



swzaq Update README.md ...

26 days ago

🕒 18

[View code](#)

☰ README.md

# YJCMS file upload vulnerability

## 1. Vulnerability Background

Yunjing cms is developed by gansu yunjing digital technology co., ltd. YJcms (Cloudscape cms) is an open source PHP enterprise website building management system developed based on ThinkPaPHP5.0.24. Yjcms adheres to the concept of minimalist, fast and extreme development, integrates enterprise, tourism and mall modules for development, and is a module and plug-in that can be easily and rapidly expanded. To facilitate developers to quickly build their own applications.

Address of the company's official website: <http://www.xjyunjing.com/>

Test targets:

1. [https://gzyjg.cn/user\\_login.html](https://gzyjg.cn/user_login.html)
2. [https://gsxwjks.com/user\\_login.html](https://gsxwjks.com/user_login.html)

## 2. Vulnerability exploitation process

The homepage of the normal website is shown as follows

<https://xx.com/>



This cms has the registration function

<https://xx.com/user>

Entering the user path will jump to the login and registration page, as shown below





You can register and log in here

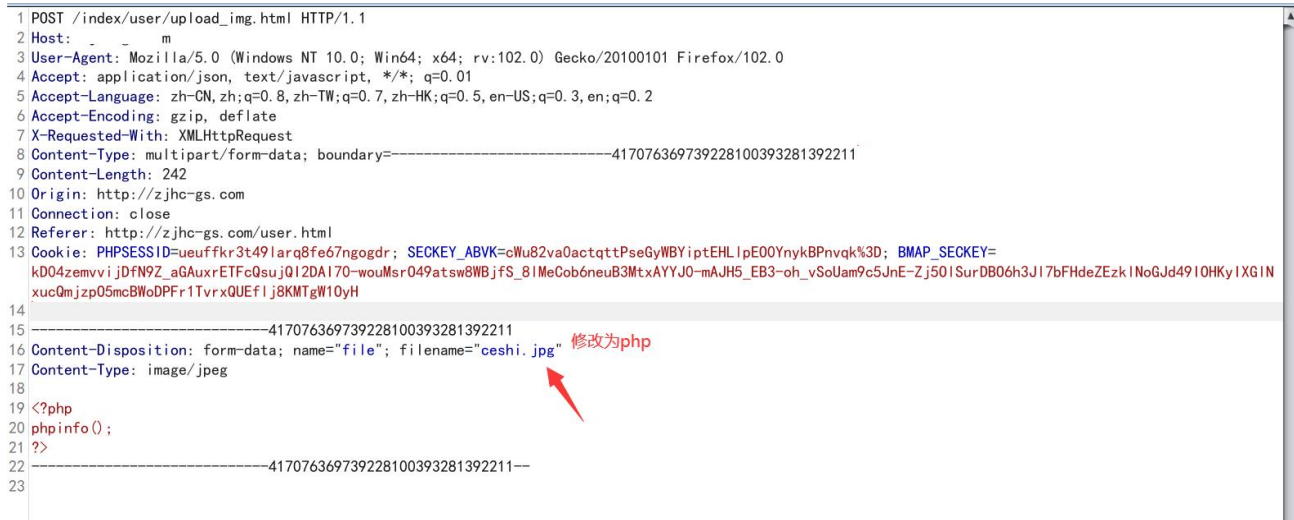


After registering the account, log in to the background as follows

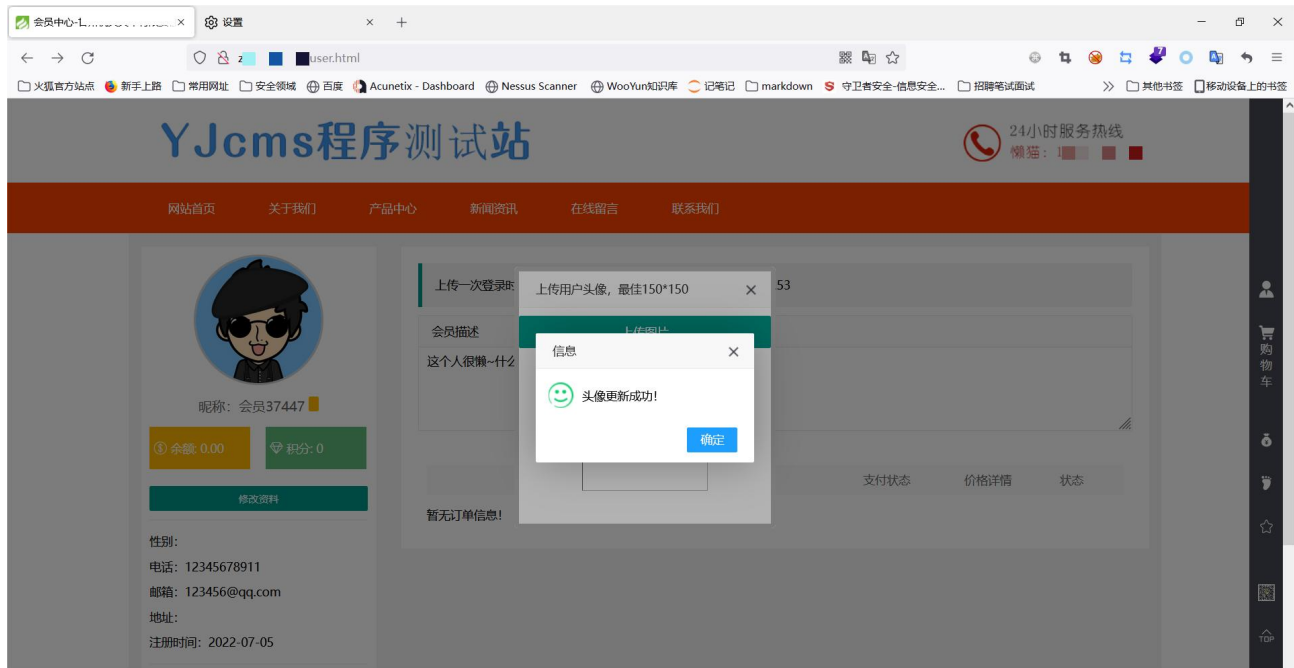


After the account is registered, log in to the background and there is a file upload vulnerability in the modified avatar. However, the front-end verification is done here, so first change the php file to the image format

![]image/62.jpg)

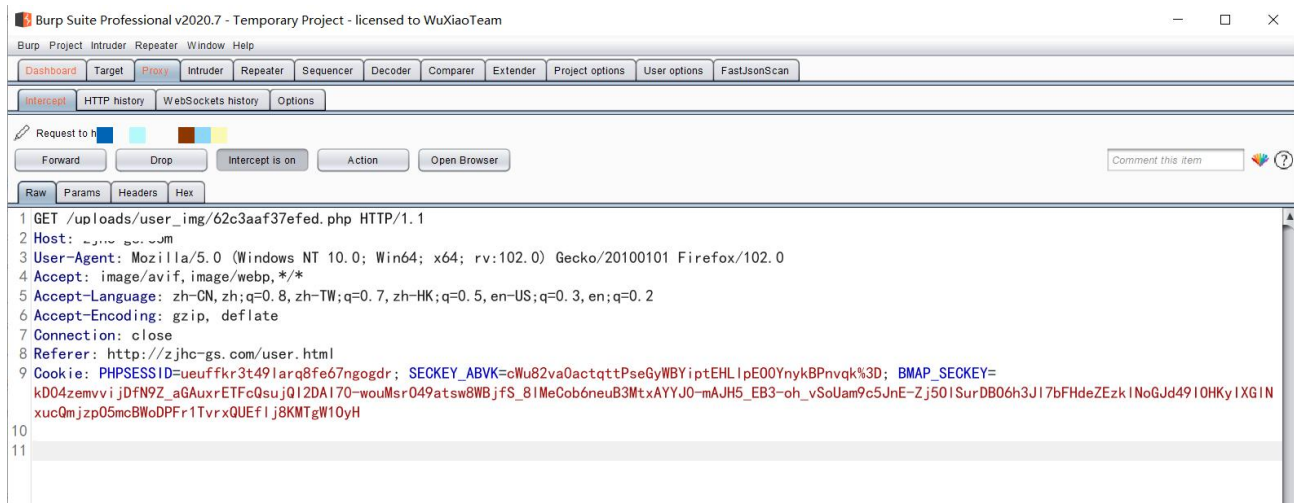


The successful upload is shown as follows




Click OK to capture the package and return to the address of the uploaded file

/uploads/user\_img/62c3aaf37efed.php



Accessing this file shows that the PHP file has been uploaded successfully



PHP Version 7.3.32	
	
System	Linux i20j2u2mlcdbmw9he1zriZ 5.10.0-11-amd64 #1 SMP Debian 5.10.92-2 (2022-02-28) x86_64
Build Date	May 13 2022 10:53:19
Configure Command	'./configure' '--prefix=/www/server/php/73' '--with-config-file-path=/www/server/php/73/etc' '--enable-fpm' '--with-fpm-user=www' '--with-fpm-group=www' '--enable-mysqlnd' '--with-mysqli=mysqlnd' '--with-pdo-mysql=mysqlnd' '--with-iconv-dir' '--with-freetype-dir=/usr/local/freetype' '--with-jpeg-dir' '--with-png-dir' '--with-zlib' '--with-libxml-dir=/usr' '--enable-xml' '--disable-rpath' '--enable-bcmath' '--enable-shmop' '--enable-sysvsem' '--enable-inline-optimization' '--with-curl=/usr/local/curl' '--enable-mbregex' '--enable-mbstring' '--enable-intl' '--enable-ftp' '--with-gd' '--with-openssl=/usr/local/openssl' '--with-mhash' '--enable-pcntl' '--enable-sockets' '--with-xmlrpc' '--enable-soap' '--with-gettext' '--disable-fileinfo' '--enable-opcache' '--with-sodium=/usr/local/libsodium' '--with-webp-dir=/usr'
Server API	FPM/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/www/server/php/73/etc
Loaded Configuration File	/www/server/php/73/etc/php.ini
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)
PHP API	20180731
PHP Extension	20180731
Zend Extension	320180731
Zend Extension Build	API320180731.NTS
PHP Extension Build	API20180731.NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	enabled
Zend Memory Manager	enabled
Zend Multibyte Support	provided by mbstring
IPv6 Support	enabled

## Releases

No releases published

## Packages

No packages published