Cute Http File Server JWT

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.Xc17butuxIOJkq1pwI8CHsNJndo8gXdjvmqfDLzh8Q4;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

实验效果

before login

successful jwt forgery