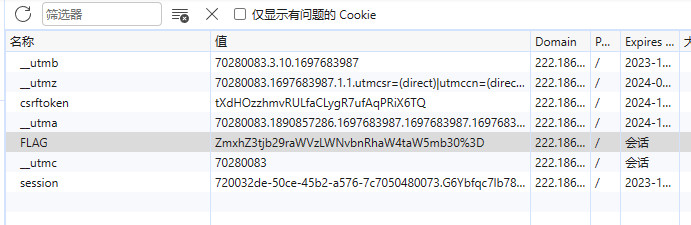
**题目1：**

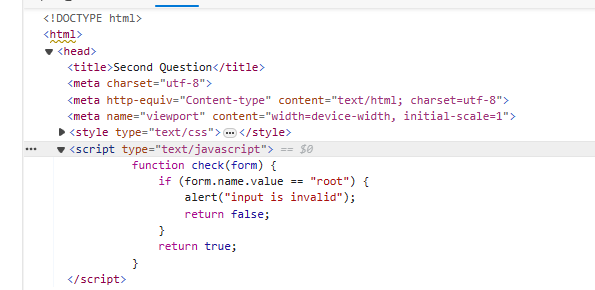
打开网站，发现cookie里有类似flag的字段，是base64编码的，解码即可得到flag



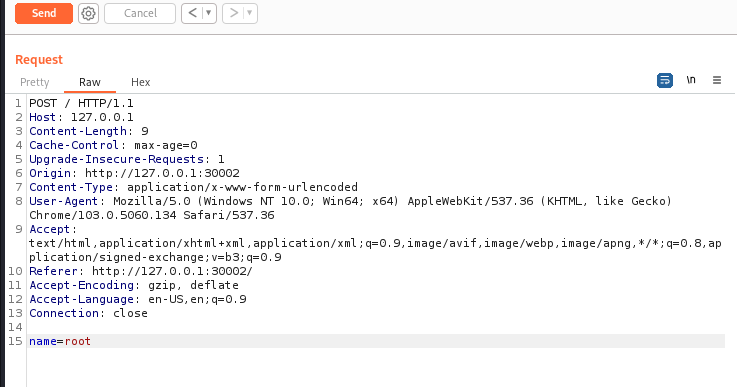


**题目2：**

首先检查页面源代码，发现对于root的校验在前端js中，

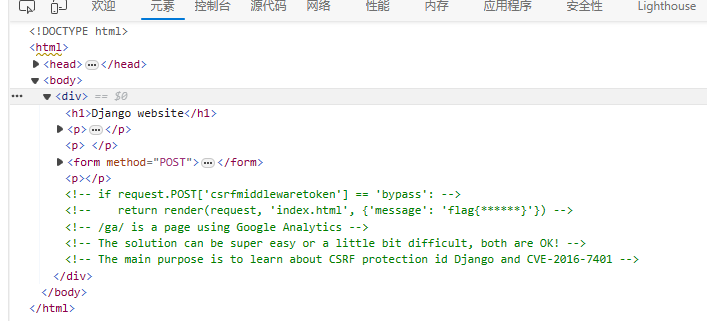


可以直接抓包修改该值，发送后又发现服务器只接受Host是127.0.0.1的请求，再修改该Host值即可，如下所示



**题目3：**

在/csrf查看源代码，可以看到如下的提示



将cookie里的csrftoken和post请求里的都改成bypass，再重新发送，得到flag

