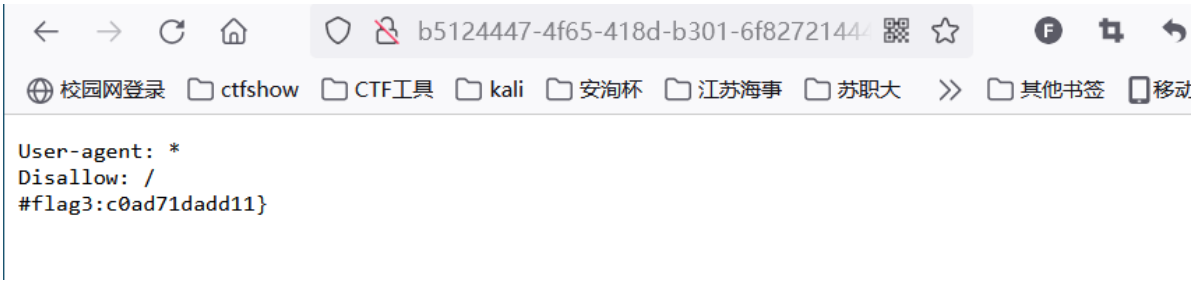
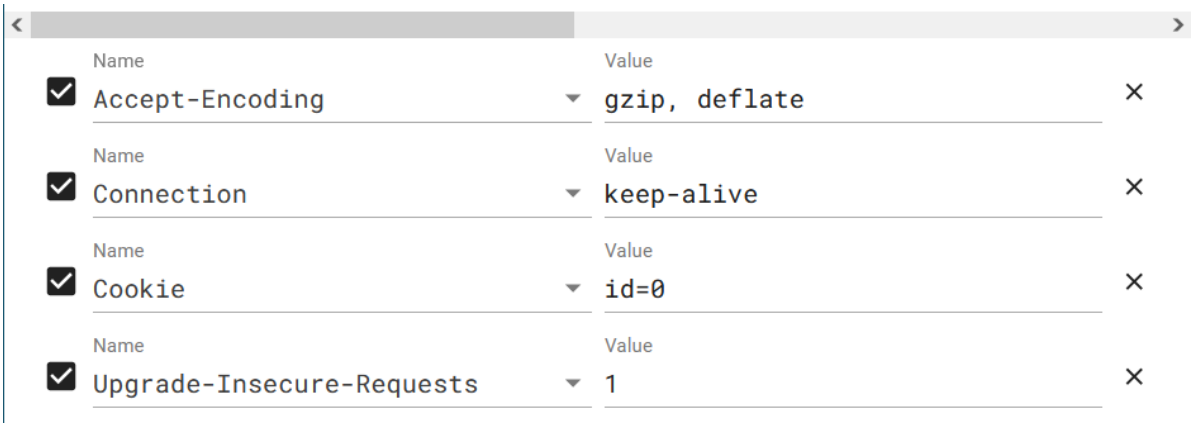
发现robots.txt

打开查看，发现flag3

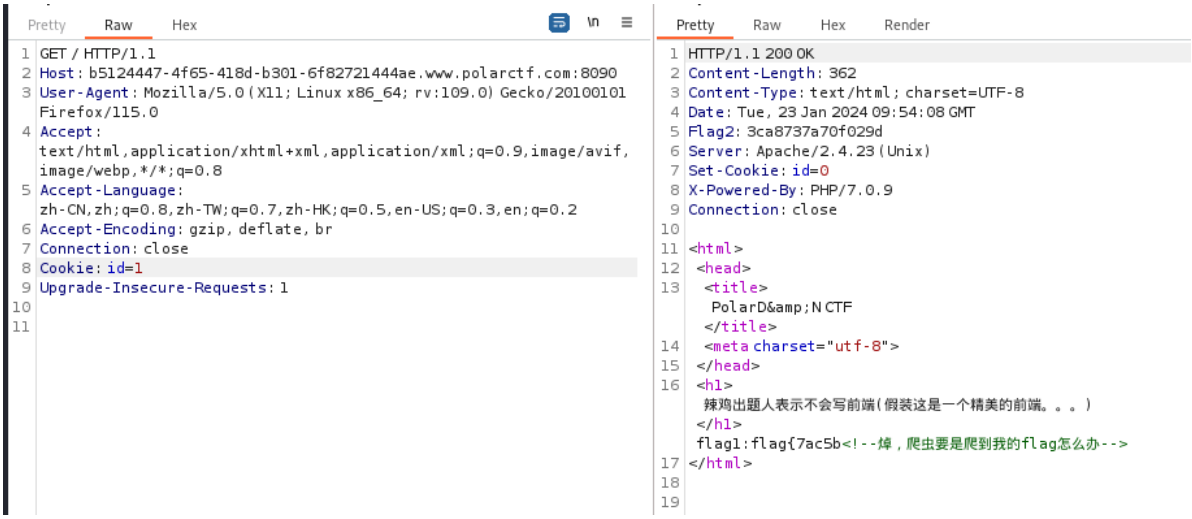


发现cookie



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。

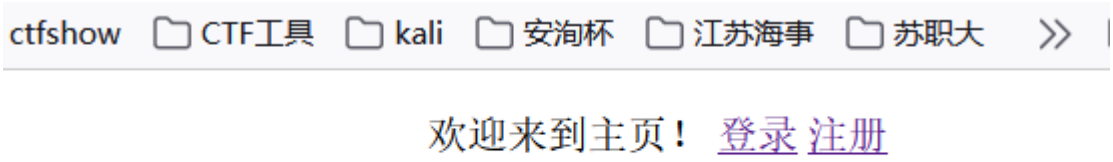
通过JSON形式作为Web应用中的令牌，用于在各方之间安全地将信息作为JSON对象传输。在数据传输过程中还可以完成数据加密、签名等相关处理。巴拉巴拉的
https://blog.csdn.net/Top_L398/article/details/109361680
看去吧

简单点说

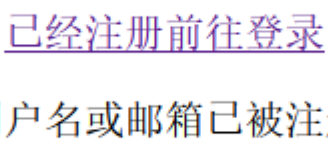
JWT分为三部分abc

a:标头 b:有效载荷 c:签名

先看题目



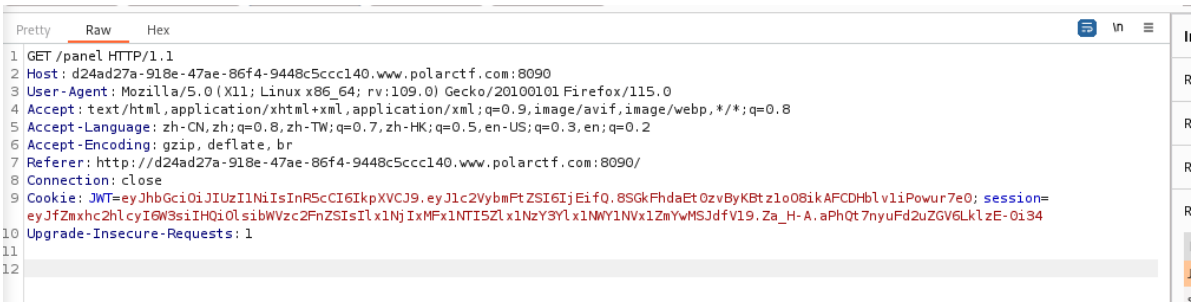
没有账号，我们先注册一个admin



提示用户名已经被注册，猜测可能flag可能和admin有关，可能需要登录admin账户

随便注册一个登录

查看个人中心并进行抓包



发现JWT

拿过来分析一下

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6IjEifQ.8SGkFhdaEt0zvByKBtz1oO8ikAFCDHblv1iPowur7e0

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/

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

我们将

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

改成

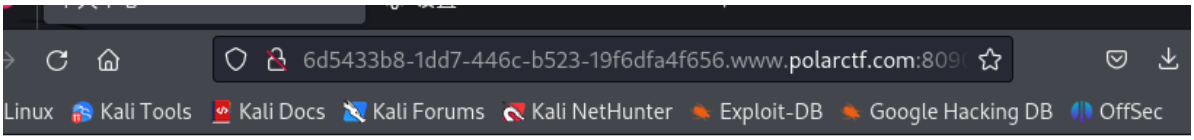
```
{
  "username": "admin"
}
```

并且加上密钥，进行编译

得到一串新的JWT

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImFkbWluIn0.9avq5ApZ-XZul2kbon8z2cB6Y4bNru_OnnIZfJ1mO5O
```

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{ec39c705cfb5295f9dddcedc819a1659}

邮箱：admin@polarctf.com

得到flag