

Forum:[Hack Forums](#)

Thread: [Admin Page To Upload Page](#)

SchSec - April 19, 2017, 4:00 am

Hi HF

Basically I am in process of creating a bootstrap powered Music Site - The goal though i would like to be able to create an admin page protected by a PHP powered login - I would only like this feature right now in the admin panel as this would allow the Artist's to add music to the upload feature of the site which this upload would be put into the automatic random music player of all the files in the folder.

I am going to do my own research into this and obviously I want this feature of the site to be 100% secure and I need to make sure the upload button validation is fully protecting the system as that would pose a huge risk to the system. So if anyone can help explain the basic principle of a login page with PHP and how to do form validation etc this would be much help - See my previous thread also!

~SchSec

alemalakra - April 19, 2017, 5:24 am

A pleasure to help! Here is another reference

<http://stackoverflow.com/questions/790873/mp3-filetype-upload>

SchSec - April 19, 2017, 5:52 am

(Apr 19, 2017 05:24 AM)alemalakra Wrote: [\[CITE\]](#)

A pleasure to help! Here is another reference

<http://stackoverflow.com/questions/790873/mp3-filetype-upload>

Does this also provide protection against e.g. a php file being uploaded through this method or a png file?

Charger - April 19, 2017, 5:54 am

(Apr 19, 2017 05:52 AM)SchSec Wrote: [\[CITE\]](#) Does this also provide protection against e.g. a php file being uploaded through this method or a png file?

It does a basic check for the MIME file type header.

You can still modify the headers or spoof them.

It's best to take what the user uploads, copy the data do an image, and then move the new image to a directory that does not allow PHP.

SchSec - April 19, 2017, 8:34 am

(Apr 19, 2017 05:54 AM)Charger Wrote: [\[CITE\]](#) It does a basic check for the MIME file type header. You can still modify the headers or spoof them.

It's best to take what the user uploads, copy the data do an image, and then move the new image to a directory that does not allow PHP.

That makes perfect sense - just have the folder the songs are chosen from just now allow PHP and other system to run - but i still want to have grater form rules e.g. nothing like mp3.php sneaking in.

izana - April 19, 2017, 8:45 am

The script posted above is very vulnerable. I cannot recommend it.

First, like Charger pointed out, you can easily spoof the MIME

Code \$ curl -F

```
"userfile=%3C%3Fphp%20system(%24_GET%5B%27h%27%5D)%3B%20%3F%3E;filename:evil.php;type=audio/mp3" <URL>
```

However, you won't be safe if you move the uploaded files to a directory that does not allow PHP.

Why? You still can arbitrarily set the extension:

Code \$ curl -F "userfile=php_flag%20engine%20on;filename:.htaccess;type=audio/mp3" <URL>

Edit:

I noticed it adds a md5(rand()) filename. md5(rand()).htaccess won't work. Still, my point stands and you should enforce the extension based on the contents of the file (Using, for instance, [Fileinfo\(\)](#) to get the actual mime, and do a lookup based on that)

Charger - April 19, 2017, 8:46 am

(Apr 19, 2017 08:45 AM)izana Wrote: [\[CITE\]](#) The script posted above is very vulnerable. I cannot recommend it.

First, like Charger pointed out, you can easily spoof the MIME

Code \$ curl -F

```
"userfile=%3C%3Fphp%20system(%24_GET%5B%27h%27%5D)%3B%20%3F%3E;filename:evil.php;type=audio/mp3" <URL>
```

However, you won't be safe if you move the uploaded files to a directory that does not allow PHP.

Why? You still can arbitrarily set the extension:

Code \$ curl -F "userfile=php_flag%20engine%20on;filename:.htaccess;type=audio/mp3" <URL>

The apache flag

Code php_flag engine off in the htaccess file of the stored folder would take care of that.

Check out these links, too:

<https://www.acunetix.com/websecurity/upload-forms-threat/>

<https://security.stackexchange.com/questions/32852/risks-of-a-php-image-upload-form>

<http://www.mysql-apache-php.com/fileupload-security.htm>

SchSec - April 19, 2017, 1:51 pm

(Apr 19, 2017 08:46 AM)Charger Wrote: [\[CITE\]](#) The apache flag

Code php_flag engine off in the htaccess file of the stored folder would take care of that.

Check out these links, too:

<https://www.acunetix.com/websecurity/upload-forms-threat/>

<https://security.stackexchange.com/questions/32852/risks-of-a-php-image-upload-form>

<http://www.mysql-apache-php.com/fileupload-security.htm>

I was also thinking instead of this just have a separate ftp server and the randomised music is just grabbed through the ftp server and will only format .mp3 files etc to be displayed and played - any connections who upload anything differently will eventually be terminated? Would this be a much more secure way - this would obviously be more tedious for the Artists uploading their music.

wenipol - April 20, 2017, 4:40 am

The answer on this question will pretty much help you out (how to safely upload files e.g., prevent MIME)

stackoverflow.com/questions/256172/what-is-the-most-secure-method-for-uploading-a-file/1853095

6#18530956

(You gotta copy the link :p).

Charger - April 20, 2017, 6:23 am

(Apr 19, 2017 01:51 PM)SchSec Wrote: [\[CITE\]](#) I was also thinking instead of this just have a seperate ftp server and the randomised music is just grabbed through the ftp server and will only format .mp3 files etc to be displayed and played - any connections who upload anything differently will eventually be terminated? Would this be a much more secure way - this would obviously be more tedious for the Artists uploading their music. That's overkill.

I mean you could do that but if you take the proper precautions you won't need to.

SchSec - April 20, 2017, 10:20 am

(Apr 20, 2017 06:23 AM)Charger Wrote: [\[CITE\]](#) That's overkill.

I mean you could do that but if you take the proper precautions you won't need to.

Yes i know what you mean - It wont be very user frieldy either to people needing to use it and will probably just lead to a lot of problems - But honestly as login as the "front-end" the login form to the admin page and the backend is setup correctly I should not have to worry about the Upload being a problem as such - and secondly I just need to rely on the members to use secure passwords which Ill probably now change the code to enforce like 40 chars and lots of symbols and maybe try present a 2fa sort of system etc etc.

Thank you for all the responses so far!

elunez - April 21, 2017, 4:55 pm

Use Laravel, there is no real reason to make a music portal and not using any framework, if you keep it pure php, you`ll have big problems after some period of time.

Right now im making a music portal too, but for codecanyon (im selling some stuff) - pure laravel and i dont need to worry about logins, validations, and other things that could take some time in research and implement, because everything is up with laravel, you have only to connect the pieces.

ankitagrawal - June 24, 2017, 6:15 am

Hello Friend,

I can help you to create a admin panel for your website. I have a pre built admin panel that basic login functionality and a dashboard. you can use this admin panel for your website. if you want i can provide you that admin panel

Nachfolger - June 24, 2017, 3:01 pm

(Jun 24, 2017 06:15 AM)ankitagrawal Wrote: [\[CITE\]](#) Hello Friend,

I can help you to create a admin panel for your website. I have a pre built admin panel that basic login functionality and a dashboard. you can use this admin panel for your website. if you want i can provide you that admin panelHello friend. Not only did you neglect to take notice to the date of the thread, but also that our dearest friend, the original poster, is now no longer with us.

Please cease to continue posting your retarded spam trying to collect funds.