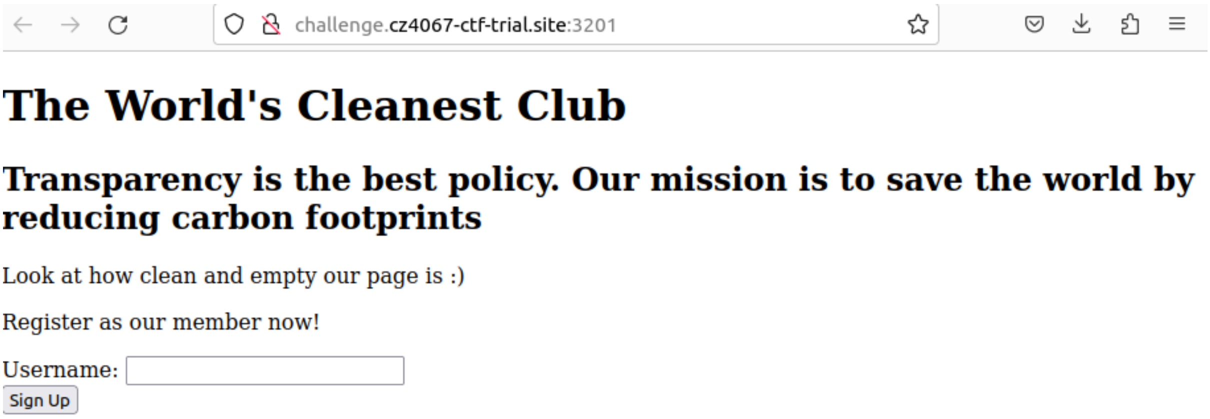
Door Gift CTF hosted on http://challenge.cz4067-ctf-trial.site:3201

1. Try playing around with the website and sign up as a user.



The World's Cleanest Club

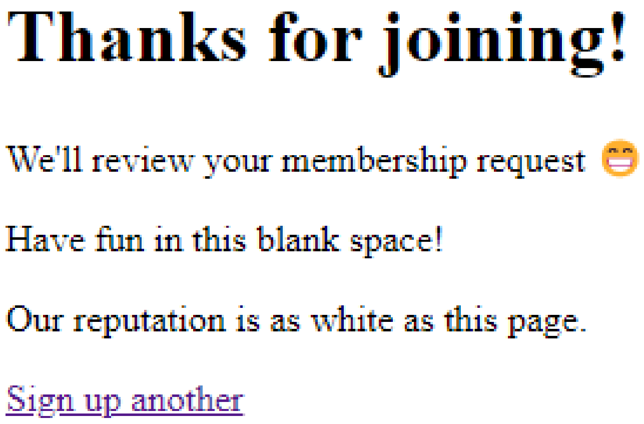
Transparency is the best policy. Our mission is to save the world by reducing carbon footprints

Look at how clean and empty our page is :)

Register as our member now!

Username:

The first step was to sign up as a user and explore the website, which only allowed access to certain pages after registration.



Thanks for joining!

We'll review your membership request 😁

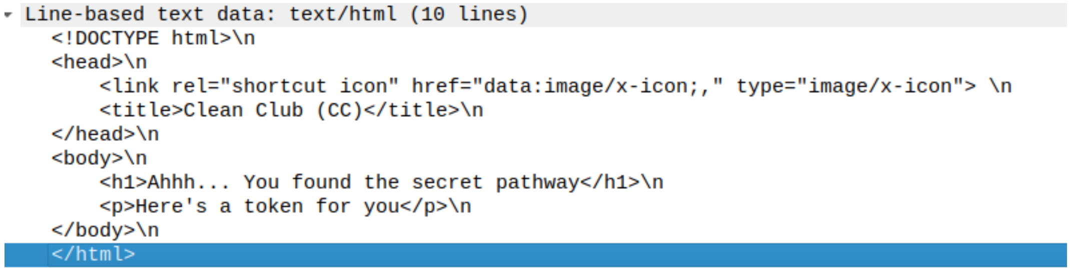
Have fun in this blank space!

Our reputation is as white as this page.

Sign up another

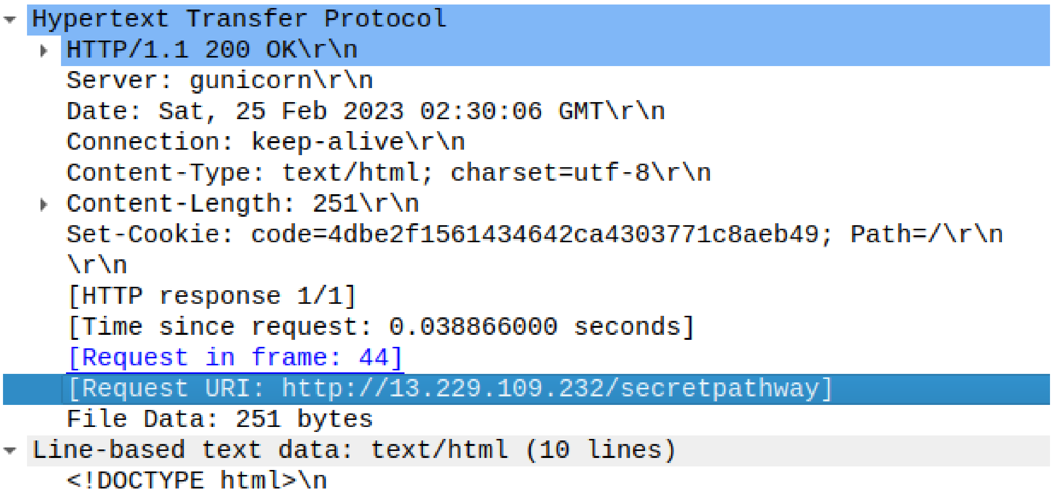
2. The next step was to analyse the pcapng file using either Wireshark or the command $strings asset.pcapng (Will show wireshark demo)

Look though the HTTP protocols with HTTP 200 OK success status; Eventually you will locate an HTML block that revealed the existence of a secret pathway:



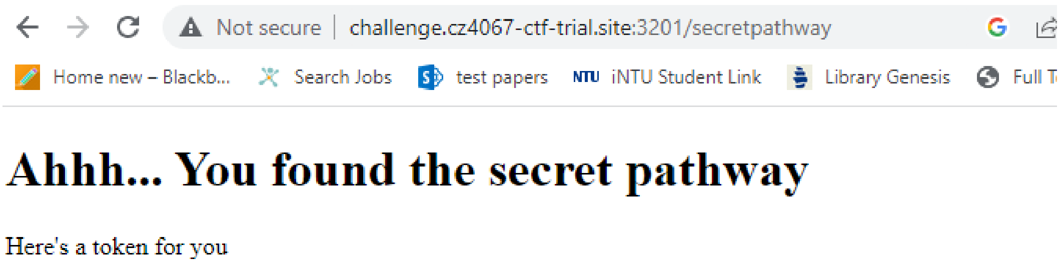
```
▾ Line-based text data: text/html (10 lines)
    <!DOCTYPE html>\n
    <head>\n
        <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> \n
        <title>Clean Club (CC)</title>\n
    </head>\n
    <body>\n
        <h1>Ahhh... You found the secret pathway</h1>\n
        <p>Here's a token for you</p>\n
    </body>\n
    </html>
```

By examining the HTTP information, it was determined that the secret pathway could be accessed by adding "/secretpathway" to the website URL.



```
▾ Hypertext Transfer Protocol
  ▸ HTTP/1.1 200 OK\r\n
    Server: gunicorn\r\n
    Date: Sat, 25 Feb 2023 02:30:06 GMT\r\n
    Connection: keep-alive\r\n
    Content-Type: text/html; charset=utf-8\r\n
  ▸ Content-Length: 251\r\n
    Set-Cookie: code=4dbe2f1561434642ca4303771c8aeb49; Path=/\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.038866000 seconds]
    [Request in frame: 44]
    [Request URI: http://13.229.109.232/secretpathway]
    File Data: 251 bytes
▾ Line-based text data: text/html (10 lines)
    <!DOCTYPE html>\n
```

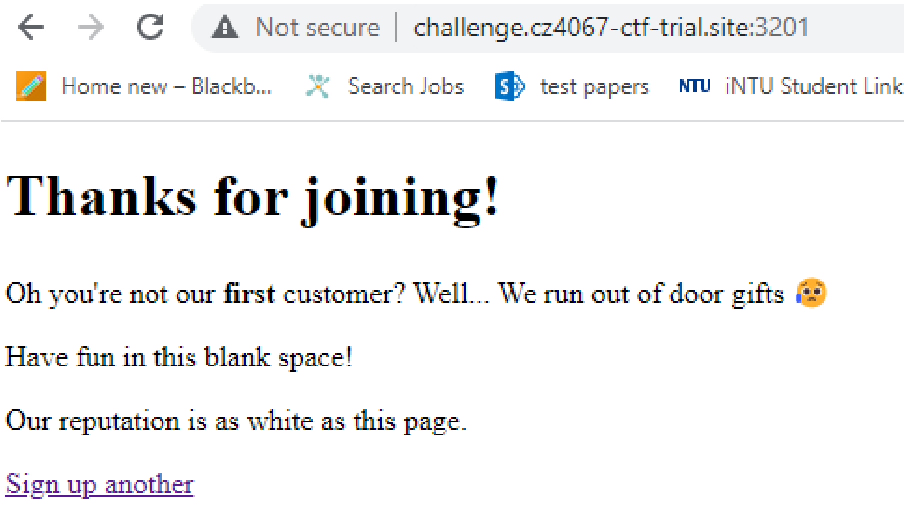
However, this pathway did not contain the flag.



Ahhh... You found the secret pathway

Here's a token for you

3. Let’s go back to the main page and register again, we are now registered BUT we are not the **first** customer. So, we can infer that only the first customer is able to get access to the token.



Thanks for joining!

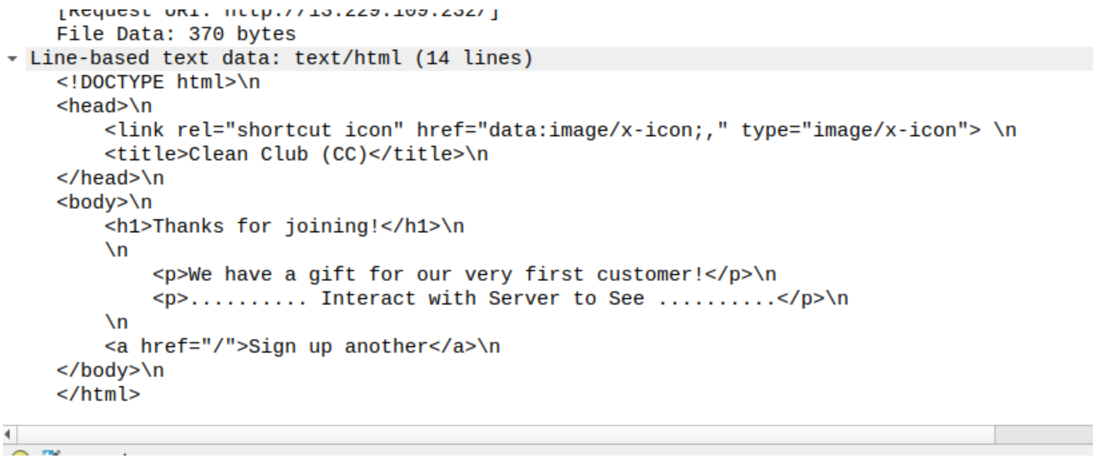
Oh you're not our **first** customer? Well... We run out of door gifts 😢

Have fun in this blank space!

Our reputation is as white as this page.

Sign up another

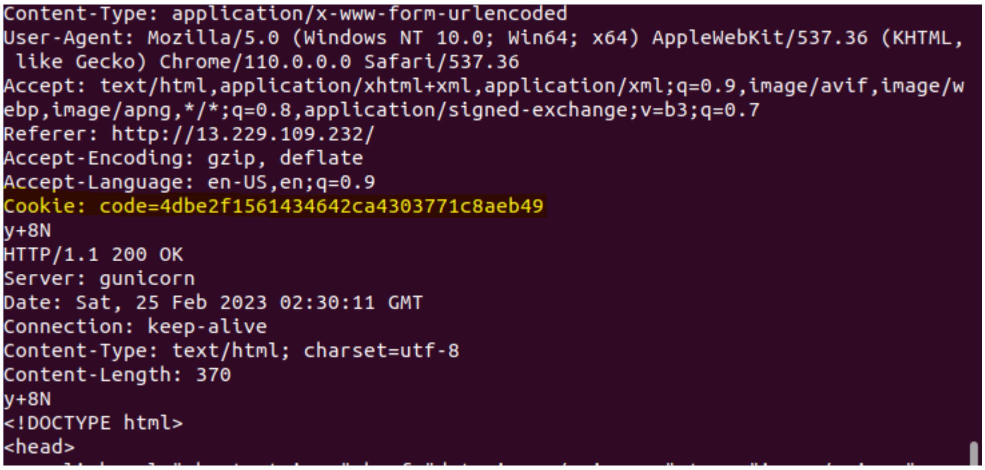
4. To obtain this token, the pcapng file was inspected again to locate the first customer's login page and find their cookie information. (look at the html for those with HTTP 200 status OK). We found a page which shows the following:



```
    [Request URI: http://13.229.109.232/]
    File Data: 370 bytes
▾ Line-based text data: text/html (14 lines)
    <!DOCTYPE html>\n
    <head>\n
        <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> \n
        <title>Clean Club (CC)</title>\n
    </head>\n
    <body>\n
        <h1>Thanks for joining!</h1>\n
        \n
            <p>We have a gift for our very first customer!</p>\n
            <p>.......... Interact with Server to See ..........</p>\n
        \n
        <a href="/">Sign up another</a>\n
    </body>\n
    </html>
```

Now, we need to look for "cookies" of the first customer. It is abit tricky to look for that info on wireshark hence I am doing it via $strings asset.pcapng in the terminal.

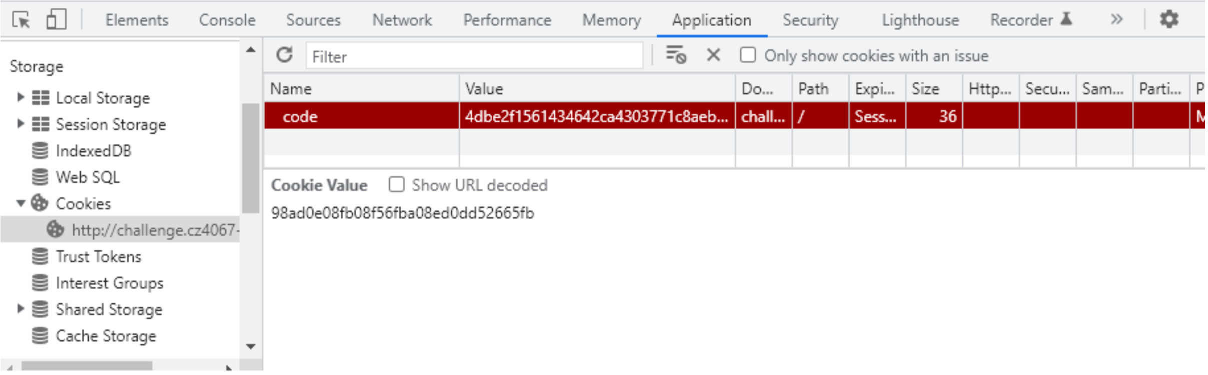
Just slightly above the html info, we are able to find the cookie



```
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/110.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/w
ebp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://13.229.109.232/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: code=4dbe2f1561434642ca4303771c8aeb49
y+8N
HTTP/1.1 200 OK
Server: gunicorn
Date: Sat, 25 Feb 2023 02:30:11 GMT
Connection: keep-alive
Content-Type: text/html; charset=utf-8
Content-Length: 370
y+8N
<!DOCTYPE html>
<head>
```

5. Modify cookie

Now go to the main page (sign up page) and modify the cookie. Go to Application and select cookies and change it

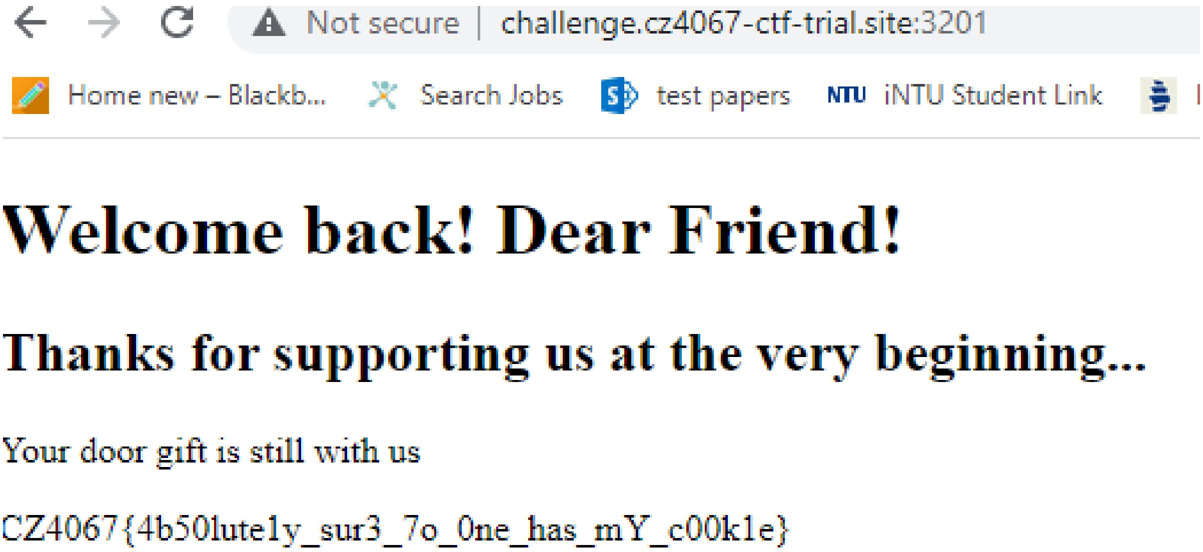


Name	Value	Do...	Path	Expi...	Size	Http...	Secu...	Sam...	Parti...	P
code	4dbe2f1561434642ca4303771c8aeb...	chall...	/	Sess...	36					M

Cookie Value ☐ Show URL decoded

98ad0e08fb08f56fba08ed0dd52665fb

Once you changed it, sign up again and the flag will show.



Welcome back! Dear Friend!

Thanks for supporting us at the very beginning...

Your door gift is still with us

CZ4067{4b50lute1y_sur3_7o_0ne_has_mY_c00k1e}