

Forum:[Hack Forums](#)

Thread: [\[Tutorial\] Shelling a 3.x.x PHPBB Forum \[Pics/Detailed\]](#)

-DownFall - January 6, 2012, 9:52 pm

So today I'm going to be showing you how to shell a phpbb 3.x.x forum.

Once you have administrator access, go to your forum and login.
Now go down once you get redirected all the way to the forum.

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

As you can see, if your account has administrator access, you can view the link to the admin panel.

It'll come up with another login.

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

It should look something like this.

Code `http://site.com/adm/index.php`

You should now be successfully logged in.
Here's what the admin panel looks like.

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

On the settings tab, scroll down to security settings.

It looks like this.

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

Now scroll down to Allow php in templates.
Make sure this option is checked to YES.

Now go to the styles tab.
Under Style Components, click Templates.

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

Now it shows the installed templates. Click edit on the top one.

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

Now under select template, choose `faq_body.html`.

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

It should take you to the template edit screen.

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

Copy everything on here, and paste it in notepad and save it as backup.txt.

Now delete everything on the page, and see if you can execute some commands to get the php info displayed.

Code [b]<!--[/b] PHP -->

phpinfo();

[b]<!--[/b] ENDPHP -->

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

Hit submit.

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

Code Information

Template file updated successfully.

« Back to previous page

Now go to your sites FAQ page.

Code `http://www.site.com/faq.php`

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

Now we know we can execute remote commands. Now we can spawn our shell on there.

Go back to where you edited the file, and replace a `phpinfo();` with your shell code.

You can use this one.

[PHPBB Shell](#)

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

Now go to your sites FAQ page again. Your shell will be on there.

Now use the uploader on that shell, and upload another one of your choide.

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

Now go back to where you put your shell code, open up backup.txt, and put the default code back in.

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

Then go back to your site, and the default FAQ page will be on there.

Now to remove suspicion, go back to the security settings on the general tab and set Allow php in templates to no.

Now click submit.

Code Information

Configuration updated successfully.

Now we want to be sneaky, and delete all our dirty work off the admin log.
Spoiler ([Click to View](#))

Check everything you did, scroll down and go to delete checked.
Then confirm it.

Now you can go to your shell and do what you want!

Shoutout to Hooded Robin and the rest of Zer0Lulz, for the idea and hash cracking!

Let me know if you have any questions.

-DownFall

.bLaZeD - January 6, 2012, 10:05 pm

Great tutorial. Will definatly bookmark this. :D

-zerocool - January 6, 2012, 10:28 pm

Nice tutorial bro.Bookmarked for future reference <3

??????? - January 6, 2012, 10:37 pm

but i know this way from 2009 its old for me

but thanks

Hooded Robin - January 7, 2012, 12:59 am

This may be old but not so well documented. Glad you were able to make it all work finally and great job on capturing all the details in an easy to follow tutorial. Keep up the great work!

-DownFall - January 7, 2012, 6:17 am

(Jan 6, 2012 11:37 PM)? ? ? ? ? Wrote: ([CITE](#)) but i know this way from 2009 its old for me

but thanks

As Hooded Robin said, you won't find one that explains everything how mine does. Thanks for the feedback!

Numinous - January 7, 2012, 6:21 am

yea bro that's the best way which u described here ..

gud luck ..

CR33T3N - January 7, 2012, 7:00 am

Nice tutorial, did it in a little other way then I did.

Just wanna mention that I did a Tutorial covering that too, yours is better tho imo. (For people interested: <https://hackforums.net/showthread.php?tid=2031654>)

But you could basically use any shell, you just need to change <?php and ?> in "<!-- PHP -->" and "<!-- ENDPHP -->"

So that phpbb recognizes it.

Offtopic: Are you still on Skype? havent seen you there for some time :D

kakker - January 7, 2012, 7:04 am

GREAT tut , once again :) learned a lot of you , keep up the good work!!! :)

-DownFall - January 7, 2012, 7:09 am

(Jan 7, 2012 08:00 AM)CR33T3N Wrote: [\[CITE\]](#) Nice tutorial, did it in a little other way then I did.

Just wanna mention that I did a Tutorial covering that too, yours is better tho imo. (For people interested: <https://hackforums.net/showthread.php?tid=2031654>)

But you could basically use any shell, you just need to change <?php and ?> in "<!-- PHP -->" and "<!-- ENDPHP -->"

So that phpbb recognizes it.

Offtopic: Are you still on Skype? havent seen you there for some time :D

I kept getting parsing errors the first few times, started to get on my nerves lol.

Im on skype right now if you want to hop on.

Prominent - January 7, 2012, 8:41 am

phpBB, haven't seen tutorials on how to hack it for a while. Very nice tutorial :3

-DownFall - January 7, 2012, 1:49 pm

(Jan 7, 2012 09:41 AM)Prominent Wrote: [\[CITE\]](#) phpBB, haven't seen tutorials on how to hack it for a while. Very nice tutorial :3

Thanks Prominent! Added this to the list in my mega-thread under shells.

Retribute - January 7, 2012, 1:55 pm

Problem here is that it'll say "Admin log cleared" which would spark suspicion, otherwise this is a nice tutorial.

-DownFall - January 7, 2012, 2:01 pm

(Jan 7, 2012 02:55 PM)RubiksHQ Wrote: [\[CITE\]](#) Problem here is that it'll say "Admin log cleared" which would spark suspicion, otherwise this is a nice tutorial.

Thanks, but there's not really much you can do about that :/

Leaves a lot less suspicion then leaving all the rest of the stuff on there though lol.

Retribute - January 7, 2012, 2:09 pm

You should also add a note in the OP that only Admins with Founder status may do this ;)

-DownFall - January 7, 2012, 2:11 pm

(Jan 7, 2012 03:09 PM)RubiksHQ Wrote: [\[CITE\]](#) You should also add a note in the OP that only

Admins with Founder status may do this ;)

Nope, the admin account I used there didn't have founder status.

That's why I was worried before I made the tutorial. For this specific site, there was only 1 user named Administrator who had founder status. I couldn't get the hash cracked, but there were 4 other accounts in the admin group (53 by default I think?). The one I used was one of the 4 that didn't have it.

diodolo - January 7, 2012, 2:13 pm

(Jan 7, 2012 02:55 PM)RubiksHQ Wrote: [\[CITE\]](#) Problem here is that it'll say "Admin log cleared" which would spark suspicion, otherwise this is a nice tutorial. With a shell, you can access to database and delete record from phpbb_log. So all traces are deleted.

Retribute - January 7, 2012, 2:16 pm

(Jan 7, 2012 03:11 PM)-DownFall Wrote: [\[CITE\]](#) Nope, the admin account I used there didn't have founder status.

That's why I was worried before I made the tutorial. For this specific site, there was only 1 user named Administrator who had founder status. I couldn't get the hash cracked, but there were 4 other accounts in the admin group (53 by default I think?). The one I used was one of the 4 that didn't have it.

Really? Last time I checked, non-founders couldn't access the Styles tab and Security Settings (I tried on one of my forums).

duodolo Wrote: With a shell, you can access to database and delete record from phpbb_log. So all traces are deleted. True...didn't think of that.

-DownFall - January 7, 2012, 2:17 pm

(Jan 7, 2012 03:16 PM)RubiksHQ Wrote: [\[CITE\]](#) Really? Last time I checked, non-founders couldn't access the Styles tab and Security Settings (I tried on one of my forums).

Must be somewhere in your settings...I was worried about being able to log in, but once I saw Administrator Control Panel at the bottom, I knew I was set :3

Thanks for the information though, maybe it's a specific version of PHPBB.

UNKNOWN SKILLS - January 7, 2012, 3:10 pm

downfall all ways post some thing good lol he is smart

-DownFall - January 7, 2012, 3:25 pm

(Jan 7, 2012 04:10 PM)UNKNOWN SKILLS Wrote: [\[CITE\]](#) downfall all ways post some thing good lol he is smart

Thanks bro, it seems like whenever people post something, it barely gets any replies. The requests for hacking subsection is more active then any of the main website/forum hacking section + sql injection subforum, that's a fucking shame. Most of the shit they could do it themselves if they actually took the time to read great threads. Those only people who reply to these threads are the ones willing to learn.

If you want to read up on any other of my threads check the link in my signature, it has a few things. I'm almost done with a paper I'm writing for Error Based Injection, it's something you can open up in notepad real quick and use as a help guide lol.

BeggFoMercy - January 7, 2012, 4:09 pm

Nice tut mate another great tut keep it up

thethatguy - January 7, 2012, 5:08 pm

Very well put together out of the tutorials that are available all lack some information. You have all the steps in place a first timer will manage this.

"Inside" - February 6, 2012, 4:10 pm

Thanks for this I would give you rep if i could. I just used this guide to help me take a site.

-DownFall - February 7, 2012, 8:44 am

(Feb 6, 2012 05:10 PM)"Inside Wrote: [\[CITE\]](#) Thanks for this I would give you rep if i could. I just used this guide to help me take a site.

Congrats on the shell man, thanks for the reply. Now rape the site ?

Rage DDos - February 20, 2012, 11:12 am

you are super smart bro dam nioce tut is the best bro thanks

kamrulahsan06 - February 21, 2012, 11:34 pm

just bookmarked this amazing tutorial...Thanks a looot

Schiz0 - March 13, 2012, 11:35 pm

Oh snap. DO you realize how long ive been looking for this? lmao.. thanks a fucking million bro! I truly owe you.

EliteKane - May 3, 2012, 11:51 am

I'm not trying to troll. Its a good tutorial nonetheless. Although why the hell do we wanna know how to shell a site if we have admin access.... Show us how to deface the site without admin access, much better.

Prime virus - May 3, 2012, 12:11 pm

thank you very much my brother .. for this tutorial <3

keep going ?

-DownFall - May 3, 2012, 12:40 pm

(May 3, 2012 11:51 AM)EliteKane Wrote: [\[CITE\]](#) I'm not trying to troll. Its a good tutorial nonetheless. Although why the hell do we wanna know how to shell a site if we have admin access.... Show us how to deface the site without admin access, much better.

You won't be able to deface anything if you don't get some kind of backdoor or shell on the server. That's the point of this tutorial, go read up on web shells. As for defacing w.o admin access, use another exploit to get a shell up.

HaLFMD5 - May 4, 2012, 11:04 am

yes u forget the first step lol

once u have the administrator access :D

-DownFall - May 4, 2012, 11:31 am

(May 4, 2012 11:04 AM)HaLFMD5 Wrote: [\[CITE\]](#) yes u forget the first step lol

once u have the administrator access :D

Not really, the tutorial is on shelling, not getting admin access.