Bruh Web challenge writeup

```
he is my brother , can he go instead of me ?
```

```
<?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,$_GET['password']);
    if ($username=="admin" && $_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{oH_mY_BruuoohH_pLAEStine_iN_our_Hearts}":
"sorry u r not admin";
        }
        else
        {
            echo "Error : Wrong Creds";
        }

    }
}
else
```

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

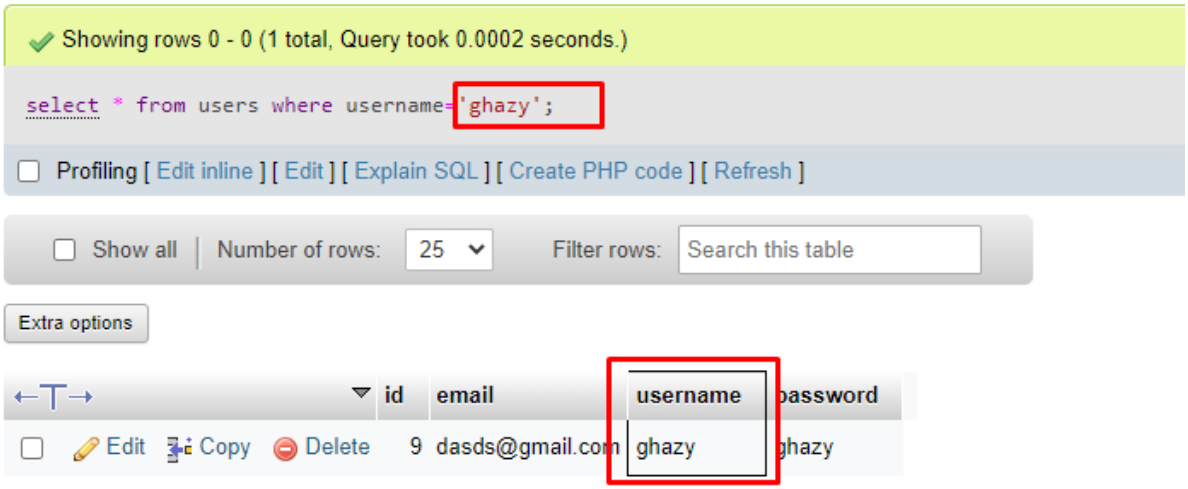
As you can see from the source it's just checking if the username==admin and the request is came from the localhost

and then if it's not admin so the query will work and i put the admin creds beside the query

The main point here is the sql query is case insensitive by default

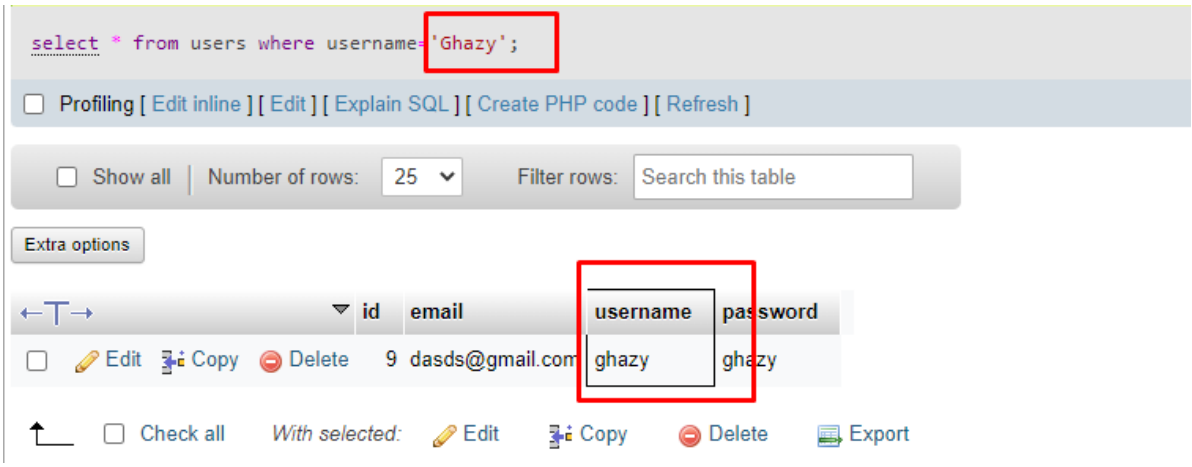
Example :

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



is equal to

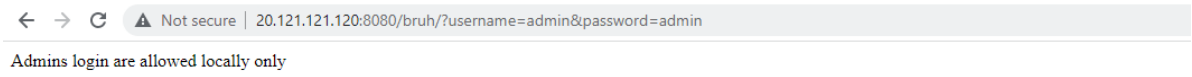
```
select * from users where username='Ghazy';
```



both will return same thing so we can easily bypassing the filter with this : Admin

so this condition will not work

```php
if ($username=="admin" && $_SERVER['REMOTE_ADDR']!=="127.0.0.1")
{
    die("Admins login are allowed locally only");
}
```



Admins login are allowed locally only

and then u will be in this point

```php
$res=$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{oH_mY_BruuoohH_pLAEStine_iN_our_Hearts}":"sorry u r not admin";
}
else
{
    echo "Error : Wrong Creds";
}
```

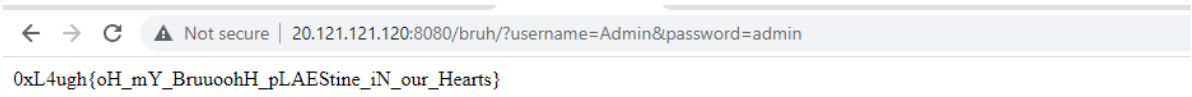
providing username=Admin&password=admin will make the query like this :

`select * from users where username='Admin' and password='admin';`

which will return the same result as this query

`select * from users where username='admin' and password='admin';`

and the the username in the result will be the original one so u will get the flag by http://20.121.121.120:8080/bruh/?username=Admin&password=admin



0xL4ugh{oH_mY_BruuoohH_pLAEStine_iN_our_Hearts}

Note: u can bypass it by add a single space ater admin like : "admin " it will work also