

Forum:[Hack Forums](#)

Thread: [htmlspecialchars\(\) tutorial for beginners ~\[Step by Step | Pictures\]~](#)

~[DogiD]~ - December 24, 2012, 4:06 am

Here is my tutorial how to setup [htmlspecialchars\(\)](#) and protect your site to xss vulnerability.

If you didn't know what XSS vulnerability is then i recommend you read this tutorial first,
<https://hackforums.net/showthread.php?tid=2910051>

What you need, before you start read tutorial?Website or other think to run php files (ex. XAMPP)

Notepad++ or other program to edit php files.

Steps,

First make 2 php file, "index.php" and "without.php".

Open "index.php" and build simple form page. Like this,

Spoiler [\(Click to View\)](#)

When "index.php" is ready, open "without.php" file and make it looks like this,

Spoiler [\(Click to View\)](#)

Code `<?php echo 'You type: ' . $_POST["without"]; ?>`

Now when you type something in "index.php" its send it to "without.php" page. So if i type in textbox script,

Code `<script>alert(1)</script>`

Then i press send..

Spoiler [\(Click to View\)](#)

Now we just need add htmlspecialchars() function in "without.php" file,

Spoiler [\(Click to View\)](#)

Code `echo 'You type: ' . htmlspecialchars( $_POST["without"] );`

Lets try again, what happen if i try send same script,

Spoiler [\(Click to View\)](#)

Now htmlspecialchars() function change all <, > etc to html code and xss vulnerability is fixed.

Congratulations! ?

Hope this tutorial help you understand how to use htmlspecialchars() function,

Good luck and have fun!

~ DogiD?

LevelUp - December 24, 2012, 4:18 am

Very nice tutorial, well explained mate.

redpois0n - December 24, 2012, 4:40 am

thank you for this! Well explained and confirmed what I knew :)

Using this for my site

~**[DogiD]**~ - December 24, 2012, 8:34 am

(Dec 24, 2012 05:40 AM)redpois0n Wrote: [\[CITE\]](#) thank you for this! Well explained and confirmed what I knew :)

Using this for my site

Good to hear ;)

Thank you,

~ DogiD?

illi L???Y illi - December 24, 2012, 8:57 am

Have learned a good thing. Thanks for the share.

what else? - December 24, 2012, 9:15 am

You forgot to mention htmlspecialchars is only used while parsing the content.

Do not use htmlspecialchars then save a content to a db then parse it.

GambleSickness - December 24, 2012, 9:50 am

woow very good and detailed tutorial , many have knowledge leak when it comes to these stuff ...

alexlandonflicksss - December 24, 2012, 7:20 pm

Nice tut....it will be better...if this was a video...

Volim te - December 24, 2012, 7:23 pm

I use htmlentities() myself but great tut anyway.

VoidEx. - December 24, 2012, 7:27 pm

(Dec 24, 2012 10:15 AM)what else? Wrote: [\[CITE\]](#) You forgot to mention htmlspecialchars is only used while parsing the content.

Do not use htmlspecialchars then save a content to a db then parse it.

Yes this exactly.

However I myself do use htmlspecialchars when saving to db for certain things, such as usernames for my website. This is fine. Otherwise, parse on output is the recommended practice.

(Dec 24, 2012 08:23 PM)Jebi se Wrote: [\[CITE\]](#) I use htmlentities() myself but great tut anyway.

If you allow certain tags with htmlentities(), eg , ensure that you are aware of the fact that people can still execute scripts.

Eg:

<b onload='alert(1)'\>

To the OP:

Well done and thanks for the tutorial :) This should help a lot of people secure their websites.

KernelMode - December 24, 2012, 7:30 pm

Why make this thread? You can just look at php's site.
<http://php.net/manual/en/function.htmlspecialchars.php>

Volim te - December 24, 2012, 7:32 pm

(Dec 24, 2012 08:27 PM)?ne™ Wrote: [\[CITE\]](#) Yes this exactly.

However I myself do use htmlspecialchars when saving to db for certain things, such as usernames for my website. This is fine. Otherwise, parse on output is the recommended practice.

If you allow certain tags with htmlentities(), eg , ensure that you are aware of the fact that people can still execute scripts.

Eg:

<b onload='alert(1)'>

To the OP:

Well done and thanks for the tutorial :) This should help a lot of people secure their websites. I mostly add a number is `disallowed` words like javascript, onload, onerror, document.cookie etc.

PigBacon - December 24, 2012, 8:29 pm

(Dec 24, 2012 08:27 PM)?ne™ Wrote: [\[CITE\]](#) However I myself do use htmlspecialchars when saving to db for certain things, such as usernames for my website. This is fine. Otherwise, parse on output is the recommended practice.

You know why its the recommended practice?

Because it makes sense.

You should never store escaped data, I mean, what if you want to export it to a CSV file, you'll have HTML escapes all over.

RebornX - December 24, 2012, 8:35 pm

On the 5th step the image should say "With htmlspecialchars()" i think.

Nice tutorial though :)

badbrains - December 24, 2012, 9:03 pm

.. You made a tutorial for a DOCUMENTED function?

.. Why?

<http://php.net/htmlspecialchars>

~[DogiD]~ - December 25, 2012, 2:50 am

(Dec 24, 2012 10:03 PM)PeopleUnderTheStairs Wrote: [\[CITE\]](#) .. You made a tutorial for a DOCUMENTED function?

.. Why?

<http://php.net/htmlspecialchars>

Just because i can ?

~ DogiD?

hebrew878 - December 27, 2012, 9:30 am

how about this ? htmlentities(\$_POST['anything'], ENT_QUOTES, 'UTF-8');