Zomato CTF

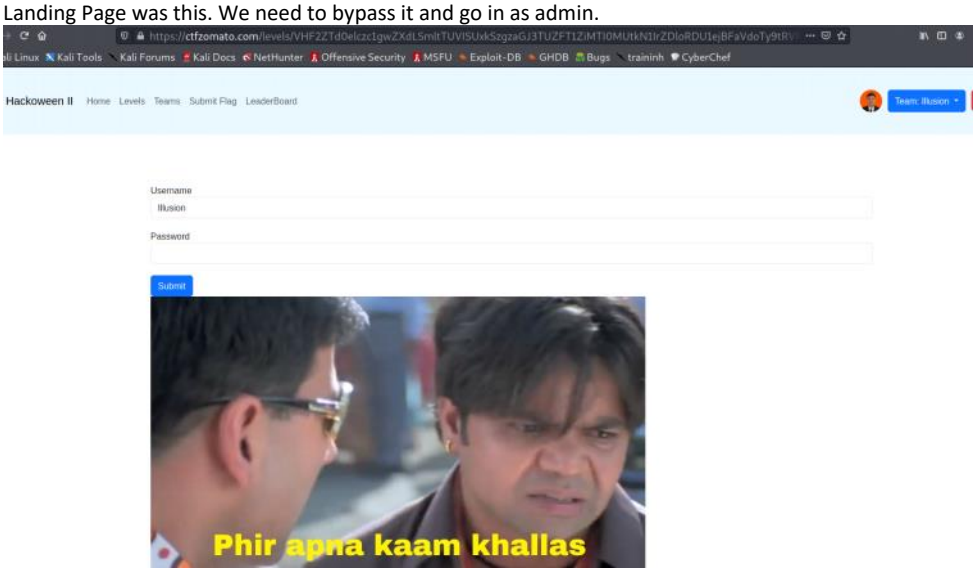
10 October 2023 23:47

Level 0:

Flag was there!

Level 1:

Landing Page was this. We need to bypass it and go in as admin.



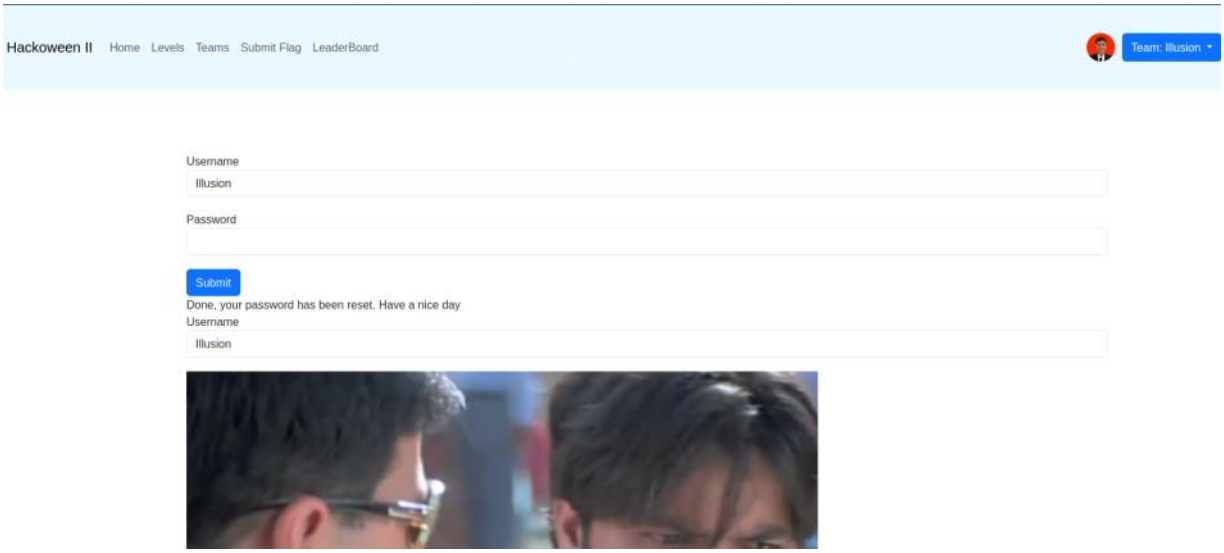
Tried admin:admin
Output Message - "It is not that simple."

Tried Administrator: different password
Output Message- "Host is right but not the credentials, invalid username."

This meant username is admin only, tried SQL injection to bypass it but failed. On inspecting found hidden field authentication token, but nothing particular there.

Came back after some time, the username already has Illusion as value (as seen in above image), I didn't setup any password there so what password? Tried random password, and we got to following page.

Clicked on reset request,



But where is password?

Fired up burp and intercepted response also. Intercepted the Reset request again and changed username to admin.

```
Pretty Raw Hex \n
1 POST
/levels/VHF2ZTdOelczc1gwZXdLSmltTUVISUxkSzgzaGJ3TUZFT1ZiMTI0MUtkN1IrZDloRDU1ejBFaVdoTy9tRVRXTlBoNjE3SXNjTSt6U0diNDdBRE1LSmdLcEZtWWk4b1BtZ0JqcU9jajlJSitiME5oZ1B6Mjh2Zk9xVkowc3dr
XlONWowa2lXM3VscDgwNXljcXNOWlExROktLVkrVkdINVFxeGxVWEl3YVktLUV3S2EwZXlLZlMwdzVhUTFJemRheVE9PQ== HTTP/2
2 Host: ctfzomato.com
3 Cookie: _hackathon2_session=
lwNodH3RaZzyByuSIxaKGOLT6D0%2B6fGP%2FiADZNzCrgO%2FvJsD6qsrEkXnjVLgAwl2rRVI%2BDPu8bp508GE3a9depHUODJhsb458jUj7qwheaeLkmeFRcKGBkiIcXdGfG3YEtFeDP%2Bu6HfHsQaYR2vnmFBONc5%2FiREZ%2Br
jOKJghh94P%2B0vH1FxB%2F63vC2L9rmt2AUHKDS3NGWvsvoORi5gO8P3yWS2Wj0F2ZaKmhJUJsaR2Wg6VWdzJC2ECKHIg7NTR%2Fx6fw8JmiRum4fsYK2iRipCqXgycSP3GOtEKexk4u27Fq73Id5lu7K6UFue%2BlJPNnvcS3IQDwc
6pmRLGAe%2FqSDdnvvu658SvI5mPUznbbaW33zpsnMxkROKmPwIGp6KphqDSYl7LbAedE45HpS--pZTbQCULSwolvWgF--jvDR%2Bznus5uqLi1HQ87Muw%3D%3D
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Referer:
https://ctfzomato.com/levels/VHF2ZTdOelczc1gwZXdLSmltTUVISUxkSzgzaGJ3TUZFT1ZiMTI0MUtkN1IrZDloRDU1ejBFaVdoTy9tRVRXTlBoNjE3SXNjTSt6U0diNDdBRE1LSmdLcEZtWWk4b1BtZ0JqcU9jajlJSitiME5
Z1B6Mjh2Zk9xVkowc3drMXlONWowa2lXM3VscDgwNXljcXNOWlExROktLVkrVkdINVFxeGxVWEl3YVktLUV3S2EwZXlLZlMwdzVhUTFJemRheVE9PQ==
9 Content-Type: application/x-www-form-urlencoded
10 Content-Length: 238
11 Origin: https://ctfzomato.com
12 Upgrade-Insecure-Requests: 1
13 Te: trailers
14
15 authenticity_token=LULhBiOReii-2OkOgYP25rOHhlMhaSsjS9ei8FK3E7cmdbngAgzuPVBW9Gd92YgGNrSiuaBXdF2vV3lOxu-oqw&username=admin&reset-request-id=
VGlhUVVRPTOtLUJucC9SNzlOME9scjRJc3MtLXROTlU3OU5USUlGaWxndDQwK3JZZ1E9PQ%3D%3D&commit=Request+Reset
```

Here is response

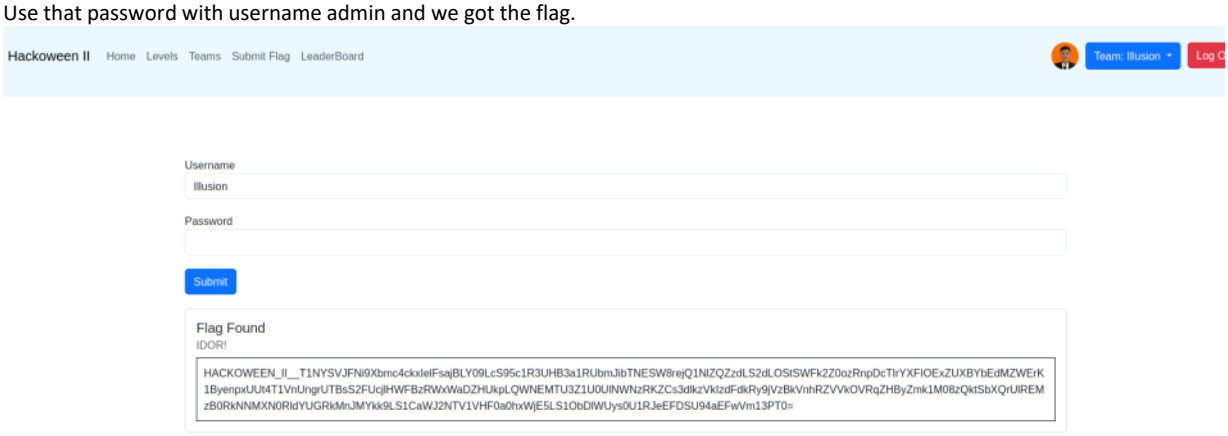
Response from https://ctfzomato.com:443/levels/VHF2ZTdOelczc1gwZXdLSmltTUVISUxkSzgzaGJ3TUZFT1ZiMTI0MUtkN1IrZDloRDU1ejBFaVdoTy9tRVRXTlBoNjE3SXNjTSt6U0diNDdBRE1LSmdLcEZtWWk4b1BtZ0JqcU9jajlJSitiME5oZ1B

Forward | Drop | Intercept is on | Action | Open Browser | Comment this item

Pretty Raw Hex Render \n

```
83          </div>
84        </div>
85      </nav>
86
87      <main class="container" style="padding-top: 4em;">
88
89        <form action="/levels/VHF2ZTdOelczc1gwZXdLSmltTUVISUxkSzgzaGJ3TUZFT1ZiMTI0MUtkN1IrZDloRDU1ejBFaVdoTy9tRVRXTlBoNjE3SXNjTSt6U0diNDdBRE1LSmdLcEZtWWk4b1BtZ0JqcU9jajlJSit
          <input type="hidden" name="authenticity_token" value="lvBA6Ff_-ION6ulu0I95KA4CTmA5Y28nI-ZGrQGsmz6dxxj6dmJslmNk9Acs1QfIhbFqirhdMFnHZpOplfQgIg" autocomplete="off" />
90        <div class="form-group" style="padding-bottom: 20px;">
91          <label for="Username">
              Username
            </label>
92          <input type="text" class="form-control" id="username" name="username" value="Illusion" required>
93        </div>
94        <div class="form-group" style="padding-bottom: 20px;">
95          <label for="password">
              Password
            </label>
96          <input type="password" class="form-control" name="password" id="password" value="" required>
97        </div>
98        <input type="submit" name="commit" value="Submit" class="btn btn-primary" data-disable-with="Submit" />
99      </form>
100
101     <form action="/levels/VHF2ZTdOelczc1gwZXdLSmltTUVISUxkSzgzaGJ3TUZFT1ZiMTI0MUtkN1IrZDloRDU1ejBFaVdoTy9tRVRXTlBoNjE3SXNjTSt6U0diNDdBRE1LSmdLcEZtWWk4b1BtZ0JqcU9jajlJSit
          <input type="hidden" name="authenticity_token" value="Tr8nPNFMRyP32_M30a_v8gcvSase8XEwlY9AG5Y-V39FiH8u8NHTNhlV7l4t9ZESjJxtQZ_PLk5xD5ufAmbsYw" autocomplete="off" />
102       Done, your password has been reset. Have a nice day
103       <div class="form-group" style="padding-bottom: 20px;">
104         <label for="Username">
              Username
            </label>
105         <input type="text" class="form-control" id="username" name="username" value="Illusion" required >
106       </div>
107       <input type="text" class="form-control" id="password"  value="12de5c8b78d0f3f14aec3a5d60a1aea17cb7ea37" hidden="true">
108     </form>
109
110
111     <img class="img-fluid" src="https://i.imgflip.com/5dc81q.jpg"/>
112
113   </main>
114
115   <script data-cfasync="false" src="/cdn-cgi/scripts/5c5dd728/cloudflare-static/email-decode.min.js">
      </script>
    </body>
116 </html>
117
```

We got the password hidden.
Use that password with username admin and we got the flag.



Level 2: Tip of the Iceberg (enter code after @@)

PGP private key block in the source code

Level 3: Fuzz-Buzz (Need access)

A parameter encoded in base64. On decoding it we got the obfuscated JavaScript in jsfuck. Decoding that give old_value;new_value. Tried changing grant_access parameter in the request to true but no luck!

Level 4: Git to the core

Found this "https://gist.github.com/jatindhankhar/1674eb5a892ea5b932e99929b18fecf5.js" from the source code.

Level 12: Detective Work

(Forgot to download all the images). Solved 10/14 challenges

Challenge 1: Samsung factory Noida 201305 - google lens

Challenge 2: Mayanmar - reverse search

Challenge 3: 80331 (Munich, germany) (google lens the hotel name, first link which we'll get is https://benjaminstrick.com/finding-mcafee-a-case-study-on-geoprofiling-and-imagery-analysis/ exact location is given in this blog.

Challenge 4:

Challenge 5:

First I searched EasyJet flights on 17 august, goa really long list of cities. Then zooming in and clearing some text I got the number on plane to be somewhat G-EZB0 which has airplane number A319, Filtered out the cities where a319 landed or took off. Reverse searching image on Yandex with focus on windmills got me runway 18r which happens to be in Amsterdam.
Flight is either https://www.flightaware.com/live/flight/EZY2516/history/20230817/1040Z/EHAM/EGGW
https://www.flightaware.com/live/flight/EZY2517/history/20230817/1155Z/EGGW/EHAM
https://www.alamy.com/stock-photo-g-ezfm-aircraft-taxiing-after-landing-on-runway-18r-pic2-128844810.html

Challenge 6:
Google lens on train
train number 461-030
Montenegro country

Challenge 7:

Challenge 8:

Hostinec and saris got me into Europe and that too in Czech and Slovakia. Saris locations are mostly in Slovakia, so took a shot and got lucky.

Challenge 9:

Crop the photo and tried reverse image searching with only the board sign. The middle line says the greens got this link https://www.savaari.com/blog/top-10-places-of-south-india/
City: Ooty

Challenge 10:

tried Jharkhand, Chhattisgarh, Karnataka, Kerala, Maharashtra, but no luck.

Challenge 11:
Both these images are from same hotel, need to find that.

Siam design hotel,
Reverse searching second image it shows the location is pattaya and the view is somewhat similar to second image.
https://yandex.com/images/search?cbir_id=9462544%2FS06Pn265f1l1NEbrqKR22w8252&cbir_page=similar&lr=10562&rpt=imageview&url=https%

3A%2F%2Favatars.mds.yandex.net%2Fget-images-cbir%2F9462544%2FS06Pn265f1l1NEbrqKR22w8252%2Forig

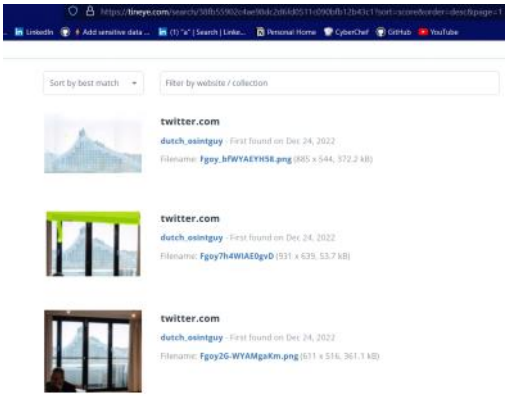
Challenge 12: seems antilia (Mumbai) and biowonder (Kolkata)

Challenge 13:

Using Google lens focusing on two unique buildings, I got a medium article where same image was given as challenge.
https://samanthactf.medium.com/downunderctf-2021-24-26-sept-86d12bafcdb6

Challenge 14:

Google reverse searching didn't work.
Although I could remove the window and then search for the monument but I was lazy.
Searched on tineye and got the results



Checked the dutch_osintguy twitter but it seems he has removed it.
The first image on reverse searching reveals the monument name: National Library of Latvia, city = Riga.