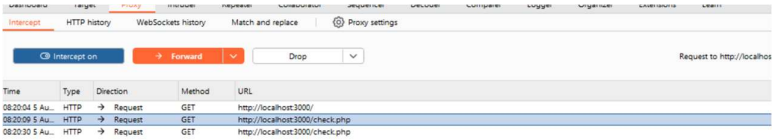
ACM WEEK -3 CHALLENGES

-G.Yeshwanthi Reddy(AM.SC.U4CYS24020)

CHALL1:

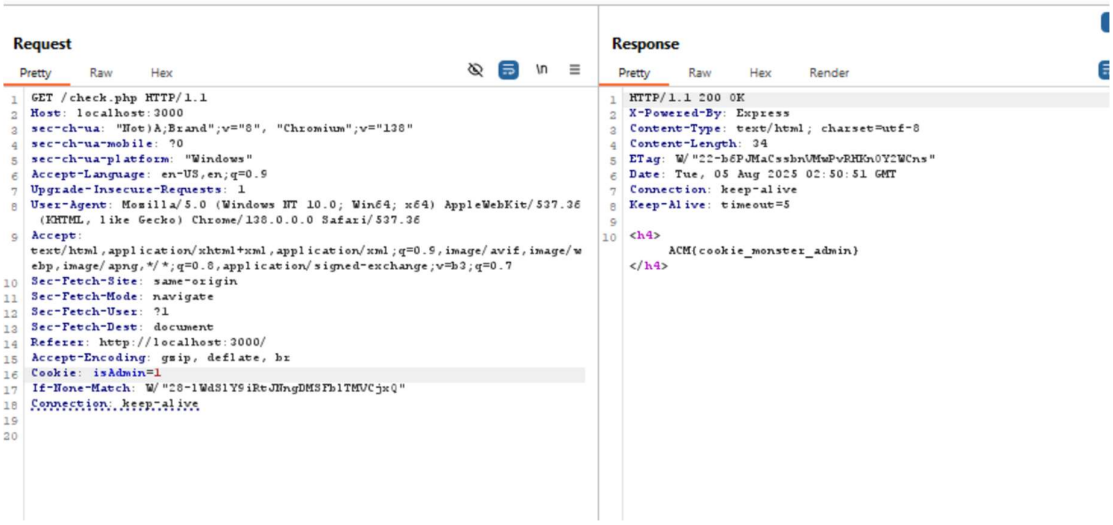
Tools used : burp suit(proxy and repeater)

Process : Used burp suit to modify the http request (isadmin = 0 to isadmin = 1)



Intercepted request to /check.php from proxy

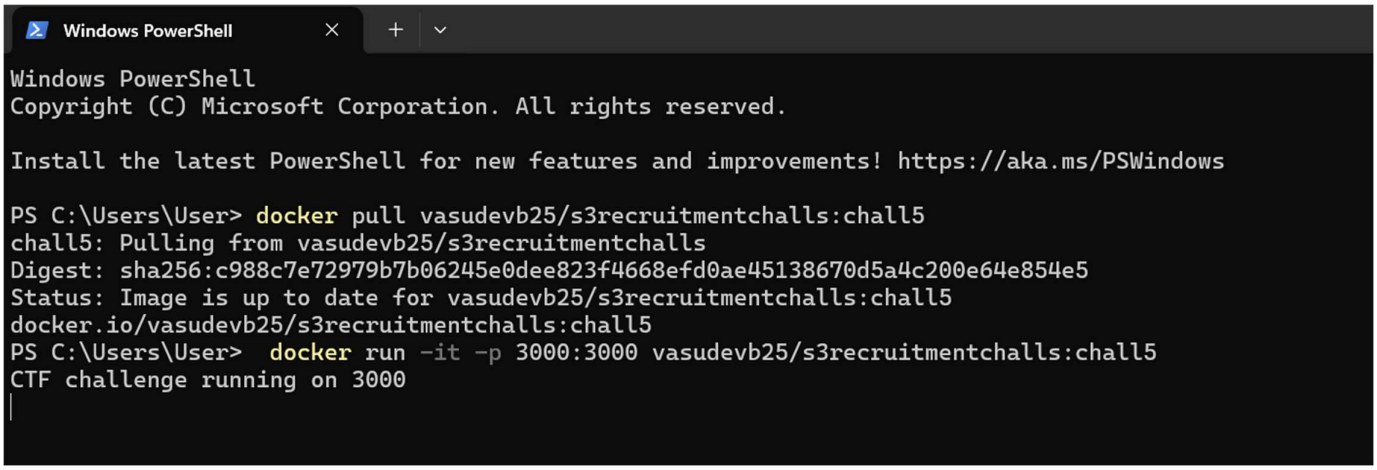
Sent to repeater



Changed the cookie isadmin = 0 to isadmin = 1 and sent the request…got the flag - **ACM{cookie_monster_admin}**

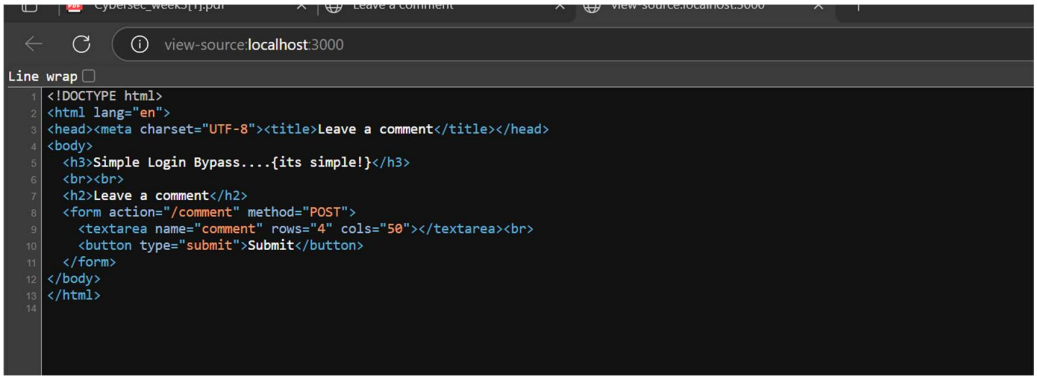
CHALL5:

Tools used : burpsuit

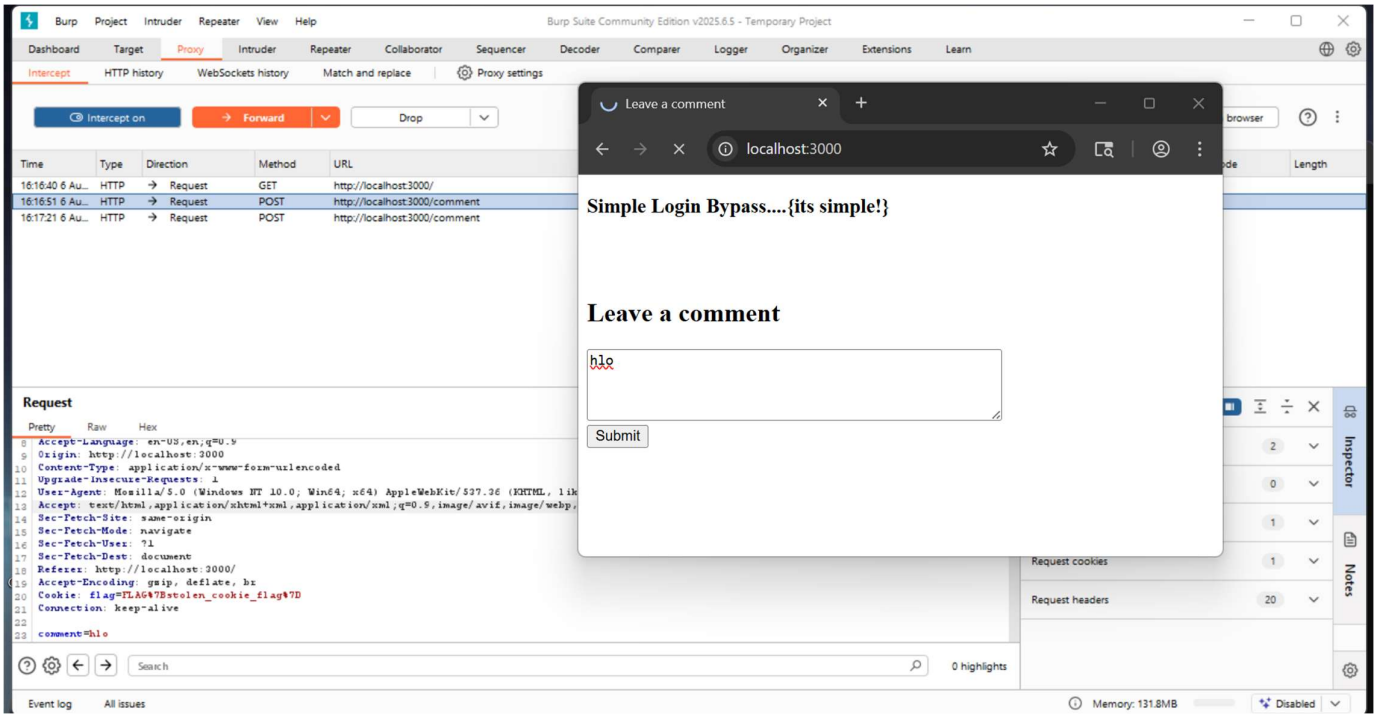


Opened the browser:

Searched in page source for the flag:



AS it says simple bypass login …I tried to run in burpsuit to find any flag



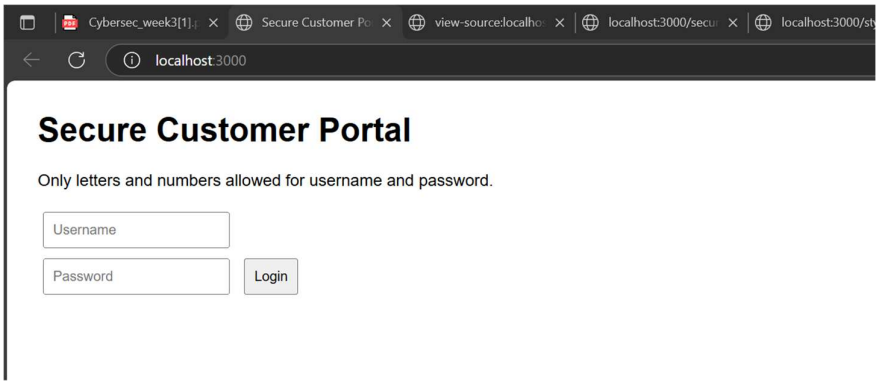
Intercepted the Get request and typed “hlo” in comment to get the POST request ..as we can see in the above pic we got the flag : **FLAG%7Bstolen_cookie_flag%7D**

CHALL3:

Tools used: page source

Process :

```
Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\User> docker pull vasudevb25/s3recruitmentchalls:chall3
chall3: Pulling from vasudevb25/s3recruitmentchalls
Digest: sha256:007fcd78ce5d51821c28f9ac7448bdb9574f9a4219162f13c221f48fd4c755f6
Status: Image is up to date for vasudevb25/s3recruitmentchalls:chall3
docker.io/vasudevb25/s3recruitmentchalls:chall3
PS C:\Users\User>  docker run -it -p 3000:3000 vasudevb25/s3recruitmentchalls:chall3
CTF challenge running on 3000
```

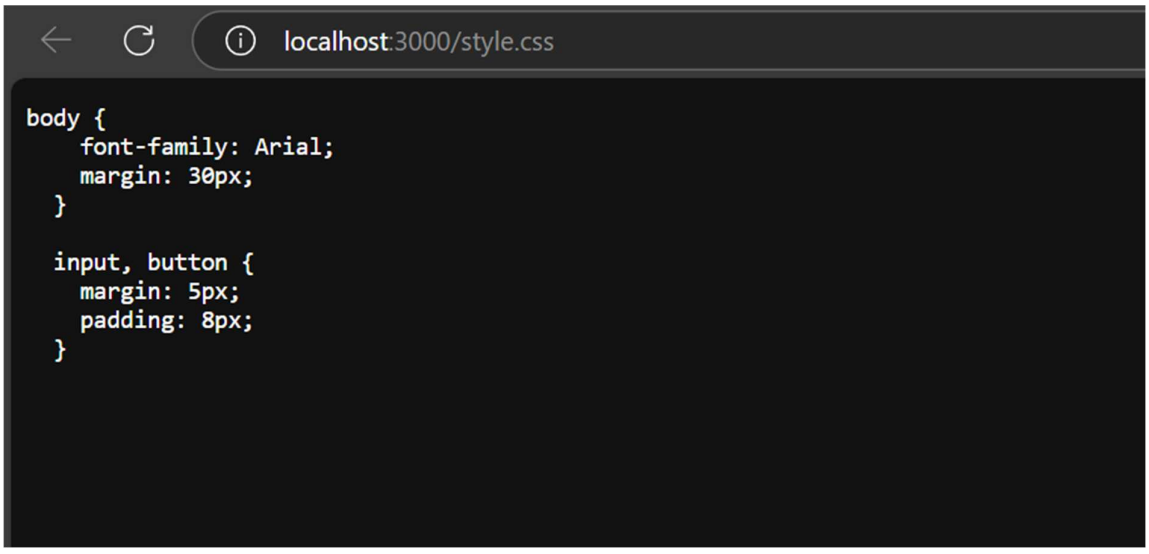


Visited the page source to find any hidden scripts..etc related to flag

Line wrap

```
<!DOCTYPE html>
<html lang="en">
<head>
  <meta charset="UTF-8">
  <title>Secure Customer Portal</title>
  <link rel="stylesheet" href="style.css">
</head>
<body>
  <h1>Secure Customer Portal</h1>
  <p>Only letters and numbers allowed for username and password.</p>

  <form>
    <input type="text" id="username" placeholder="Username" required><br>
    <input type="password" id="password" placeholder="Password" required>
    <button type="button" onclick="login()">Login</button>
  </form>

  <form hidden action="admin.php" method="POST" id="hiddenAdminForm">
    <input type="text" name="hash" id="adminFormHash">
  </form>

  <p id="msg"></p>

  <script src="secure.js"></script>
</body>
</html>

```

Here I found a javascript(secure.js) and css script(style.css) files..lets open it



The above one is style.css script..

Nothing related to flag found from this…

```
function filter(input) {
    for (let i = 0; i < input.length; i++) {
      let cc = input.charCodeAt(i);
      if (!((cc >= 48 && cc <= 57) || (cc >= 65 && cc <= 90) || (cc >= 97 && cc <= 122))) {
        return false;
      }
    }
    return true;
  }

  function checkPassword(username, password) {
    return username === "admin" && password === "strongpassword";
  }

  function login() {
    const user = document.getElementById("username").value;
    const pass = document.getElementById("password").value;

    if (!filter(user) || !filter(pass)) {
      document.getElementById("msg").innerText = "Illegal character in username or password.";
      return;
    }

    if (checkPassword(user, pass)) {
      document.getElementById("msg").innerText = "Login Successful!";
      document.getElementById("adminFormHash").value = "2196812e91c29df34f5e217cfd639881";
      document.getElementById("hiddenAdminForm").submit();
    } else {
      document.getElementById("msg").innerText = "Login Failed!";
    }
  }
```

The above one is secure.js script …here we can see username = admin , password = strongpassword

Entered the login credentials :

ACM{client_side_authentication_is_bad}

Got the flag : **ACM{client_side_authentication_is_bad}**

CHALL2:

Tools used : page source,base64 decoder

Process :

```
Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\User> docker pull vasudevb25/s3recruitmentchalls:chall2
chall2: Pulling from vasudevb25/s3recruitmentchalls
Digest: sha256:644a0235de00a9aeb6445a173461dd29eceadb5c194fd6c78b80f0ff974a00fc
Status: Image is up to date for vasudevb25/s3recruitmentchalls:chall2
docker.io/vasudevb25/s3recruitmentchalls:chall2
PS C:\Users\User>  docker run -it -p 3000:3000 vasudevb25/s3recruitmentchalls:chall2
CTF challenge running on 3000
```

Opened the browser and headed to localhost:3000

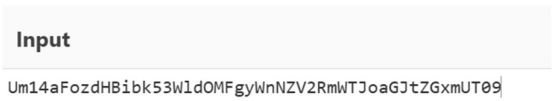
Then got into **about** page and viewed its page source

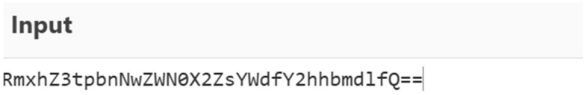
```
Line wrap
<div style="background-color: aqua; min-height: 100vh; position: relative;">
  <section class="about" notify_true="Um14aFozdHBibk53WldOMFgyWnNZV2RmWTJoaGJtZGxmUT09">
    <h1 style="text-align: center; font-size: 50px;">U HAVE BEEN MOGGED BY</h1>
    <img src="2.jpeg" style="width: 30%; height: auto; position: absolute; left: 35%;">
    <footer>
    <h2>HAHAHAHAHA!!!!</h2>
    <h3>Nah just kidding!</h3>
    </footer>
</section>
</div>
```

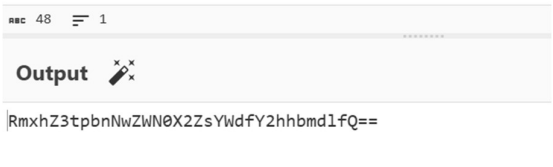
From the page source I found a base64 encoded script

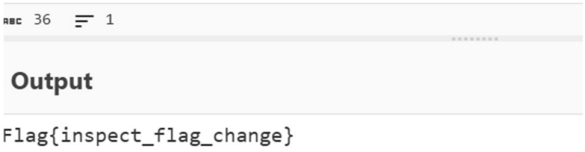
“Um14aFozdHBibk53WldOMFgyWnNZV2RmWTJoaGJtZGxmUT09”

Decoded it 2 times using cyberchef







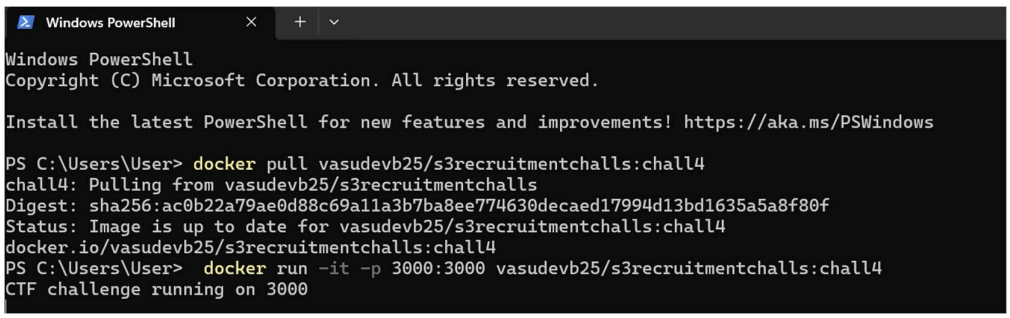


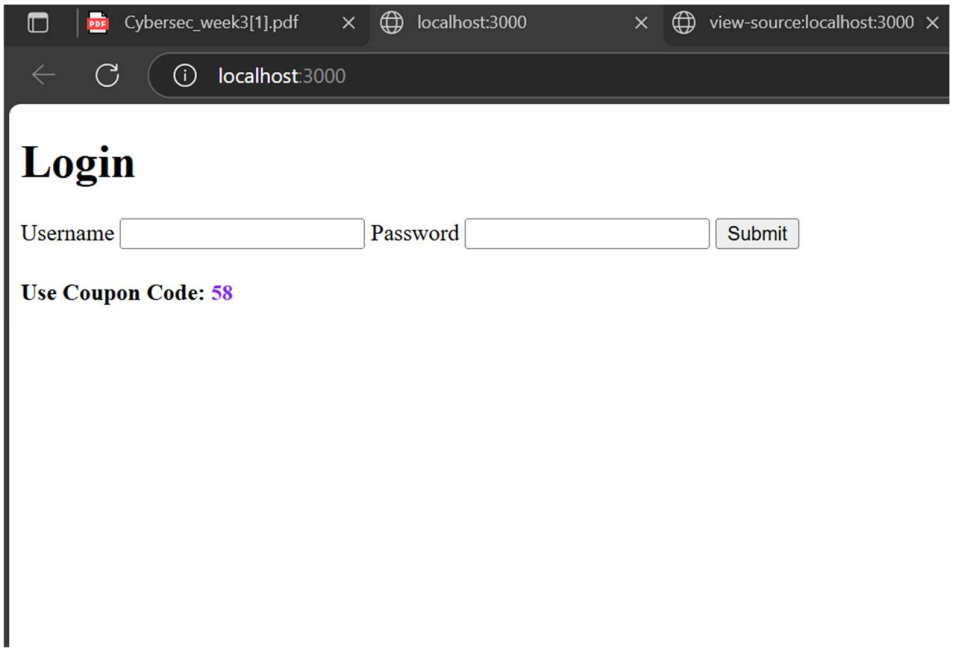
Flag obtained is **Flag{inspect_flag_change}**

CHALL4:

Tools used : page source,base58 decoder

Process :





Viewed page source and found a javascript(index.js)

```
Line wrap
<!doctype html>
<html>
    <head>
        <script src="index.js"></script>
    </head>
    <body>
        <div>
          <h1>Login</h1>
          <form method="POST">
            <label for="username">Username</label>
            <input name="username" type="text"/>
            <label for="username">Password</label>
            <input name="password" type="password"/>
            <input type="submit" value="Submit"/>
          </form>
        </div>
        <h4>Use Coupon Code: <b style="color: blueviolet;font-size: 15px;">58 </b></h4>
    </body>
</html>
```

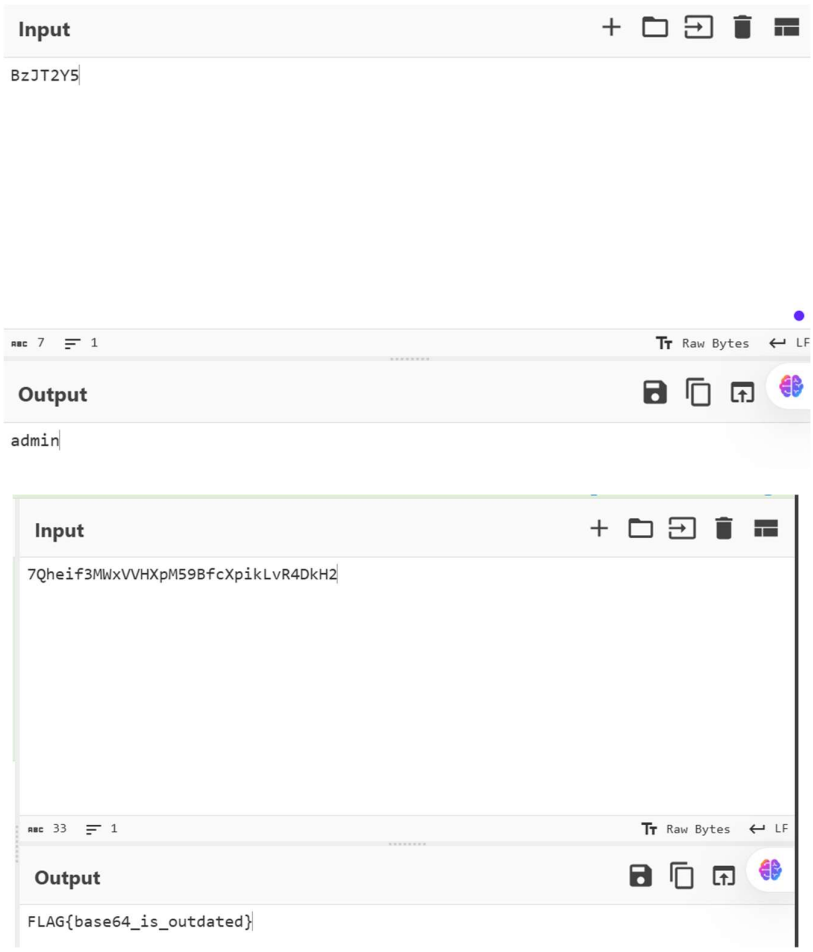
Viewed index.js:

```
(async()=>{function delay(ms){return new Promise(res=>setTimeout(res,ms));}const handler={eventType:"load",listener:(cb)=>window.addEventListener("load",cb)};async function
onReady(){await new Promise(resolve=>{handler.listener(()=>{delay(50).then(resolve);});});}function encodeValue(input){const base64=btoa(input);const
stripped=base64.replace(/=/g,"");const noise=stripped.split("").map(char=>char).join("");return noise;}function revealFlag(encoded){const
decoded=atob(encoded);console.log("Decrypting...");return decoded;}await onReady();const selectors={u:"input[name=username]",p:"input[name=password]"};const keySet=
["BzJT2Y5","7Qheif3MWxVVHXpM59BfcXpikLvR4DkH2"];function auditLog(data){console.debug("Captured Input ->",data);}document.querySelector("form").addEventListener("submit",
(event)=>{event.preventDefault();const inputs={};for(const key in selectors){const
val=document.querySelector(selectors[key]).value;inputs[key]=encodeValue(val);}auditLog(inputs);const checkUser=()=>inputs.u===keySet[0];const checkPass=
()=>inputs.p===keySet[1];return!checkUser()?alert("Incorrect Username"):!checkPass()?alert("Incorrect Password"):void alert(`Correct Password! Your flag is
${revealFlag(inputs.p)}.`);});})();
```

From this we can see a base58 encoded script

"BzJT2Y5","7Qheif3MWxVVHXpM59BfcXpikLvR4DkH2"

Now decode it with cyberchef



By decoding base58 script we got the flag as **FLAG{base64_is_outdated}**