debug601 Create UCMS-RCE1.md History

1 contributor

23 lines (13 sloc) | 1.09 KB

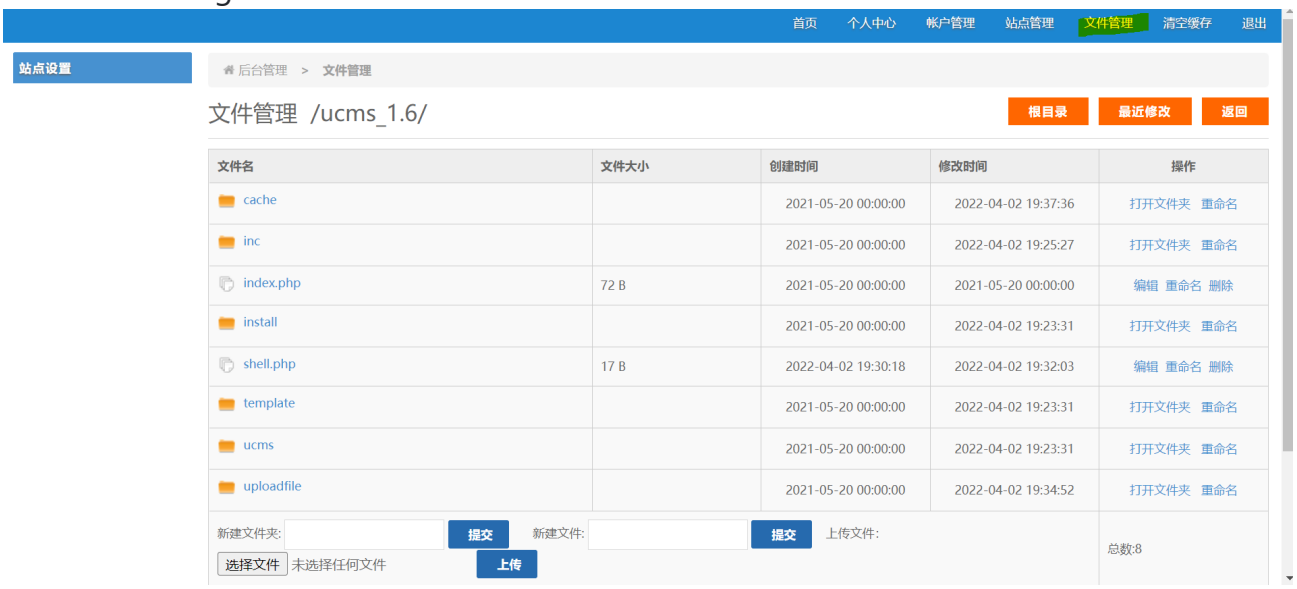
There is an arbitrary file upload vulnerability (RCE) in the file management module in UCMS 1.6.

vendor: http://uuu.la/

UCMS 1.6 installation package： http://uuu.la/uploadfile/file/ucms_1.6.zip

After installation, log in to the background

Click File Management



Click uploadfile

Click to select the file, and after selecting the file ---> Click upload to upload to the "uploadfile directory"

We visit the shell.php file from the browser and upload it to the uploadfile directory of the website, and we find that the code has been executed

JFJF

PHP 版本 5.2.17

系统	Windows NT 桌面-EVF2JTB 6.2 构建 9200
建造日期	2011年1月6日17:26:08
配置命令	cscript /nologo configure.js "--enable-snapshot-build" "--en snapshot-template=d:\php-sdk\snap_5_2\vc6\x86\template" sdk\snap_5_2\vc6\x86\php_build" "--with-pdo-oci=D:\php- sdk\oracle\instantclient10\sdk,shared" "--with -oci8=D:\php sdk\oracle\instantclient10\sdk,shared" "--without-pi3web"
服务器 API	Apache 2.4 处理程序 - Apache Lounge
虚拟目录支持	启用
配置文件 (php.ini) 路径	C:\Windows