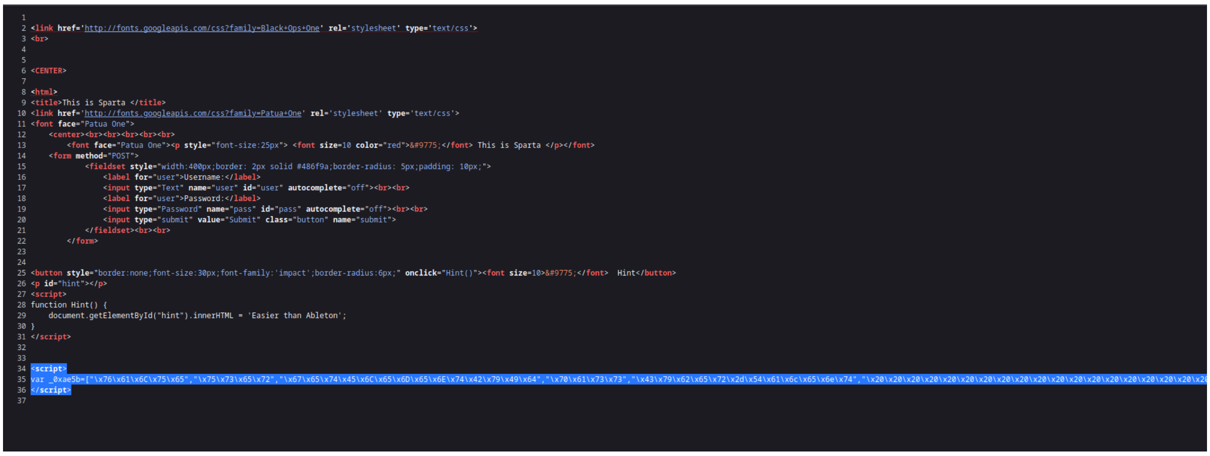
Morning has broken today they're fighting in the shade when arrows blocked the sun they fell tonight they dine in hell

FLAG Format: `{flagbody}`

Answer

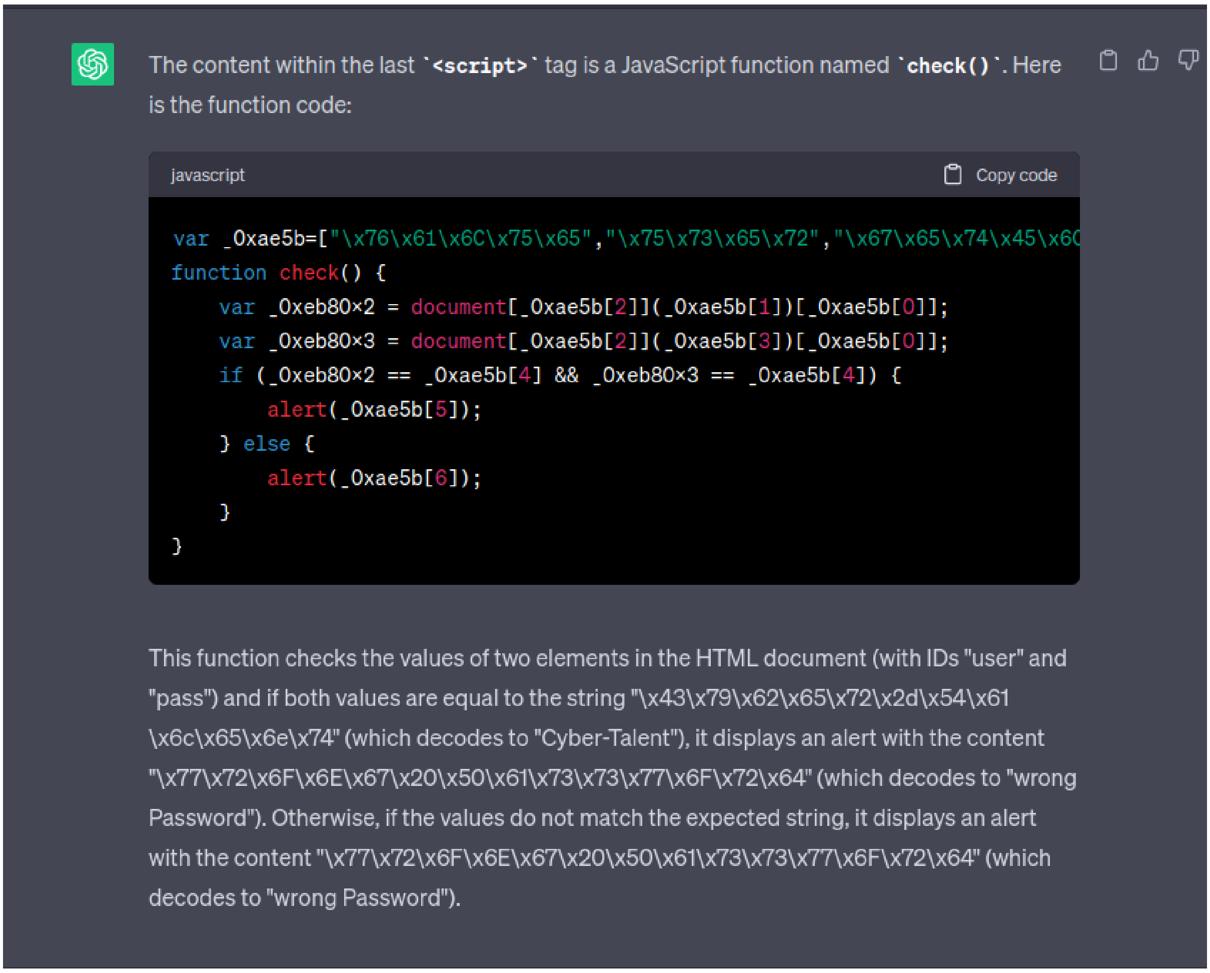


```
First we start by the things we previously learnt
  1. Check html code in the viewpage source info <Firefox>
```



```

<link href='http://fonts.googleapis.com/css?family=Black+Ops+One' rel='stylesheet' type='text/css'>
<br>


<CENTER>

<html>
<title>This is Sparta </title>
<link href='http://fonts.googleapis.com/css?family=Patua+One' rel='stylesheet' type='text/css'>
<font face="Patua One">
    <center><br><br><br><br><br>
        <font face="Patua One"><p style="font-size:25px"> <font size=10 color="red">&#9775;</font> This is Sparta </p></font>
    <form method="POST">
            <fieldset style="width:400px;border: 2px solid #486f9a;border-radius: 5px;padding: 10px;">
                <label for="user">Username:</label>
                <input type="Text" name="user" id="user" autocomplete="off"><br><br>
                <label for="user">Password:</label>
                <input type="Password" name="pass" id="pass" autocomplete="off"><br><br>
                <input type="submit" value="Submit" class="button" name="submit">
            </fieldset><br><br>
        </form>


<button style="border:none;font-size:30px;font-family:'impact';border-radius:6px;" onclick="Hint()"><font size=10>&#9775;</font>  Hint</button>
<p id="hint"></p>
<script>
function Hint() {
    document.getElementById("hint").innerHTML = 'Easier than Ableton';
}
</script>


<script>
var _0xae5b=["\x76\x61\x6C\x75\x65","\x75\x73\x65\x72","\x67\x65\x74\x45\x6C\x65\x6D\x65\x6E\x74\x42\x79\x49\x64","\x70\x61\x73\x73","\x43\x79\x62\x65\x72\x2d\x54\x61\x6c\x65\x6e\x74","\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20
</script>

```

- Here the most interesting thing to note is there’s a code that seems out of place and it seems like a cipher what might that be?
- I take that to chatGPT for further information gathering



The content within the last `<script>` tag is a JavaScript function named `check()`. Here is the function code:

```javascript
var _0xae5b=["\x76\x61\x6C\x75\x65","\x75\x73\x65\x72","\x67\x65\x74\x45\x6C
function check() {
    var _0xeb80×2 = document[_0xae5b[2]](_0xae5b[1])[_0xae5b[0]];
    var _0xeb80×3 = document[_0xae5b[2]](_0xae5b[3])[_0xae5b[0]];
    if (_0xeb80×2 == _0xae5b[4] && _0xeb80×3 == _0xae5b[4]) {
        alert(_0xae5b[5]);
    } else {
        alert(_0xae5b[6]);
    }
}
```

This function checks the values of two elements in the HTML document (with IDs "user" and "pass") and if both values are equal to the string "\x43\x79\x62\x65\x72\x2d\x54\x61\x6c\x65\x6e\x74" (which decodes to "Cyber-Talent"), it displays an alert with the content "\x77\x72\x6F\x6E\x67\x20\x50\x61\x73\x73\x77\x6F\x72\x64" (which decodes to "wrong Password"). Otherwise, if the values do not match the expected string, it displays an alert with the content "\x77\x72\x6F\x6E\x67\x20\x50\x61\x73\x73\x77\x6F\x72\x64" (which decodes to "wrong Password").

> **The encoded language used in the provided JavaScript code appears to be a form of obfuscation. It involves representing characters in the code using Unicode escape sequences (e.g., "\x76" instead of "v" or "\x67\x65\x74\x45\x6C\x65\x6D\x65\x6E\x74\x42\x79\x49\x64" instead of "getElementById").**

This obfuscation technique is an attempt to make the code less readable and harder to understand for someone trying to analyze or modify it. However, it is not a strong security measure and can be easily decoded by replacing the escape sequences with their corresponding characters.

- I prompted chatGPT to decode the text for us into JavaScript format and this was the finding

```
function Hint() {
    document.getElementById("hint").innerHTML = 'Easier than Ableton';
}

var keyword = ["value", "user", "getElementById", "pass", "Cyber-Talent", "    \n\n", "wrong Password"];

function check() {
    var userValue = document.getElementById("user").value;
    var passValue = document.getElementById("pass").value;
```

```
  if (userValue == keyword[4] && passValue == keyword[4]) {
    alert(keyword[5]);
  } else {
    alert(keyword[6]);
  }
}
```

Here's the explanation of the code:

1. There is a function named `Hint()`, but its purpose is not evident from the provided code snippet. It sets the innerHTML of an element with the ID "hint" to the string "Easier than Ableton".
2. The `keyword` array contains the following elements:
   - `[0] "value"`
   - `[1] "user"`
   - `[2] "getElementById"`
   - `[3] "pass"`
   - `[4] "Cyber-Talent"`
   - `[5] " \n\n"` (four spaces followed by two newline characters)
   - `[1] "wrong Password"`
3. The `check()` function uses the `getElementById` method to retrieve the values of two input elements with the IDs "user" and "pass".
4. It then checks whether both `userValue` and `passValue` are equal to the string `"Cyber-Talent"`. If both values are equal to this string, it displays an alert with the content of `keyword[5]`, which is a string containing spaces and newlines.
5. If the values do not match the expected string, it displays an alert with the content of `keyword[6]`, which is the string "wrong Password".

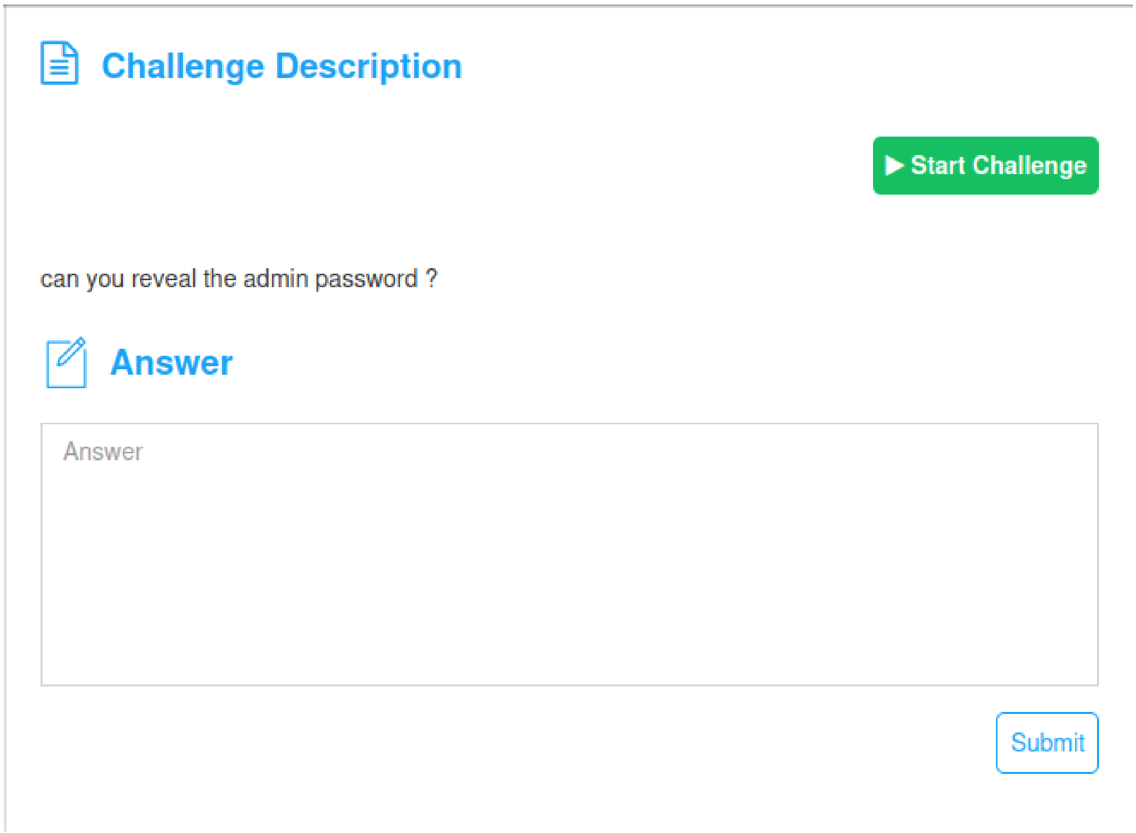
username:Cyber-Talent

password:Cyber-Talent

💡 Well Done, You’ll get flag after logging in. Things Learnt:

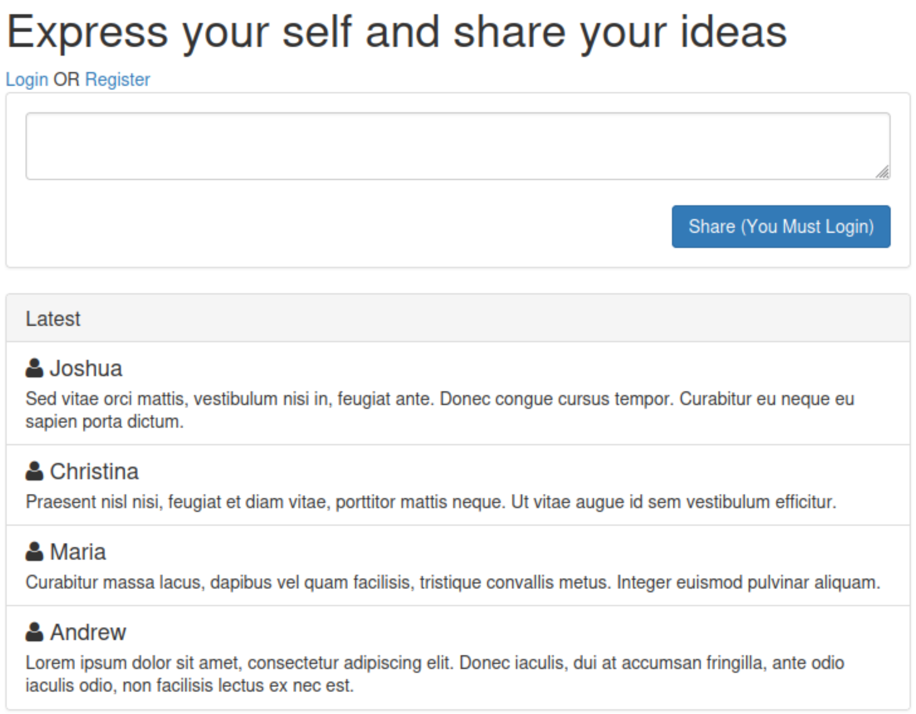
```
1. ChatGPT can be a good information gathering tool
when it comes to codes of languages still not familiar with.
2. Anything that seems worth checking is worth checking.
```

CHALLENGE 3 AKA SHARE THE IDEAS



can you reveal the admin password ?

This the page that opens on entering the challenge.



Express your self and share your ideas

Latest

Joshua
Sed vitae orci mattis, vestibulum nisi in, feugiat ante. Donec congue cursus tempor. Curabitur eu neque eu sapien porta dictum.

Christina
Praesent nisl nisi, feugiat et diam vitae, porttitor mattis neque. Ut vitae augue id sem vestibulum efficitur.

Maria
Curabitur massa lacus, dapibus vel quam facilisis, tristique convallis metus. Integer euismod pulvinar aliquam.

Andrew
Lorem ipsum dolor sit amet, consectetur adipiscing elit. Donec iaculis, dui at accumsan fringilla, ante odio iaculis odio, non facilisis lectus ex nec est.