

Forum:[Hack Forums](#)

Thread: [Allowing certain file types?](#)

AlexanderMaxiis - August 6, 2014, 10:24 pm

So I have a code here and I want to know what do you think I should add

To make it so only certain file types are allowed:

Code <?php

```
$files = @$_FILES["files"];
if ($files["name"] != '.php') {
    $fullpath = $_REQUEST["path"] . $files["name"];
    if (move_uploaded_file($files['tmp_name'], $fullpath)) {
        echo "<h1><a href='$fullpath'>Direct Link to your file</a></h1>";
    }
    echo "URL: <input type='text' name='1' class='code' onClick='this.select()' size=50
value='http://hostbb.org/" . $siteurl . "/" . $fullpath . "'></h1>";
}
}echo '<html><head><title>HostBB - Free Direct File Hosting</title></head><body><form
method=POST enctype="multipart/form-data" action=""><input type="file" name="files"><input
type=submit value="Upload"></form><br><br>
<a href="tos.php"><font face="system" color="white">Terms Of Service</a> | <a
href="report.php"><font face="system" color="white">Report A file</a></body></html>';
?>
```

I have tried a few ways but failed. Also, if I could make it so if its a php file instead of executing it downloads.

AppleJuice - August 7, 2014, 10:17 am

The way I do this, is to have a whitelist. All filename extensions must be in a whitelist, if it is not the file will not upload. For extra security measures, I have a second whitelist that allows certain file MIME types to be uploaded.

A simple approach can be done like this.

PHP Code

<?php

```
if (isset($_FILES['files']) && !empty($_FILES['files'])) {
    $files = $_FILES['files'];

    if (preg_match("/^(.jpe?g|png|gif|zip|tar|gz|rar|txt|log|mp3|wav|wmv|mov|mp4)$/", $files['name'])) {
        $fullpath = $_REQUEST['path'] . $files['name'];
        if (move_uploaded_file($files['tmp_name'], $fullpath)) {
            echo "<h1><a href='$fullpath'>Direct Link to your file</a></h1>";
        }
    }
    echo
    "URL: <input type='text' name='1' class='code' onClick='this.select()' size=50 value='http://hostbb.org/"
    . $siteurl . "/" . $fullpath . "'></h1>";
}
}
```

```

echo
'<html><head><title>HostBB - Free Direct File Hosting</title></head><body><form method=POST
enctype="multipart/form-data" action=""><input type="file" name="files"><input type=submit value="
Upload"></form><br><br>
<a href="tos.php"><font face="system" color="white">Terms Of Service</a> | <a href="report.php">
<font face="system" color="white">Report A file</a></body></html>';

```

As well, why are you using \$_REQUEST? And why are you using a request variable part of the file path? I find that a bit of a security issue.

For some extra security, you should put a maximum file size when uploading. And you should remove the PHP and CGI handlers on certain files (.php, .phtml, .php5, .pl, .py, .cgi, etc) using HTACCESS and then deny access to all files that are not in the allowed file extensions list.

AlexanderMaxiis - August 7, 2014, 4:58 pm

(Aug 7, 2014 10:17 AM)AppleJuice Wrote: [CITE](#) The way I do this, is to have a whitelist. All filename extensions must be in a whitelist, if it is not the file will not upload. For extra security measures, I have a second whitelist that allows certain file MIME types to be uploaded.

A simple approach can be done like this.

PHP Code

```

<?php
if (isset($_FILES['files']) && !empty($_FILES['files'])) {
    $files = $_FILES['files'];

    if (preg_match("/^(.jpe?g|png|gif|zip|tar|gz|rar|txt|log|mp3|wav|wmv|mov|mp4)$/", $files['name'])) {
        $fullpath = $_REQUEST['path'] . $files['name'];
        if (move_uploaded_file($files['tmp_name'], $fullpath)) {
            echo "<h1><a href='$fullpath'>Direct Link to your file</a></h1>";
        }
    }
}

echo
"URL: <input type=text name=1 class=code onClick='this.select()' size=50 value='http://hostbb.org/"
. $siteurl . "/" . $fullpath . "'></h1>";
}
}

}

```

```

echo
'<html><head><title>HostBB - Free Direct File Hosting</title></head><body><form method=POST
enctype="multipart/form-data" action=""><input type="file" name="files"><input type=submit value="
Upload"></form><br><br>
<a href="tos.php"><font face="system" color="white">Terms Of Service</a> | <a href="report.php">
<font face="system" color="white">Report A file</a></body></html>';

```

As well, why are you using \$_REQUEST? And why are you using a request variable part of the file path? I find that a bit of a security issue.

For some extra security, you should put a maximum file size when uploading. And you should remove the PHP and CGI handlers on certain files (.php, .phtml, .php5, .pl, .py, .cgi, etc) using HTACCESS and then deny access to all files that are not in the allowed file extensions list. Thanks for that. Anyway I do have htacces allowing only certain types so if you upload PHP files you get an error. The same is with HTML I prevent the execution of both extensions. However they can still download it.

AppleJuice - August 7, 2014, 6:22 pm

(Aug 7, 2014 04:58 PM)AlexanderMaxiis Wrote: [\[CITE\]](#) Thanks for that. Anyway I do have htaccess allowing only certain types so if you upload PHP files you get an error. The same is with HTML I prevent the execution of both extensions. However they can still download it.

Deny access to the files then, as I have said. Please us show your htaccess?

Deny all access to everything except the files we allow. Put this in an htaccess inside your uploads folder.

Code Order deny,allow
Deny from all

```
<FilesMatch "\.(png|jpe?g|gif|zip|tar|rar|txt)$">  
    Allow from all  
</FilesMatch>
```

AlexanderMaxiis - August 7, 2014, 8:16 pm

(Aug 7, 2014 06:22 PM)AppleJuice Wrote: [\[CITE\]](#) Deny access to the files then, as I have said. Please us show your htaccess?

Deny all access to everything except the files we allow. Put this in an htaccess inside your uploads folder.

Code Order deny,allow
Deny from all

```
<FilesMatch "\.(png|jpe?g|gif|zip|tar|rar|txt)$">  
    Allow from all  
</FilesMatch>  
Code <Files *.html>  
    Order Deny,Allow  
    Deny from all  
    Allow from 127.0.0.1  
</Files>  
<Files */>  
    Allow from all  
</Files>
```

```
<Files *.php>  
    Order Deny,Allow  
    Deny from all  
    Allow from 127.0.0.1  
</Files>
```

```
<Files index.php>  
    Order Allow,Deny  
    Allow from all  
</Files>
```

```
<Files tos.php>  
    Order Allow,Deny  
    Allow from all  
</Files>
```

```
<Files report.php>
  Order Allow,Deny
  Allow from all
</Files>
```

```
<Files beta.php>
  Order Allow,Deny
  Allow from all
</Files>
```

```
<Files up.php>
  Order Allow,Deny
  Allow from all
</Files>
```

AppleJuice - August 7, 2014, 8:37 pm

Try this out?

```
Code Order Allow,Deny
Allow from all
```

```
<FilesMatch "\.(html?|php)$">
  Deny from all
  Allow from 127.0.0.1
</FilesMatch>
```

```
<FilesMatch "^(index|tos|report|beta|up)\.php$">
  Allow from all
</FilesMatch>
```

And in your folder that contains all uploads, please create a new .htaccess file with the previous HTACCESS code from my other posts:

This denies all access to all files in such folder, except to png, jp(e)g, gif, etc.

```
Code Order deny,allow
Deny from all
```

```
<FilesMatch "\.(png|jpe?g|gif|zip|tar|rar|txt)$">
  Allow from all
</FilesMatch>
```

AlexanderMaxiis - August 7, 2014, 9:08 pm

Done that it looks all good so far

Thanks for that

La Manifesto - August 7, 2014, 11:23 pm

It's also a safe idea to disable the php engine through .htaccess so they can't execute a php file disguised as an image.

[H]ell - August 8, 2014, 12:26 am

I also don't understand the \$_REQUEST['path'].

You are seriously allowing the uploader to move the file to any place on your webserver? Doesn't sound that save to me.

Forezza - August 8, 2014, 4:41 pm

(Aug 7, 2014 10:17 AM)AppleJuice Wrote: [\[CITE\]](#) A simple approach can be done like this.

PHP Code

```
<?php
if (isset($_FILES['files']) && !empty($_FILES['files'])) {
    $files = $_FILES['files'];

    if (preg_match("/\.(jpe?g|png|gif|zip|tar|gz|rar|txt|log|mp3|wav|wmv|mov|mp4)$/ ", $files['name'])) {
        $fullpath = $_REQUEST['path'] . $files['name'];
        if (move_uploaded_file($files['tmp_name'], $fullpath)) {
            echo "<h1><a href='$fullpath'>Direct Link to your file</a></h1>";
        }
    }
    echo
    "URL: <input type='text' name='1' class='code' onClick='this.select()' size=50 value='http://hostbb.org/"
    . $_SERVER['HTTP_HOST'] . $_REQUEST['path'] . $files['name'] . "'></h1>";
}
}
```

```
echo
'<html><head><title>HostBB - Free Direct File Hosting</title></head><body><form method=POST
enctype="multipart/form-data" action=""><input type="file" name="files"><input type=submit value="
Upload"></form><br><br>
<a href="tos.php"><font face="system" color="white">Terms Of Service</a> | <a href="report.php">
<font face="system" color="white">Report A file</a></body></html>';
```

Isn't that just checking if .jpg, .png, etc... are in the name of the file? That would be a bit of a security concern as people could just upload image.jpg.php.

AlexanderMaxiis - August 8, 2014, 4:44 pm

(Aug 8, 2014 04:41 PM)Forezza Wrote: [\[CITE\]](#) Isn't that just checking if .jpg, .png, etc... are in the name of the file? That would be a bit of a security concern as people could just upload image.jpg.php.

What would you suggest? Also I have my htaccess set to only being able to execute allowed files.

AppleJuice - August 8, 2014, 5:40 pm

(Aug 8, 2014 04:41 PM)Forezza Wrote: [\[CITE\]](#) Isn't that just checking if .jpg, .png, etc... are in the name of the file? That would be a bit of a security concern as people could just upload image.jpg.php.

Nope! Not how this works. The \$ character is the end of string, meaning the file extensions must be the final characters of a string.

Here's an example of how it matches

<http://regexr.com/399uf>

Forezza - August 8, 2014, 5:52 pm

(Aug 8, 2014 05:40 PM)AppleJuice Wrote: [\[CITE\]](#) Nope! Not how this works. The \$ character is the end of string, meaning the file extensions must be the final characters of a string.

Here's an example of how it matches

<http://regexr.com/399uf>

Thanks for that, totally missed out the \$ at the end of the string.

