

Forum:[Hack Forums](#)

Thread: [\[TuT\] Extremely easy SQL injection prevention, PHP](#)

ChineseFountain - February 17, 2010, 5:45 pm

How to protect your forms from SQL injection!

We all know it's fun to hack and deface websites. But how would you feel if it happened to you? So, here is an easy tutorial to prevent your website from being SQLi'd.

Here is the code for a vulnerable form:

PHP Code

```
<?php
```

```
include "conn.php"; //connect to database
$username = $_POST['username'];
$password = $_POST['password'];
$sql = "INSERT INTO users (username, password) VALUES ('$username', '$password')";
mysql_query($sql);
echo "User registered";
?>
```

Anyone could inject that.

But, we can make a simple adjustment to fix that up! Use this code instead!

PHP Code

```
<?php
```

```
include "conn.php"; //connect to database
$username = $_POST['username'];
$username = mysql_real_escape_string($username);
$password = $_POST['password'];
$password = mysql_real_escape_string($password);
$password = md5($password);
$sql = "INSERT INTO users (username, password) VALUES ('$username', '$password')";
mysql_query($sql);
echo "User registered";
?>
```

As you can see, I've added the function `mysql_real_escape_string()`; to the `$username` and `$password` variables. It's that simple! I've also md5'd the password, since it was all lonely and unencrypted out there. :D That was for an example, I recommend using a salt so you can't just take that hash to a decoder and decode the md5.

Thanks for reading this fairly short tutorial!

OX!DE - February 17, 2010, 5:56 pm

PHP Code

```
<?php
function cleanstring($query){
if(get_magic_quotes_gpc()){ $string = stripslashes($query);}
if (phpversion() >= '4.3.0'){ $query = mysql_real_escape_string($query);
}else{
$string = mysql_escape_string($string); }
return $string;
}
```

-mothered- - February 17, 2010, 6:11 pm

Looks good mate. Will definitely check it out.
Thanks for the share :)

ChineseFountain - February 17, 2010, 7:58 pm

(Feb 17, 2010 06:56 PM)OX!DE Wrote: [\[CITE\]](#) PHP Code

```
<?php
function cleanstring($query){
if(get_magic_quotes_gpc()){ $string = stripslashes($query);}
if (phpversion() >= '4.3.0'){ $query = mysql_real_escape_string($query);
}else{
$string = mysql_escape_string($string); }
return $string;
}
```

I was trying to keep it simple.

If you look at the title: Extremely easy SQL injection prevention, PHP.

OX!DE - February 18, 2010, 2:48 am

How is that not extremely easy.

PHP Code

```
<?php
"WHERE ID = " . cleanstring($query) . "";
```

ChineseFountain - February 18, 2010, 8:15 pm

(Feb 18, 2010 03:48 AM)OX!DE Wrote: [\[CITE\]](#) How is that not extremely easy.

PHP Code

```
<?php
"WHERE ID = " . cleanstring($query) . "";
```

Well, I mean mysql_real_escape_string(); is more widely known and used, and in many people's eyes, easier to remember.

steven44 - February 17, 2011, 12:33 am

where would this code be added.?

see my forum was hacked the other day i now get a 404 forbidden response when trying to access
i contacted my hosting server there response was this ;

Your PHP coding is/was causing severe disruption on the servers and our security measures automatically kicked in to prevent further disruption which is for the benefit of all of our customers. It appears that a number of instances of PHP scripts running on the server are not closing properly, and are left hanging on the server. I've pasted the scripts and the number of instances below- forumdisplay.php (89), index.php (1), infernoshout.php (2), misc.php (4), search.php (78), showthread.php (158)

Please check your PHP code and ensure that your scripts close properly after they have finished executing.

Once you have done this please confirm and we will reactivate scripting on the server for you.

this is caused by sql injection right or is it caused by somethink else?

i was using vbulletin 3.8.6 patch 1

thanks in advance for your time and hope to successfully secure my site with your help

cheers steven

iBones - February 17, 2011, 1:10 am

@Steven, was it nulled vB? The nulner probably has some sort of shit going on in there, if so.

steven44 - February 17, 2011, 1:38 am

It was but it was vb 3.8.6 so im thinking maybe vunrabilities '

would the nulner wait nearly 5 weeks before messing the forum up ? seems abit bad tht if its the case

i did varlfy the forums files before install and all was ok .

maybe some ppl have a vendetta against me . or wel time wil tel

what would you suggest , also where would this code be added ?

thanks in advance steven

Uncomplicated - February 17, 2011, 2:04 am

If it's vB, it shouldn't be prone to sql injections. The script might be backdoored. Please use a freeware alternative or buy vB license.

steven44 - February 17, 2011, 2:19 am

it isnt backdoord (wel i hope its not ffs) i was targeted . the person thretened tht if i ban them the site would be coming down and should you no it soon after it was . and that was the responce given from the host provider shown in previous post.if it isnt sql injection then its ddos there must be precaution or ways of better securing a forum from these attacks unless there out there and i cant find them

if i upgraded the forum would that help or is it a case of converting vb to mybb would scripts and plugins work the same in mybb also

thanks in advance

iBones - February 17, 2011, 1:40 pm

(Feb 17, 2011 03:19 AM)steven44 Wrote: [\[CITE\]](#) the person thretened tht if i ban them the site would be coming down

So why didn't you give their IP to the police? Threats like that are illegal.

ChineseFountain - *February 19, 2011, 10:10 am*

Gawd thanks for ub3r p..

1 year much.

If you were hacked by a SQL injection vulnerability then you need to find a patch for that. It would especially help if you knew what form they injected through.