

Forum:[Hack Forums](#)

Thread: [Only allowing admin user types to access admin page](#)

~Rexon - April 27, 2017, 8:33 am

I have to submit some project in tomorrow and I just realised that every logged in user can access the admin page. I have a login table with usertype as a column. What is the best way to do this? Was thinking make a variable in one page then Checking that variable to see if it equals admin. Can't seem to find anything online that can do that so if someone can help id really appreciate it! Thanks

Leroy Jethro Gibbs - April 27, 2017, 8:34 am

So any user can login to the admin panel? Is there a separate panel for basic users?

Kanoplya - April 27, 2017, 8:36 am

Store an additional variable per user as an admin rank.

Then check if user admin rank == 1, then let him access it, else display something.

SIM-3468354 - April 27, 2017, 8:37 am

If your admin page is just a link hanging around somewhere do an if statement before you display to check if the user is an admin and if they are show the link, else if they're a user to not display it.

For the actual page run an if statement to check user type before it loads the content and if they are an admin let them see it, else if they're a user redirect them to a no permissions page.

newQuery - April 27, 2017, 8:37 am

I would create a function as a middleware named "authenticate" with parameter the ID of the user, then retrieve the user in the database and

PHP Code

```
<?php
```

```
if($user -> usertype != 'admin') header('Location: 403.php');
```

And put the function on the top of the pages that requires admin level
Or better make a router and pass the middleware function to it.

~Rexon - April 27, 2017, 8:44 am

Thanks a lot for the fast replies. Much appreciated!

CodeBinary - April 27, 2017, 9:10 am

(Apr 27, 2017 08:37 AM)?TheZdo Wrote: [\[CITE\]](#) I would create a function as a middleware named "authenticate" with parameter the ID of the user, then retrieve the user in the database and

PHP Code

```
<?php
```

```
if($user -> usertype != 'admin') header('Location: 403.php');
```

And put the function on the top of the pages that requires admin level
Or better make a router and pass the middleware function to it.

I would do something similar to this but be sure to add in an exit; or people can use an extension to block redirects and still see the page.

newQuery - April 28, 2017, 2:04 am

(Apr 27, 2017 09:10 AM)Brian OConner Wrote: [\[CITE\]](#) I would do something similar to this but be sure to add in an exit; or people can use an extension to block redirects and still see the page. Indeed, without the die/exit this would be to easily exploitable ?

Rushax - April 28, 2017, 8:09 am

Yup I would create another table in DB for something like isadmin

Have all set to default 0 and if the user is an admin, create a session for isadmin = 1 when user logs in as an admin and use an if statement on the admin page.

Charger - April 28, 2017, 9:27 am

(Apr 28, 2017 09:25 AM)Yani Wrote: [\[CITE\]](#) Wat? You'd just have a COLUMN in your user table for each user.

There's no need for an extra TABLE.

If you think that you'll have less data, because of the 5 extra cells from 5 users compared to 1 row with 2 cells in an admin table, you are correct, but you'll have to do 2 queries to check if somebody is an admin, which is bad programming. A simple way would be a column such as 'rank'. It could be 0 = banned, 1 = logged in| 2 = admin.

OP;

Ideally, for larger permission sets, you'd want to create a table of permissions and then assign those to the user. That's a little overkill for this, however.

SIM-429621 - April 28, 2017, 10:06 am

(Apr 27, 2017 08:33 AM)rexwest999 Wrote: [\[CITE\]](#) I have to submit some project in tomorrow and I just realised that every logged in user can access the admin page. I have a login table with usertype as a column. What is the best way to do this? Was thinking make a variable in one page then checking that variable to see if it equals admin. Can't seem to find anything online that can do that so if someone can help id really appreciate it! Thanks

Most websites do this by checking user ID from the database, you can make all of your admin users have same ID, like "1" and all the other users ID != 1.

Charger - April 28, 2017, 10:07 am

(Apr 28, 2017 10:06 AM)Passenger Wrote: [\[CITE\]](#) Most websites do this by checking user ID from the database, you can make all of your admin users have same ID, like "1" and all the other users ID != 1.

It's not good to hard code data line that. It's better to make it abstract and allow it to be set per user.

Rushax - April 28, 2017, 10:11 am

(Apr 28, 2017 09:25 AM)Yani Wrote: [\[CITE\]](#) Wat? You'd just have a COLUMN in your user table for each user.

There's no need for an extra TABLE.

If you think that you'll have less data, because of the 5 extra cells from 5 users compared to 1 row with 2 cells in an admin table, you are correct, but you'll have to do an extra lookup queries to check if somebody is an admin, which is bad programming. To be honest, having 4 of those 5 cells as null and just 1 as true for being admin could in theory still consume less data, although I'm not sure about how optimizations work under the hood.

Sorry, yeah 1 extra column not table ?

SIM-429621 - April 28, 2017, 10:36 am

(Apr 28, 2017 10:07 AM)Charger Wrote: [\[CITE\]](#) It's not good to hard code data line that. It's better to make it abstract and allow it to be set per user.

All admin users would have ID of 1, and for non admin users he could make an integer variable called userID or something like that and make it increase by 1 every time new user is registered and added to the database, that way he could also know which user was registered first. I didn't think for him to manually enter or create random ID for every new user.

Rushax - April 28, 2017, 10:39 am

(Apr 28, 2017 10:36 AM)Passenger Wrote: [\[CITE\]](#) All admin users would have ID of 1, and for non admin users he could make an integer variable called userID or something like that and make it increase by 1 every time new user is registered and added to the database, that way he could also know which user was registered first. I didn't think for him to manually enter or create random ID for every new user. You would just have a UserID like you said but set it to Auto Increment to allow it to be the primary key.

SIM-429621 - April 28, 2017, 10:51 am

(Apr 28, 2017 10:39 AM)Rushax Wrote: [\[CITE\]](#) You would just have a UserID like you said but set it to Auto Increment to allow it to be the primary key.

Yes I said to auto increment it for non admin users, if we used same function that increments ID's for all users, then there would have to be another column with boolean values true/false that states whether the user is admin. Even though I don't really have much experience with databases I don't see why not set a static ID for admin users with value of 1.

SIM-429621 - April 28, 2017, 11:53 am

(Apr 28, 2017 11:22 AM)Yani Wrote: [\[CITE\]](#) Because there can only be one user with an ID of 1?

What you're proposing makes no sense.

Ehhh, I'm pretty sure you're allowed to make duplicate entries in Database, unless you explicitly specify that you don't want duplicate entries.

Charger - April 28, 2017, 11:56 am

(Apr 28, 2017 11:53 AM)Passenger Wrote: [\[CITE\]](#) Ehhh, I'm pretty sure you're allowed to make duplicate entries in Database, unless you explicitly specify that you don't want duplicate entries.

Pretty simple to just do it as a column man.

SIM-429621 - April 28, 2017, 11:58 am

(Apr 28, 2017 11:56 AM)Charger Wrote: [\[CITE\]](#)

Pretty simple to just do it as a column man.

I was replying to a guy who said there can be only 1 user with an ID of 1.

Charger - April 28, 2017, 11:58 am

(Apr 28, 2017 11:58 AM)Passenger Wrote: [\[CITE\]](#) I was replying to a guy who said there can be only 1 user with an ID of 1.

Oh, shit, my bad.

Quoted the wrong person.

Rushax - April 28, 2017, 12:25 pm

What your thinking more of a UserGroup rather than a UserID.

The way you're saying, would potentially work but then if it had other related tables, using the

UserID as a primary key would not work say if you wanted to find a particular user's OrderID for e.g.

SIM-429621 - April 28, 2017, 12:31 pm

(Apr 28, 2017 12:06 PM)Yani Wrote: [\[CITE\]](#) Ofcourse, but then it's useless to use it as an ID. An ID should be unique. I do not want to explain such basic coding standards.

Should and can't is not the same, so there you go. Case closed.

Nachfolger - April 28, 2017, 12:32 pm

(Apr 28, 2017 12:31 PM)Passenger Wrote: [\[CITE\]](#) Should and can't is not the same, so there you go. Case closed.Truth. But you understand his point atleast, right?

SIM-429621 - April 28, 2017, 12:36 pm

(Apr 28, 2017 12:32 PM)Nachfolger Wrote: [\[CITE\]](#) Truth. But you understand his point atleast, right? Yup.

elunez - April 28, 2017, 1:45 pm

As a full time developer in a mid sized company (anyway we work with MVC) , the right way to do it is via relations. I like the discussion generated by the thread anyway.

Charger showed a perfect example - HOW NOT TO DESIGN OUR DB in a production:

<https://i.imgur.com/zTdfoKX.png> - and this could be sent to /r/programmingHorror, as i can see it stores paypal mails, thats just a horror.

should be :

users_table:

user_id-

user_role->foreign key->reference to(roles, role_id);

roles:

role_id(increment):

role_name(for example: Admin, Moderator, etc)

This will give you CRUD control over your roles, not to mention if @Charger decide after ~n months to bulk change roles or create new instance of roles -> i see pure horror.

You might need a pivot table if you need AneToMany and ManyToMany relations, but this is the right way to do it.

And its 2017, usually in a real project you have middleware / guards (gates,etc) , Authentication + Authorization. Even with a very simple APP, its better to use strict MVC pattern and frameworks, pure php is terrible by design. I never heard of any dev who is writing a full apps with pure php, expect if you are not learning, but the only thing you need to learn is the syntax and some fundamentals, then you MUST jump on MVC if you want to work.