
SOLVED! (Adding underscores)_link_ and _layer_

Posted by Balador - 2007/09/06 12:26

When I type the word link or layer on my forum it gets changed to _link_ and _layer_ for some reason, any ideas? Also, on my dark template, when I edit a post you have the edit reason box, the text "reason for editing" is black on black. Forum can be found here: www.paradiselost.nl

Re: _link_ and _layer_

Posted by zammbi - 2007/09/06 12:32

Same with the word script on my forum.

Re: _link_ and _layer_

Posted by danialt - 2007/09/06 13:28

This was to quickly avoid XSS attacks but I guess I made it a bit rigorous. You can reduce the elements by editing `class.fireboard.php`

Re: _link_ and _layer_

Posted by Balador - 2007/09/06 15:27

Ok, found the line with these words, thanks for your help! Any ideas on the dark template problem with the edit reason box?

Re: link_ and _layer_

Posted by birdie60 - 2007/09/06 19:32

Hmm. I do not know what a CSS attack is, but I know that the current behaviour makes many problems for my users.

What do you suggest as best method to get rid of the change of :blink: and words like uplink or unlinkable? Its kind of a mess now...

Re: _link_ and _layer_

Posted by danialt - 2007/09/06 20:42

XSS attack sorry.

As I said, edit `class.fireboard.php` and remove the elements you dont want. search for "script".

Re: _link_ and _layer_

Posted by birdie60 - 2007/09/06 20:55

No, `_script_` is not found, without underscores yes.

I could live with the replacements, if it would not occur in the middle of a word, like `un_link_able`. Is there maybe a way to restrict replacements to whole words only? Would that be more secure than to just delete some words from the list in the

mentioned class.fireboard.php?

I am no programmer; I just want to understand the effects of patching files in a production system.

=====

Re: link and layer

Posted by birdie60 - 2007/09/06 22:55

Then another thing here. I noticed that the addition of underscores to the dangerous words takes place, even if the underscores were added before!

This, for instance, could happen if a message containing some of these words was edited. In the end you have
link.

The algorithm should be more specific and test of really dangerous conditions and leave the words alone in other situations, imho.

=====

Re: link and layer

Posted by danialt - 2007/09/07 08:40

you can delete the first line as a whole. leave the second line.

=====

Re: link and layer

Posted by birdie60 - 2007/09/07 23:54

Thats what I did, and it works well for the user.
I'm just not sure if I am now vulnerable to this XSS attack thing!

=====

Re: link and layer

Posted by skyxliner - 2007/09/08 02:19

the word description changes to "de_script_ion"

but i couldn't find it in the same list as link and layer

i found `var $description = null;`

but removing it doesn't do anything

=====

Re: link and layer

Posted by danialt - 2007/09/08 10:28

Just delete the first line. second line must stay as whole.

=====

Re: link and layer

Posted by druckgott - 2007/09/08 10:35

there is the solution, look: class.fireboard.php
Linie around 651 entferne: 'link' und '_blink_' and so on you want to delete

Re: link and layer

Posted by greendino - 2007/09/08 23:26

Quick solution for this;

class.fireboard.php

Found :

```
// now the only remaining whitespace attacks are \t, \n, and \r
```

```
$ra1 = Array('javascript', 'vbscript', 'expression', 'applet', 'meta', 'blink', 'style', 'script', 'embed', 'object', 'iframe',  
'frame', 'frameset', 'ilayer', 'layer', 'bgsound');
```

Replace

```
// now the only remaining whitespace attacks are \t, \n, and \r
```

```
$ra1 = Array('javascript');
```

Re: link and layer

Posted by Ratman - 2007/09/09 00:21

Quick solution works fine for me, but doesn't this open some security holes?

Re: link and layer

Posted by peetree21 - 2007/09/12 13:03

ok i have removed the common words like link, title etc as these were mucking up my site's forum and now works fine.
thanks for the prompt fix

however like the person above asked, is this now at risk to security issues?

Re: link and layer

Posted by birdie60 - 2007/09/12 13:07

I guess we won't get a direct answer from the developers to this security question. Who want's to tell the world about the security holes in his software?

Re: link and layer

Posted by shapeshifta - 2007/09/12 14:41

hey ho, danialt already replied to your question.
Without replacing of all these words your Forum may be vulnerable to Cross Site Scripting.
Someone could inject javascript or flash or whatever into your site and collect passwords for example.

I don't think it is the best solution, but one that should work for now.
If you do not like it, delete it, but do not blame the developers if your site gets hacked.

Just my two cents...

=====

Re: link and layer

Posted by cosworth - 2007/09/14 09:00

I replaced
function fbReturnDashed (&\$string, \$key) {
 \$string = "_" . \$string . "_";
}
with
function fbReturnDashed (&\$string, \$key) {
 \$string = "-" . \$string . "-";
}in class.fireboard.php

The soft hyphen is less obtrusive than the underscore. The security is unchanged by this (so I hope at least)

=====

Re: link and layer

Posted by freedom - 2007/09/14 22:51

Thanks, cosworth! Your variant has helped many Russian users which use me the Russified version FireBoard 1.0.3

=====

Re: link and layer

Posted by dartagnan32 - 2007/09/16 17:45

You are talking about a soft hyphen, but it seems you put nothing in your "" quotes...
Is that a typo?
thanks

=====

Re: link and layer

Posted by cosworth - 2007/09/16 19:27

The soft hyphen was removed when I posted the thing. It should have been ampersand+"shy;"
It works nicely because the it doesn't create a space or any other visible distance between the letters.

=====

Re: link and layer

Posted by birdie60 - 2007/09/17 09:40

Be aware though, that search results may not be what the searcher expected. All words that contain the bad words will not be found any more, due to the hidden shy symbols.

=====

Re: link and layer

Posted by Scotsgait - 2007/09/17 16:52

I've just tried the soft hyphen solution without success :angry:

I just did a straight substitute of "@shy" (using "&", not "@ !") for "_" in the code - but all I got was P­-layer­

Any idea what's wrong ?

=====

Re: link and layer

Posted by cosworth - 2007/09/17 17:58

Missing a ";" ?

=====

Re: link and layer

Posted by Scotsgait - 2007/09/17 18:08

cosworth wrote:

Missing a ";" ?

:blush:

Yes !

=====

Re: link and layer

Posted by florut - 2007/09/18 13:45

The soft hyphen (& s h y ;) solution is really great !! Thanks for it !

However, this way the smiley : b l i n k : is not converted into his image... the : b l i n k : text remains.

If you find a way to fix it without removing the l i n k and b l i n k strings into the fbRemoveXSS function please tell !

maybe the best solution is to rename the tag : b l i n k : for the smiley ??

By the way how is coded on bestofjoomla forums ? The smiley :blink: works !! So how ?

=====

Re: link and layer

Posted by .WiRED - 2007/09/24 07:35

Let me do the honor :P

Thanks for this mate!! Worked 100% to remove the stupid link..

I hope Fireboard fixes this in the next release!!

=====

Re: link and layer

Posted by traveller - 2007/09/24 22:01

Worked for me too

Thanks

=====

Re: link and layer

Posted by magickz - 2007/09/25 08:47

Works well. just, if I type a word like "Link" with a capital letter in the beginning it will be also translated to a lower-case letter. Is there a way to avoid it?

=====

Re: link and layer

Posted by bky - 2007/09/26 04:18

I replaced the with a zero-width joiner (‍); it still breaks the search (I think) but visually it looks right and should have the same effect.

Why hasn't there been a more robust fix for this? And can we assume that this forum has the protection off, or is there some security/usability fix it's running that hasn't been mentioned?

=====

Re: link and layer

Posted by birdie60 - 2007/09/26 10:53

A good solution should take into account that words (like link, layer, etc) are bad only, if there is no white space, punctuation or special characters (like ampersand, asterisk, apostrophes, ellipses, etc) on the left or the right of the word. I could live with a - around bad words that are not part of a bigger word (like link in blink).

BTW: Those with the shy solution: Are you absolutely sure, that these shy character are not simply ignored by the javascript interpreter?

birdie60

=====

Re: link and layer

Posted by Vimes - 2007/10/05 04:04

Many Thanks for this fix - sorted! I'll watch this thread with interest

=====

Re: link and layer

Posted by curt - 2007/10/07 16:35

danialt,

I removed potentially valid words that can be entered by users, such as "base", "blink", "link", "object", "style", "frame", "layer", "title".

Is this going to open my Fireboard to XSS attacks? This seems like a conundrum. How do we allow users to enter valid English words and still prevent XSS attacks?

=====

Re: link and layer

Posted by bpresent - 2007/10/14 04:29

I can live with the work around - humans are pretty good at working out what's meant to be there.

My problem is that I've put in some "url" strings and they are being changed and therefore broken.

By the way - it's worth point out that the underscores are not stored in the database so when "we" find a fix to this all will be well.... :)

=====

Re: link and layer

Posted by kaeau - 2007/10/15 22:32

well, had the same problem with a fresh install..
now (as a non expert in security stuff and programming), im not sure what to do:
remove the scripts 1st line?.. do nothing?

it would be wonderful if someone could post any solution, which enables users to actually write words (like: multip_layer_ , for example..) without underscores..

please:)

cheers

ka

www.ninc.at

www.nnw.at

=====

Re: link and layer

Posted by grumblemarc - 2007/10/15 22:37

There were a couple of solutions posted in this thread. Did you try any of them?

=====

Re: link and layer

Posted by kaeau - 2007/10/16 00:13

no, because there was no distinct answer, if those solutions are dangerous (because of those xss attacks) or not..
nice greetings!

ka

www.ninc.at

=====

Re: link and layer

Posted by grumblemarc - 2007/10/16 00:20

Yes they are dangerous. You put your site at risk because you are in effect circumventing (overly aggressive) security

measures. Until this bug is worked out in future releases there has only been these workarounds presented.

=====

Re: link_ and layer_
Posted by bpresent - 2007/10/16 00:32

The work arounds (for what is in effect a work around itself) work fine thanks.

=====

Re: link_ and layer_
Posted by zottaro - 2007/10/17 13:30

1000 thanks, to all, for this topic!!

=====

Re: link_ and layer_
Posted by Philip Roy - 2007/10/17 13:36

Is there any chance someone could attach a file with the changes...I'm slightly confused as there seems to be multiple workarounds (plural) so I've kinda been sitting here waiting for the dust to clear and an agreed fix to show up.....but if there's just one example file, that would be great.

Cheers,

Phil

=====

Re: link_ and layer_
Posted by bpresent - 2007/10/17 15:20

The suggested fixes are all the same - just slight variations of your choosing to suit your desired balance of appearance versus security.

The fix ranges from the deletion of entire line of code (line 651 in the 1.0.3 stable version) or selected words.

I deleted the words 'script' and 'link'.

The line (unaltered) looks like this:

```
$ra1 = Array('javascript', 'vbscript', 'expression', 'applet', 'meta', 'xml', 'blink', 'link', 'style', 'script', 'embed', 'object', 'iframe', 'frame', 'frameset', 'ilayer', 'layer', 'bgsound', 'title', 'base');
```

(and I should probably now remove my signature ;))

=====

Re: link_ and layer_
Posted by guilleva - 2007/10/27 00:37

I'm wondering why don't escape the output text with htmlentities()?

Doesn't that avoid XSS at 100%?

I think it is safer than the current solution on fireboard. I did it on my forum and it works great! And also it fixes other issue when a post wrings ampersand+lang like this "&lang=es"?

=====

Re: link and layer

Posted by bpresent - 2007/10/27 05:05

Can you be more specific please - what code did you use?

Re: link and layer

Posted by guilleva - 2007/10/27 05:17

On file components/com_fireboard/template/default/smile.class.php

Replace:

```
$fb_message_txt = FBTools::fbRemoveXSS($fb_message_txt);
```

With:

```
$fb_message_txt = htmlentities($fb_message_txt);
```

And delete the line:

```
$after_replace = FBTools::fbRemoveXSS($after_replace, 1);
```

But my question is, why fireboard doesn't use htmlentities or strip_tags or htmlspecialchars to avoid this? Is there any reason why this should not be done?

Re: link and layer

Posted by helo - 2007/11/07 23:00

thank god.

Re: link and layer

Posted by whiskymac - 2007/11/16 18:47

guilleva wrote:

On file components/com_fireboard/template/default/smile.class.php

Replace:

```
$fb_message_txt = FBTools::fbRemoveXSS($fb_message_txt);
```

With:

```
$fb_message_txt = htmlentities($fb_message_txt);
```

And delete the line:

```
$after_replace = FBTools::fbRemoveXSS($after_replace, 1);
```

But my question is, why fireboard doesn't use htmlentities or strip_tags or htmlspecialchars to avoid this? Is there any reason why this should not be done?

I've just done this change on my forum as I assume its safer than the other workaround? anyway, it seems to work fine

for me, *but* it seems to do something to forum signatures. Instead of my signature displaying the "£" symbol it has changed to the html code instead "£".

Does anyone know how I can correct this?

Thanks

=====

Re: link_ and _layer_

Posted by florut - 2007/11/16 18:54

guilleva wrote:

On file components/com_fireboard/template/default/smile.class.php

Replace:

```
$fb_message_txt = FBTools::fbRemoveXSS($fb_message_txt);
```

With:

```
$fb_message_txt = htmlentities($fb_message_txt);
```

And delete the line:

```
$after_replace = FBTools::fbRemoveXSS($after_replace, 1);
```

But my question is, why fireboard doesn't use htmlentities or strip_tags or htmlspecialchars to avoid this? Is there any reason why this should not be done?

Are you really sure that htmlentities is never applied before to the message text ????. Isn't it the basics of XSS security ????

=====

Re: link_ and _layer_

Posted by linker3000 - 2007/11/19 23:01

Any chance this topic could be FAQd or somehow stickied as it's quite a common problem.

Thanks

=====

Re:(Adding underscores)link_ and _layer_

Posted by grumblemarc - 2007/11/19 23:07

Umm. It IS stickied. Has been for quite some time.

=====

Re: link_ and _layer_

Posted by Ritter - 2007/11/28 20:08

I love Fireboard, and with every release I get excited about how its getting better and better. However, it boggles my mind that this "solution" of adding underscores was the method picked and determined to solve XSS vulnerabilities.

I know this is developed by people on their free time, but please, I'm begging you, think about problems or even ask for

peoples opinions before making rash implementations to solve a "might exist" problem with a "guaranteed going to break certain common language words" solution.

I'm not trying to be a troll, I really am happy with Fireboard as a whole. I just get worried about its stability when instances like these show themselves.

Thank you guilleval! For your time and efforts toward a much more sensible solution.

=====

Re: link and layer

Posted by Ritter - 2007/11/28 21:55

I am having an issue where messages that have already encoded html entities are getting encoded again.. I'll reply when I have a fix.

Ok, simple fix,.. convert the & to something that wont get encoded and then back.

```
In smile.class.php // $fb_message_txt = FBTools::fbRemoveXSS($fb_message_txt);
    $fb_message_txt = str_ireplace( '&', ':amp:', $fb_message_txt );
    $fb_message_txt = htmlentities($fb_message_txt);
    $fb_message_txt = str_ireplace( ':amp:', '&', $fb_message_txt );
```

Or a one-liner: `// $fb_message_txt = FBTools::fbRemoveXSS($fb_message_txt);
 $fb_message_txt = str_ireplace(':amp:', '&', htmlentities(str_ireplace('&', ':amp:', $fb_message_txt)));`

=====

Re: link and layer

Posted by Lixypoo - 2008/01/21 02:59

I sincerely appologize for the necromancy here, but I am brand new to Fireboard and Joomla. I am having the same problems on my forums. I know which file I have to change, and what I need to change within that file. My problem here is that using the little Fireboard Control Panel, I can't seem to access the file that is currently uploaded. It seems that the only option would be to completely uninstall the forums, then reinstall them with the edited file. Having never worked with a program like this, I don't feel comfortable doing this. I'm not gonna lie, I'm pretty much a noob when it comes to this stuff. Is there anyway to update just that file? I'm not sure if the backend I see is the same that everybody else see's or not. (Like I said, Noob) Any help here would be much appreciated.

-LiX

=====

Re: SOLVED! (Adding underscores) link and layer

Posted by topolivan - 2008/04/28 17:19

My php codes are also hidden, so no code is shown.

How can I solve that?

=====