

New issue

[Jump to bottom](#)

# [Bug]: Remote Command Execution/远程命令执行 #9

Open Mn-blue opened this issue on Mar 3 · 5 comments

Mn-blue commented on Mar 3

## baigoCMS Remote Command Execution

### Description

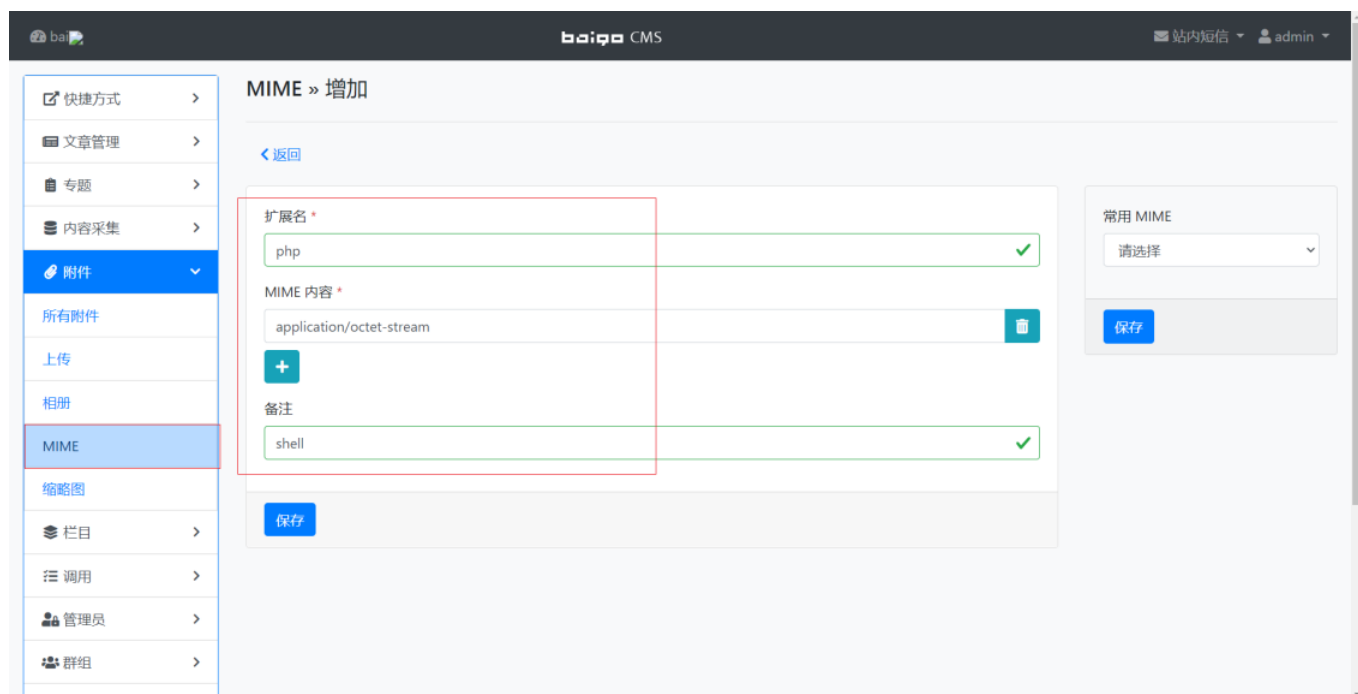
When we are already logged in to the background, we can add MIME and then upload a webshell . By this way, we can remotely execute any system command on the web server.

### Affected versions of baigoCMS

version: baigoCMS-3.0-alpha-2

### PoC

#### 1. Login to the background, add a MIME type



## 2. Upload webshell .

It is recommended to use one sentence webshell . E.g :

baigo CMS

站内短信 admin

附件

全部 1 保留数据 0


关键词

选择文件... 上传

高级上传模式

警告！此操作将耗费较长时间！

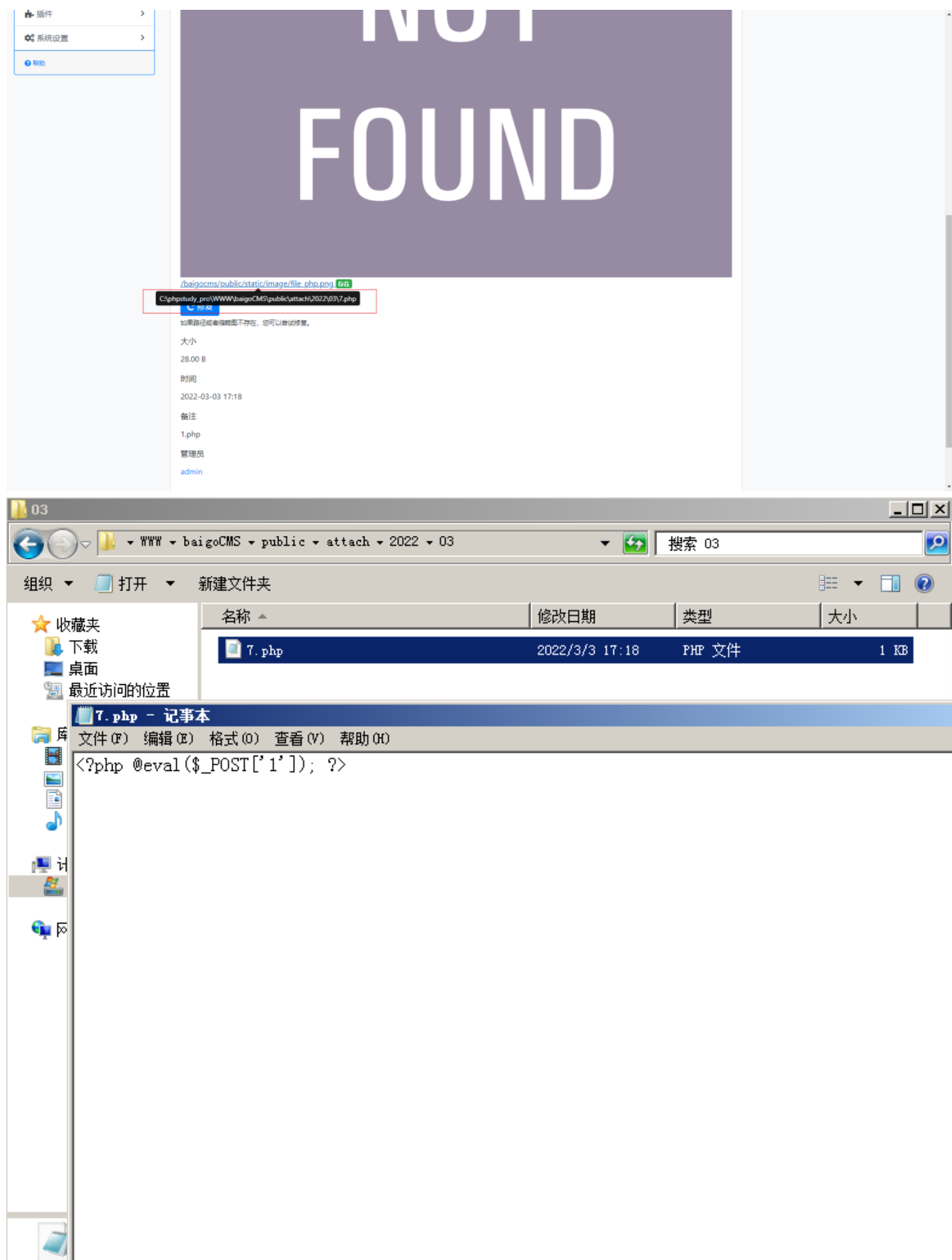
清理附件

ID	详情	管理员 / 备注	大小 / 时间
7	 1.php <a href="#">查看</a> <a href="#">编辑</a> <a href="#">回收站</a>	admin 1.php	28.00 B 03:03:17:18

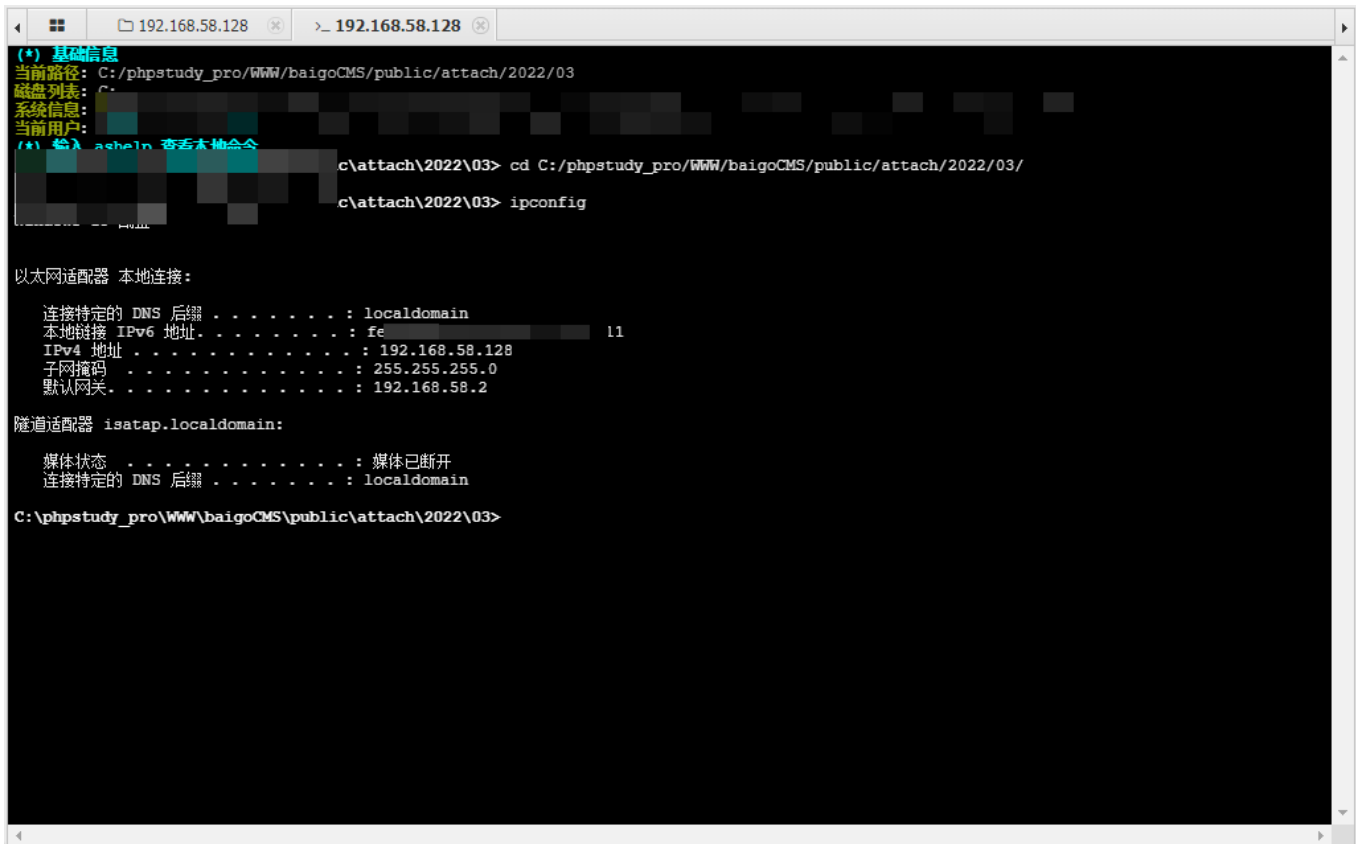
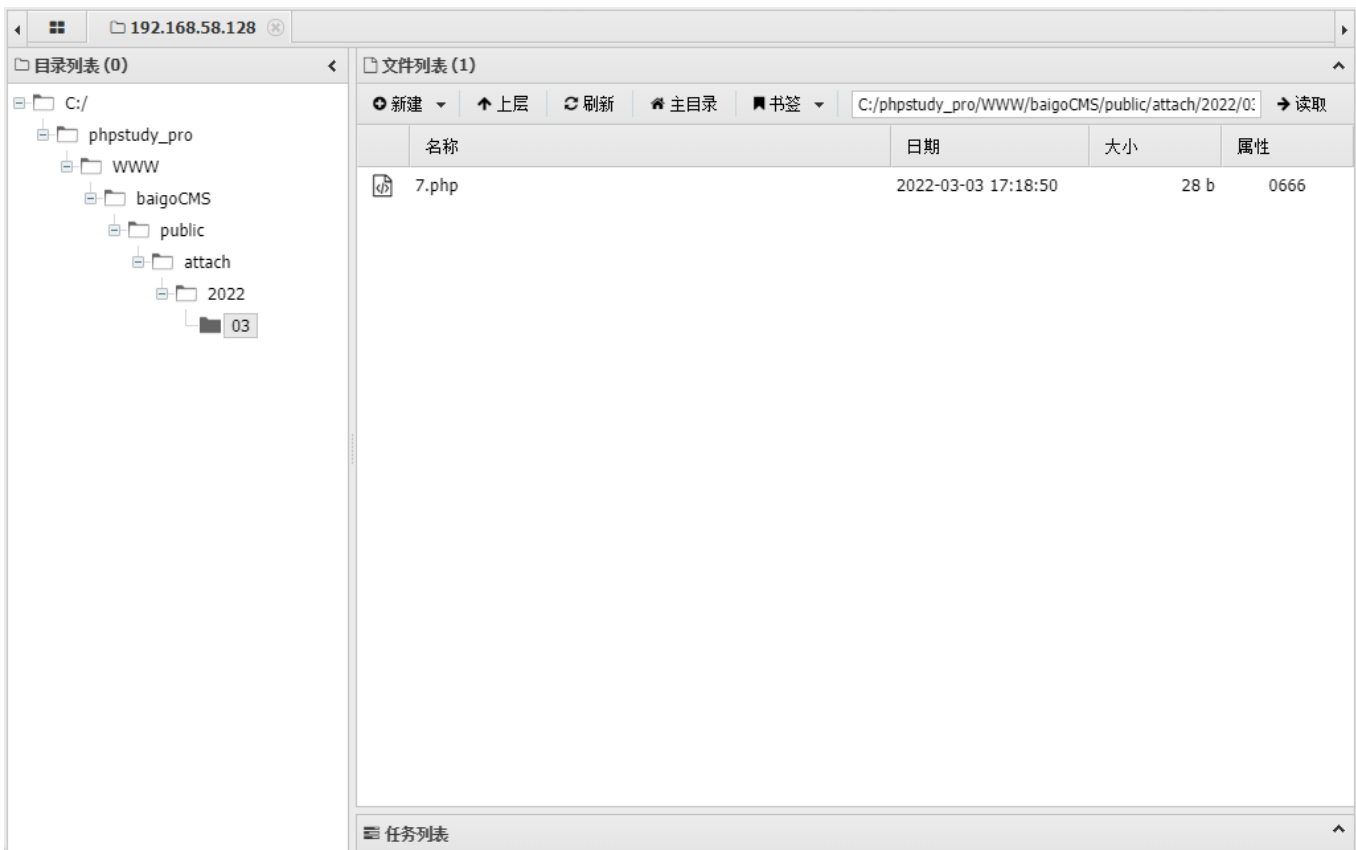
批量操作 提交

192.168.58.128/baigocms/public/index.php/console/attach/show/id/7/

Splicing website path : [http://\[192.168.58.128/baigocms/public/attach/2022/03/7.php](http://[192.168.58.128/baigocms/public/attach/2022/03/7.php)



### 3.Connect



Mn-blue commented on Mar 3

Author

Repair method:

1.Set the directory where the uploaded files are stored as non-executable permissions

2.Restrict the MIME types that attackers can customize to add

**fonerig** commented on Mar 28

Contributor

您咋不说 ftp 也可以上传 php 文件?

**fonerig** commented on Mar 28

Contributor

另外，上传目录的可执行权限是 cms 系统决定的吗?

**Mn-blue** commented on Mar 28

Author

FTP虽然可以上传PHP文件，但是不会解析执行；此处可以上传脚本文件并解析执行，存在一定危害。

**Mn-blue** commented on Mar 28

Author

而且设计附件上传的功能的初衷应该不包括上传危险的脚本文件吧

#### Assignees

No one assigned

#### Labels

None yet

#### Projects

None yet

#### Milestone

No milestone

#### Development

No branches or pull requests

Participants

2 participants

