

Forum:[Hack Forums](#)

Thread: [best way to secure admin pages?](#)

-**"h3l1m@n"** - October 19, 2011, 3:59 pm

I wonder whats the best way to make sure standard users cant get access to Admin panels on a website and such, i've used Sessions before and make it look for 0(Standard user) or 1(Admin) but it feels way to unsecure to be enough to keep someone that wants in out. Does anyone got a better way to do this or sessions the only way to go?

Xch4ng3 - October 19, 2011, 4:00 pm

Don't have it in default locations such as /admin, /administrator etc.

Most of the time people just use admin finders.

Anne - October 19, 2011, 4:01 pm

Yea and change the name of the php script to something like 34SDf64wS. Just make sure you can remember it yourself.

YERANUK - October 19, 2011, 4:04 pm

Make your admins seperate from your users. (in your database)

And like stated above, make sure the directory that leads to the backend does not "admin, administrator,administrate" anything like that. Make it unique as possible.

Also, a simple htaccess may help, that blocks all ip's except the ones you define.

If you have a dynamic IP you can easily make it so it accepts anything like 100.323.22.xx so if it changes you're still valid. Or you can just manually insert your IP each time it changes.

The odds of someone who wants to attack your site with a similar IP up the 3rd level are slim.

pushl %ebp - October 19, 2011, 4:06 pm

1. Like the above users suggested, change the admin scripts name.

2. Make the script die on all admin pages (except the login page). if (!SESSION['admin']) die();

3. Sanitize against SQLi.

4. Make an admin directory that contains 'index.php' in it. Make the index page log and ban the IP that tried to access. You can ban from the real panel, or the full site. You could also make this script just a fake login panel which doesn't do anything but say the details are incorrect.

-**"h3l1m@n"** - October 19, 2011, 4:06 pm

I've done pretty much of all the, synonyms in the DB and such. but are there anything codewise i could use to increase the security?

I use an If statement that looks wether the user is admin or not and the displays either "Admin Panel" or "Your Profile"

this is an example and not the real code ofc

```
If(Admin== 0){
echo "Admin Panel";
else
{
```

```
echo "Your Profile";  
}  
End if
```

Edit: i will take a look at that nu11byte
Thanks for the fast responds by the way

Tate's Daughter - October 19, 2011, 4:32 pm

(Oct 19, 2011 04:06 PM)-"h3l1m@n"- Wrote: [\[CITE\]](#) I've done pretty much of all the, synonyms in the DB and such. but are there anything codewise i could use to increase the security?

I use an If statement that looks wether the user is admin or not and the displays either "Admin Panel" or "Your Profile"

this is an example and not the real code ofc

```
If(Admin== 0){  
echo "Admin Panel";  
else  
{  
echo "Your Profile";  
}  
End if
```

Edit: i will take a look at that nu11byte
Thanks for the fast responds by the way
make sure it isn't easy to SQL inject with OR '1' == '1' or whatever it is that you do.

Xch4ng3 - October 19, 2011, 5:39 pm

Now that the others mentioned it, .HTaccess would be an awesome way to secure it. It'd make sure no other IP but yours can access the login page. Just make sure you update the .htaccess file if your IP changes via cPanel or however your accessing the files.

Anne - October 19, 2011, 5:45 pm

(Oct 19, 2011 04:06 PM)nu11byte Wrote: [\[CITE\]](#) 4. Make an admin directory that contains 'index.php' in it. Make the index page log and ban the IP that tried to access. You can ban from the real panel, or the full site. You could also make this script just a fake login panel which doesn't do anything but say the details are incorrect.

Now this is a great idea! I might do this once I get my website up and running.

Uncomplicated - October 19, 2011, 8:09 pm

I once made an admin panel that allowed access to only such users who had useragent = 'Let me in'. It was also protected by a .htaccess file and login system.

I think that's pretty secure.

Quad - October 20, 2011, 3:02 am

Just an idea here:

1. Username
2. Password
3. Your email

4. Security question/PIN
5. If all of them are correct, go to step 6
6. Send a randomly generated code to the email-address
7. Enter the code on the next login page.

I guess it could work.

Darkvengance - *October 20, 2011, 3:28 am*

On a old site that I had to login the user had to enter their:

+Username

+Password

+A second Password

+Answer a secret question

+IP had to be white-listed

+And they had to enter a randomly generated code that was emailed to them once every 24hrs (using a cron job)

I think it was fairly secure, I never had any breaches in security and I constantly invited people to try to hack it.

Toph Beifong - *October 20, 2011, 1:26 pm*

log all attempts to login, use the above suggested, use good hashes etc, i would suggest that you put a system in the admin panel that recognises ip's so if they are unusual IP's it asks a security question, like facebook.

phreaker - *October 20, 2011, 1:30 pm*

And you can use .htaccess protection with deny from all, allow from IP or password aswell.

(im using both on a site.)

username.txt - *October 20, 2011, 1:59 pm*

I have the admins and mods in the table as normal users, on login I save a session with the username, when I visit a profile the script checks the user privileges and shows data accordingly with a switch statement, the admin panel is separated from the site, so far its been proving to be safe, even had some (failed) SQL injection attempts, so it's all good :)

Miraculous - *October 20, 2011, 4:40 pm*

I had a friend named potatoes that made a PHP script to where if you try to access /admin/ you're prompted for a code, if you enter it successfully you're added to the allow list, if not, you're redirected to gtfo.php