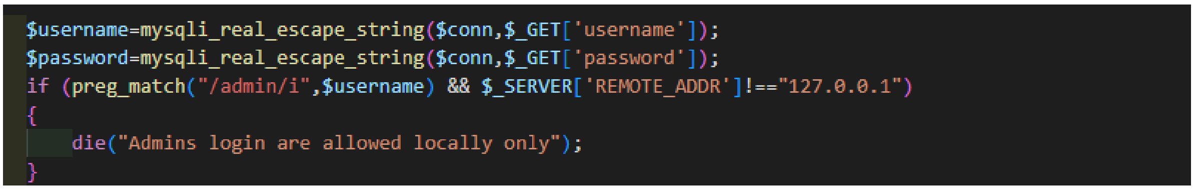
Bruh2 Web challenge writeup

```
he is my brother , can he pass instead of me again ?
```

```
<?php

$servername = "127.0.0.1";
$username = "ctf";
$dbname = "login";
$password = "ctf123";

// Create connection
$conn = new mysqli($servername, $username, $password,$dbname);

// Check connection
if ($conn->connect_error) {
    die("Connection failed: " . $conn->connect_error);
}

if(!empty($_GET['username']) && !empty($_GET['password']))
{
    $username=mysqli_real_escape_string($conn,$_GET['username']);
    $password=mysqli_real_escape_string($conn,$_GET['password']);
    if (preg_match("/admin/i",$username) && $_SERVER['REMOTE_ADDR']!=="127.0.0.1")
    {
        die("Admins login are allowed locally only");
    }
    else
    {
        $res=$conn->query("select * from users where username='$username' and password='$password'"); # admin admin
        if($res->num_rows > 0)
        {
            $user=$res->fetch_assoc();
            echo ($user['username']==="admin")?"0xL4ugh{My_Broo_Ag@in_fREE_pALESTINE}":"sorry u r not admin";
        }
        else
        {
            echo "Error : Wrong Creds";
        }

    }
}
else
{
    echo "Please Fill All Fields";
}
?>
```

As you can bypass it from the previous challenge (bruh) so i am using php regex now to check is the username contains admin or not and i added 'i' flag to make it case insensitive



```
$username=mysqli_real_escape_string($conn,$_GET['username']);
$password=mysqli_real_escape_string($conn,$_GET['password']);
if (preg_match("/admin/i",$username) && $_SERVER['REMOTE_ADDR']!=="127.0.0.1")
{
    die("Admins login are allowed locally only");
}
```

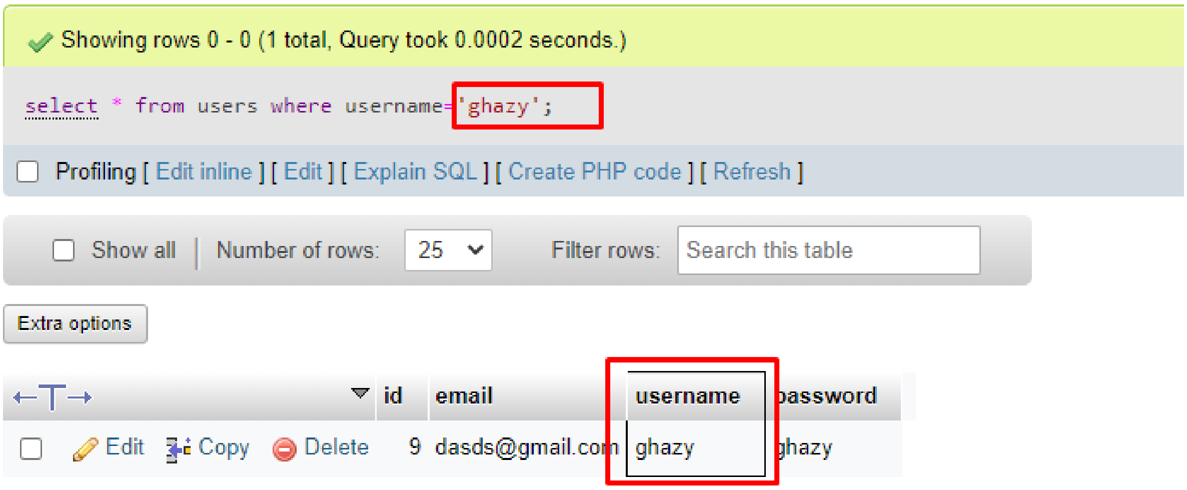
so , now u cannot use "admin" or "admin " as in the "bruh" challenge

the bug here is the sql by default normalizing your string so if we use a unicode character it will be normalized to a alphabet character

Example :

when we use

`select * from users where username='ghazy';`



✓ Showing rows 0 - 0 (1 total, Query took 0.0002 seconds.)

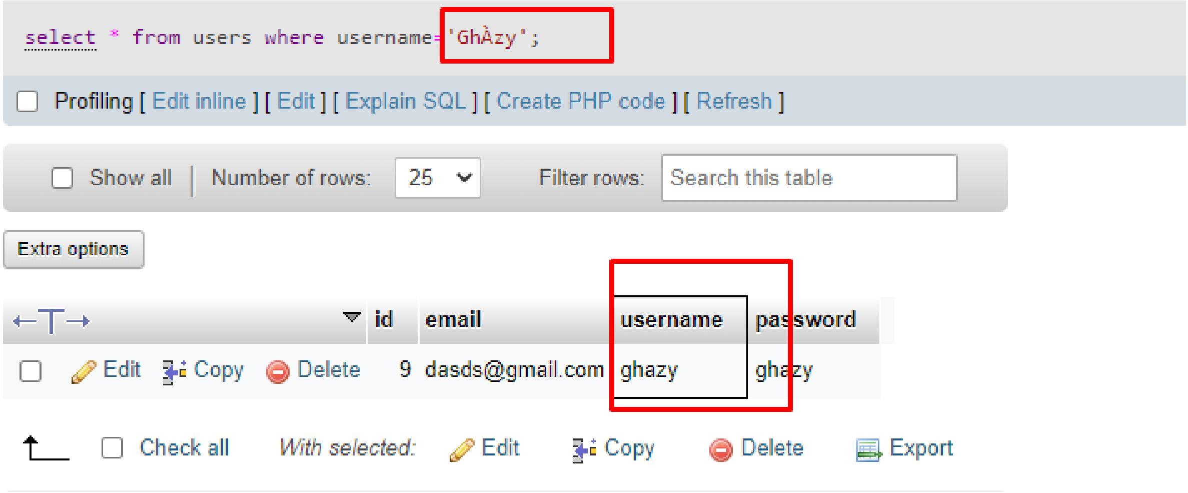
```
select * from users where username='ghazy';
```

□ Profiling [Edit inline] [Edit] [Explain SQL] [Create PHP code] [Refresh]
□ Show all | Number of rows: 25 Filter rows: Search this table
Extra options
←T→
Edit
Copy
Delete

id	email	username	password
9	dasds@gmail.com	ghazy	ghazy

is equal to

`select * from users where username='GhÀzy';`



```
select * from users where username='GhÀzy';
```

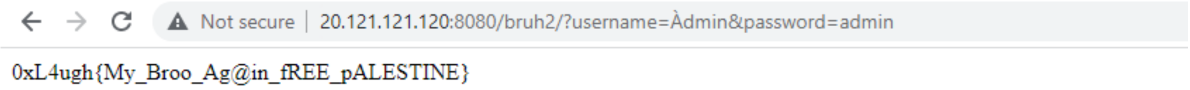
□ Profiling [Edit inline] [Edit] [Explain SQL] [Create PHP code] [Refresh]
□ Show all
Number of rows: 25
Filter rows: Search this table
Extra options
←T→

	id	email	username	password
□ Edit Copy Delete	9	dasds@gmail.com	ghazy	ghazy

□ Check all
With selected: Edit Copy Delete Export

So we just will use

?username=Àdmin&password=admin



```
20.121.121.120:8080/bruh2/?username=Àdmin&password=admin
```

```
0xL4ugh{My_Broo_Ag@in_fREE_pALESTINE}
```