

Forum:[Hack Forums](#)

Thread: [Not getting any rows search engine](#)

deadsh0t - November 9, 2018, 3:05 am

so i got a form on a page to search and i made a search engine that gos to search.php however i keep getting 0 rows so it displays nothing found

what i tried:

PHP Code

```
<?php
```

```
$sql1 = "SELECT ID,title,magnet,date FROM torrents WHERE title LIKE '%" . mysqli_escape_string($_POST['torrent']) . "%'";
```

PHP Code

```
<?php
```

```
$sql1 = "SELECT ID,title,magnet,date FROM torrents WHERE title LIKE '%{' . $_POST['torrent'] . "%'";
```

PHP Code

```
<?php
```

```
$sql1 = "SELECT ID,title,magnet,date FROM torrents WHERE title LIKE '" . $_POST['torrent'] . "'";
```

But i keep getting 0 rows even when i type the exact title

Okay im now really confused so i started from scratch and now this:

PHP Code

```
<?php
```

```
$torrent = $_POST['torrent'];
```

```
$conn = new mysqli($dbHost,$dbUsername,$dbPassword,$dbName);
```

```
$sql1 = "SELECT ID,title,magnet,date FROM torrents WHERE title LIKE '%" . mysqli_escape_string($torrent) . "%'";
```

shows all rows from my database

UPDATE:

So i got it to work using mysqli by using this :

PHP Code

```
<?php
```

```
$sql1 = "SELECT ID,title,magnet,date FROM torrents WHERE title LIKE '%" . $conn->real_escape_string($torrent) . "%'";
```

however i would still like to know how to get it to work in PDO

Vuln - November 9, 2018, 3:28 am

The query syntax is fine. Do other queries fail as well?

FoxBlood - November 9, 2018, 3:38 am

Maybe the bug isn't in your sql, check if you get the post request variable. Why you didn't use PDO?

deadsh0t - November 9, 2018, 6:04 am

(Nov 9, 2018 04:28 AM)Jailbyte Wrote: [\[CITE\]](#) The query syntax is fine. Do other queries fail as well?

(Nov 9, 2018 04:38 AM)FoxBlood Wrote: [\[CITE\]](#) Maybe the bug isn't in your sql, check if you get the post request variable. Why you didn't use PDO?

The post variable is fine because i echo it and it displays i dont use pdo cause i never used it before but i might consider using it .

If i remove the where clause it puts out every row but as soon as i put the where clause there and type a letter or even the identical title of 1 of the rows it still displays nothing and the row count is 0

(Nov 9, 2018 04:38 AM)FoxBlood Wrote: [\[CITE\]](#) Maybe the bug isn't in your sql, check if you get the post request variable. Why you didn't use PDO?

tried pdo doesnt work with this :

PHP Code

```
<?php
```

```
$stmt = $db->query('SELECT * FROM torrents WHERE title LIKE "%' . mysqli_escape_string($torrent).'%");
```

it displays all the rows

TCP - November 9, 2018, 6:41 am

(Nov 9, 2018 07:04 AM)deadsh0t Wrote: [\[CITE\]](#) The post variable is fine because i echo it and it displays i dont use pdo cause i never used it before but i might consider using it .

If i remove the where clause it puts out every row but as soon as i put the where clause there and type a letter or even the identical title of 1 of the rows it still displays nothing and the row count is 0

tried pdo doesnt work with this :

PHP Code

```
<?php
```

```
$stmt = $db->query('SELECT * FROM torrents WHERE title LIKE "%' . mysqli_escape_string($torrent).'%");
```

it displays all the rows

Don't mix mysqli and pdo

PHP Code

```
<?php
```

```
$stmt = $db->prepare('SELECT * FROM torrents WHERE title LIKE ?');
```

```
$db->execute(array('%'.$torrent.'%'));
```

```
var_dump($db->fetch());
```

What do you get with this?

deadsh0t - November 9, 2018, 6:44 am

(Nov 9, 2018 07:41 AM)Exp500 Wrote: [\[CITE\]](#) Don't mix mysqli and pdo

PHP Code

```
<?php
```

```
$stmt = $db->prepare('SELECT * FROM torrents WHERE title LIKE ?');
```

```
$db->execute(array('%'.$torrent.'%'));
```

```
var_dump($db->fetch());
```

What do you get with this?

that shows nothing 0 rows

TCP - November 9, 2018, 6:46 am

(Nov 9, 2018 07:44 AM)deadsh0t Wrote: [\[CITE\]](#) that shows nothing 0 rows
Can you show us the torrents table and the value of torrent?

FoxBlood - November 9, 2018, 6:50 am

(Nov 9, 2018 07:04 AM)deadsh0t Wrote: [\[CITE\]](#) The post variable is fine because i echo it and it displays i dont use pdo cause i never used it before but i might consider using it .

If i remove the where clause it puts out every row but as soon as i put the where clause there and type a letter or even the identical title of 1 of the rows it still displays nothing and the row count is 0

tried pdo doesnt work with this :

PHP Code

```
<?php
```

```
$stmt = $db->query('SELECT * FROM torrents WHERE title LIKE "%' . mysqli_escape_string($torrent).%"');
```

it displays all the rows

what? use pdo and prepare statement like this:

PHP Code

```
<?php
```

```
$payload = array(":title" => $title);
```

```
$stmt = $db->prepare("SELECT * FROM torrents WHERE title LIKE '%:title%' ");
```

```
// :title will be replace in execution using your payload
```

```
$stmt->execute($payload);
```

```
foreach($stmt as $row)
```

```
{
```

```
    // your stuff here, $row['title'] to get the title
```

```
}
```

deadsh0t - November 9, 2018, 6:52 am

(Nov 9, 2018 07:46 AM)Exp500 Wrote: [\[CITE\]](#) Can you show us the torrents table and the value of torrent?

PHP Code

```
<?php
```

```
$torrent = $_POST['torrent'];
```

TCP - November 9, 2018, 6:54 am

(Nov 9, 2018 07:52 AM)deadsh0t Wrote: [\[CITE\]](#) PHP Code

```
<?php
```

```
$torrent = $_POST['torrent'];
```

The value of rows and \$torrent var? Did you initialize PDO correctly?

deadsh0t - November 9, 2018, 6:59 am

i initialised the PDO like this:

PHP Code

```
<?php
```

```
$db = new PDO('mysql:host=localhost;dbname=torrents;charset=utf8mb4','user', 'password');
```

\$torrent var get the post value torrent wich is the name of a text input on a form on the index page that looks like this:

PHP Code

```
<?php
<form method="post" action="search.php">
    <input type="text" placeholder="Search for Torrents" name="torrent">
    <button name="submit" type="submit" value="Search"><i class="fa fa-search"></i></button>
</form>
```

UPDATE:

So i got it to work using mysqli by using this :

PHP Code

```
<?php
$sql1 = "SELECT ID,title,magnet,date FROM torrents WHERE title LIKE '%" . $conn->
real_escape_string($torrent)."%";
```

however i would still like to know how to get it to work in PDO

Squito - November 9, 2018, 9:56 am

UTF8 queries executed on latin1 fields?

Here's an example of using MySQLi prepared statement:

PHP Code

```
<?PHP
$conn=mysqli_connect("localhost", "username", "password", "database");
$prep=mysqli_stmt_init($conn);
$search="%" . $_POST['torrent'] . "%";
mysqli_stmt_prepare($prep, "SELECT ID, title, magnet, date FROM torrents WHERE title LIKE ?");
mysqli_stmt_bind_param($prep, "s", $search);
mysqli_stmt_execute($prep);
mysqli_stmt_store_result($prep);
if(mysqli_stmt_num_rows($prep)!=0)
{
    mysqli_stmt_bind_result($prep, $id, $title, $magnet, $date);
    while(mysqli_stmt_fetch($prep))
    {
        echo '<a href="'. $magnet. "'>'. $title. '</a><br>';
    }
}
mysqli_stmt_close($prep);
```