

Typesetter CMS 文件上传漏洞复现(CVE-2020-25790)

复现环境

PHP 版本 7.3.9

Apache 2.4.39

Typesetter cms 5.0.3

经过测试最新版本5.1已经修复这个上传漏洞

CMS 地址: <https://github.com/Typesetter/Typesetter/releases>

安裝 - v5.0.3

中文 (zh)

[Help translate Typesetter](#)

檢查伺服器...

正在檢查...	狀態	目前的值	預期的值
..._pro/WWW/Typesetter-5.0.3/data	已通過	Writable	Writable
PHP 版本	已通過	7.3.9	5.3+
SCRIPT_NAME or PHP_SELF	已通過	設定	設定
Safe Mode	已通過	關	關
Register Globals	已通過	關	關
Magic Quotes Sybase	已通過	關	關
Magic Quotes Runtime	已通過	關	關
Memory Limit	已通過	Adjustable	Adjustable
正在檢查...	狀態	備註	
...Typesetter-5.0.3/index.html	已通過		
圖片功能	已通過	jpg, png, bmp, gif	

[重新整理](#)

設定

網站標題

My Typesetter

電子郵件地址

管理者帳號

管理者密碼

請再輸入一次密碼

[更多選項...](#)

安裝

如果拓展未通过,添加bz2拓展到配置文件中(也可以去掉前面的分号),将压缩拓展开启

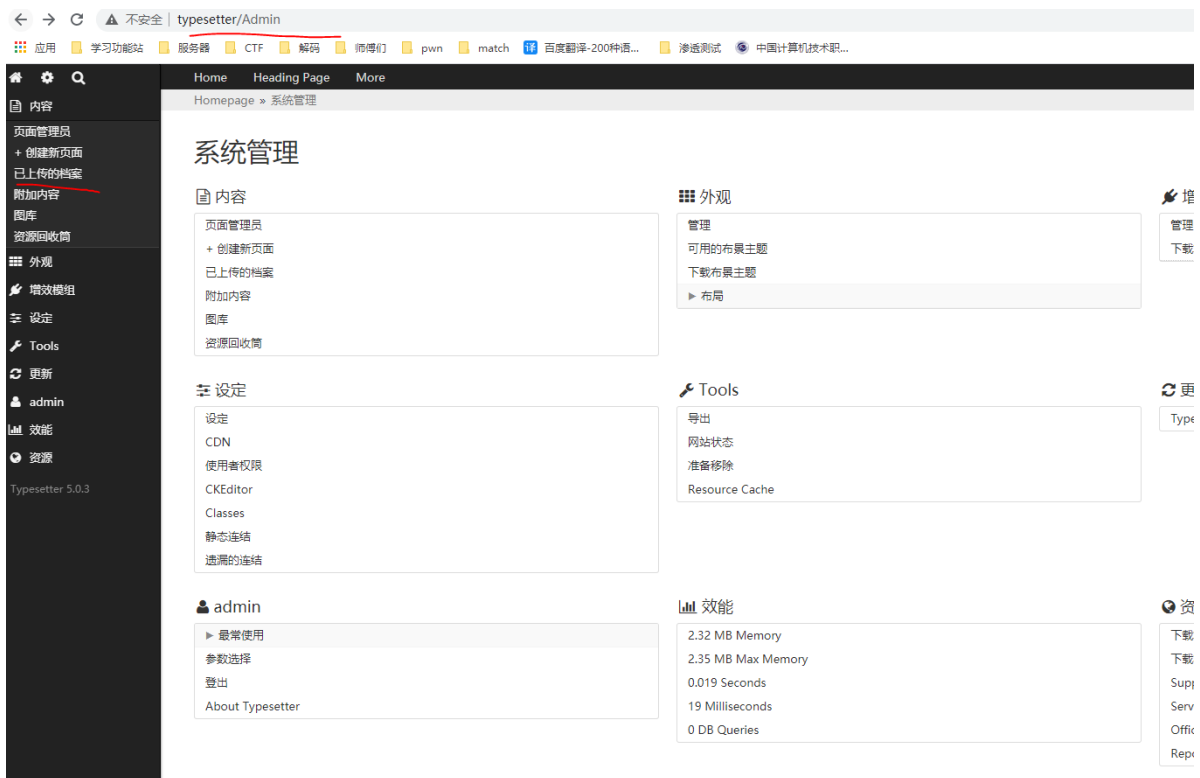
```
php.ini - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

; directory, You may specify an absolute path to the library file:
; extension=/path/to/extension/mysql.so
; Note : The syntax used in previous PHP versions ('extension=<ext>.so' and
; 'extension='php_<ext>.dll') is supported for legacy reasons and may be
; deprecated in a future PHP major version. So, when it is possible, please
; move to the new ('extension=<ext>') syntax.
; Notes for Windows environments :
; - Many DLL files are located in the extensions/ (PHP 4) or ext/ (PHP 5+)
; extension folders as well as the separate PECL DLL download (PHP 5+).
; Be sure to appropriately set the extension_dir directive.
;extension=bz2
extension=bz2
extension=pdo_mysql

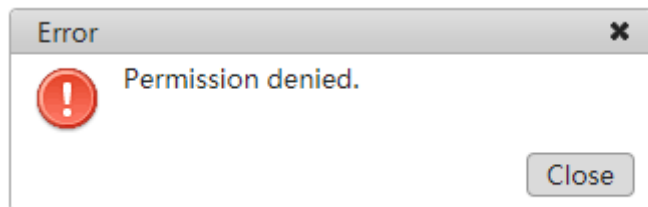
第 705 行, 第 14 列 100% Windows (CRLF)
```

随意填写账户密码,安装cms

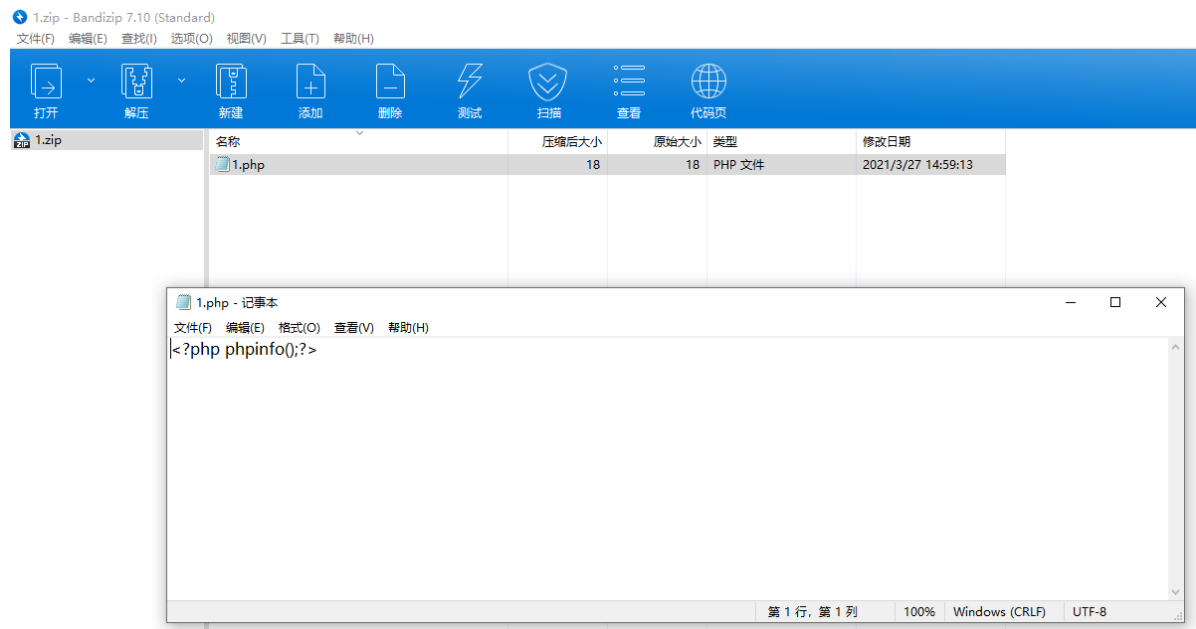
1.进入后台<http://typesetter/Admin>,登录后进入已上传的档案页面



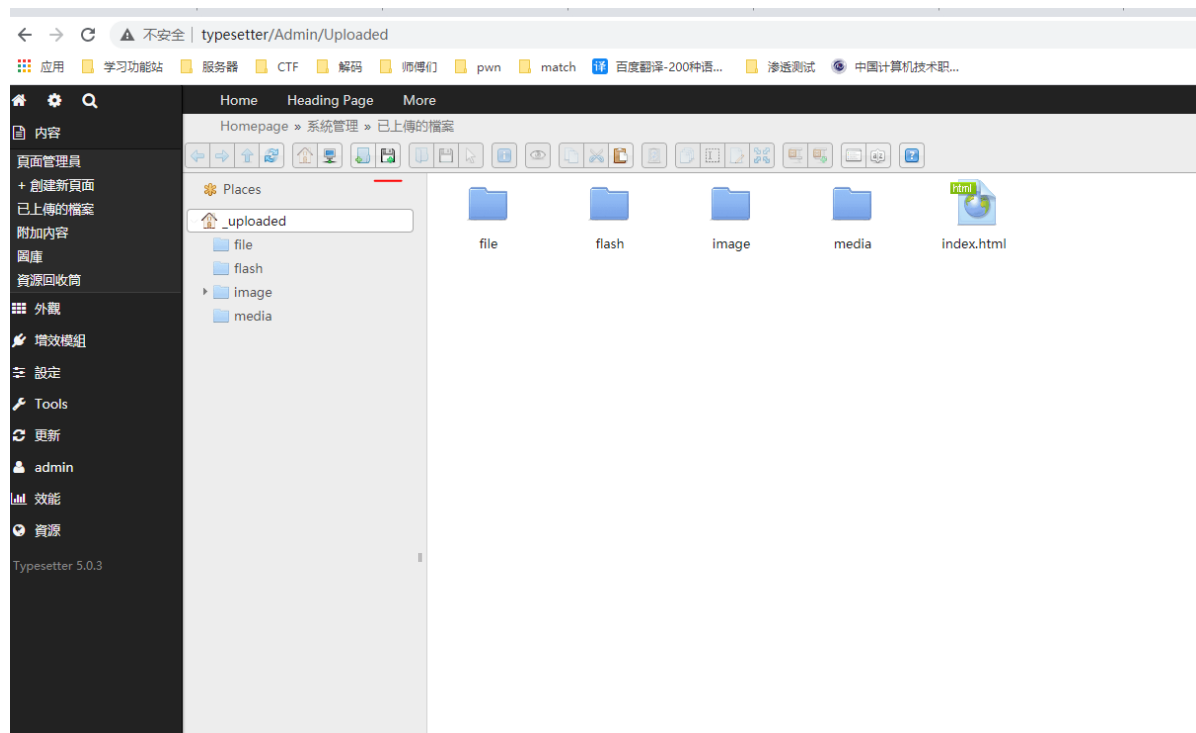
2.尝试直接上传php文件,可以看到不被允许



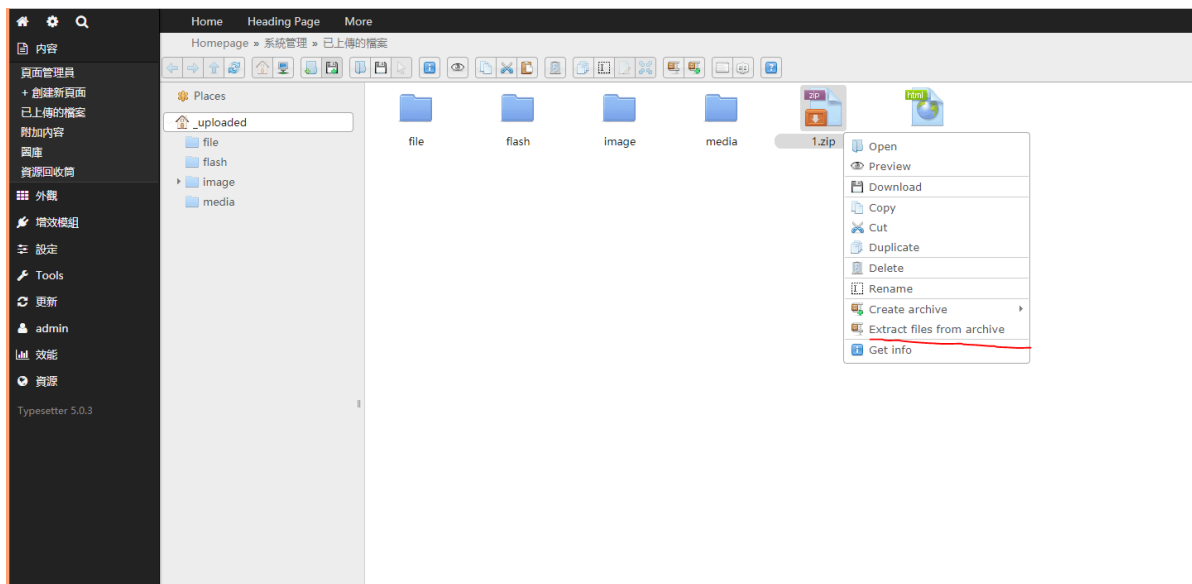
准备好包含php木马的zip文件



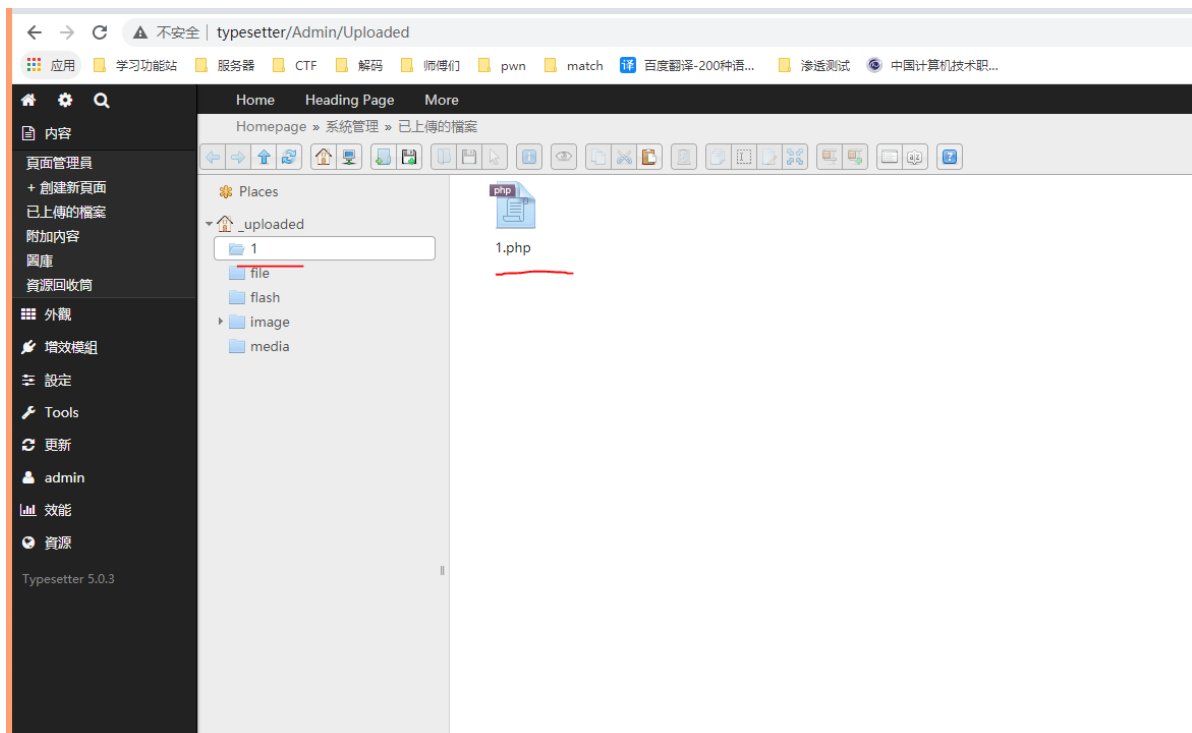
3.点击上传按钮,将zip文件上传上去



4.右击上传上去的zip文件将其解压



5.解压出来的文件名为压缩包名字,内容为木马文件



6.访问可以看到php木马被成功执行

←

→

↺

⚠ 不安全

typesetter/data/_uploaded/1/1.php

应用

学习功能站

服务器

CTF

解码

师傅们

pwn

match


13

百度翻译-200种语...

渗透测试

中国计算机技术配...

PHP Version 7.3.9



System	Windows NT LAPTOP-2F1J03Q 10.0 build 18363 (Windows 10) AMD64
Build Date	Aug 28 2019 09:20:38
Compiler	MSVC15 (Visual C++ 2017)
Architecture	x64
Configure Command	ccscript /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--disable-zts" "--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	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	C:\WINDOWS
Loaded Configuration File	D:\PHP\phpstudy_pro\Extensions\php\php7.3.9nts\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,VC15
PHP Extension Build	API20180731,NTS,VC15
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
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
Registered Stream Filters	convert.iconv.*, string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, dechunk, zlib.*, bzip2.*

This program makes use of the Zend Scripting Language Engine:
Zend Engine v3.3.9, Copyright (c) 1998-2018 Zend Technologies

