/\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*/

/\* 程序作者：爱的伊苏 \*/

/\* 程序完成时间：2019/2/3 \*/

/\* 有任何问题请联系：740531307@qq.com \*/

/\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*/

//@永远得意的笑下去

下面为题目所给信息

* **http header**

**Forbidden**

You don't have permission to access / on this server.

Please make sure you have installed .net framework 9.9!

Make sure you are in the region of England and browsing this site with Internet Explorer

请确保您已安装.net framework 9.9！

确保您在英格兰地区并使用Internet Explorer浏览此站点

可以发现需要我们装个框架并且在英格兰用IE浏览器打开

但是我们并不需要

Just only need the BrupSuite to 修改一下

哈哈哈中英结合！

下面为连接原文

ET /sHeader/ HTTP/1.1

Host: ctf5.shiyanbar.com

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:65.0) Gecko/20100101 Firefox/65.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,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: Hm\_lvt\_34d6f7353ab0915a4c582e4516dffbc3=1546615857; Hm\_cv\_34d6f7353ab0915a4c582e4516dffbc3=1\*visitor\*135746%2CnickName%3A%E5%AD%9F%E7%B9%81%E9%95%87; Hm\_lvt\_bfc6c23974fbad0bbfed25f88a973fb0=1547039949; Hm\_lvt\_f5df380d5163c1cc4823c8d33ec5fa49=1547039949

Upgrade-Insecure-Requests: 1

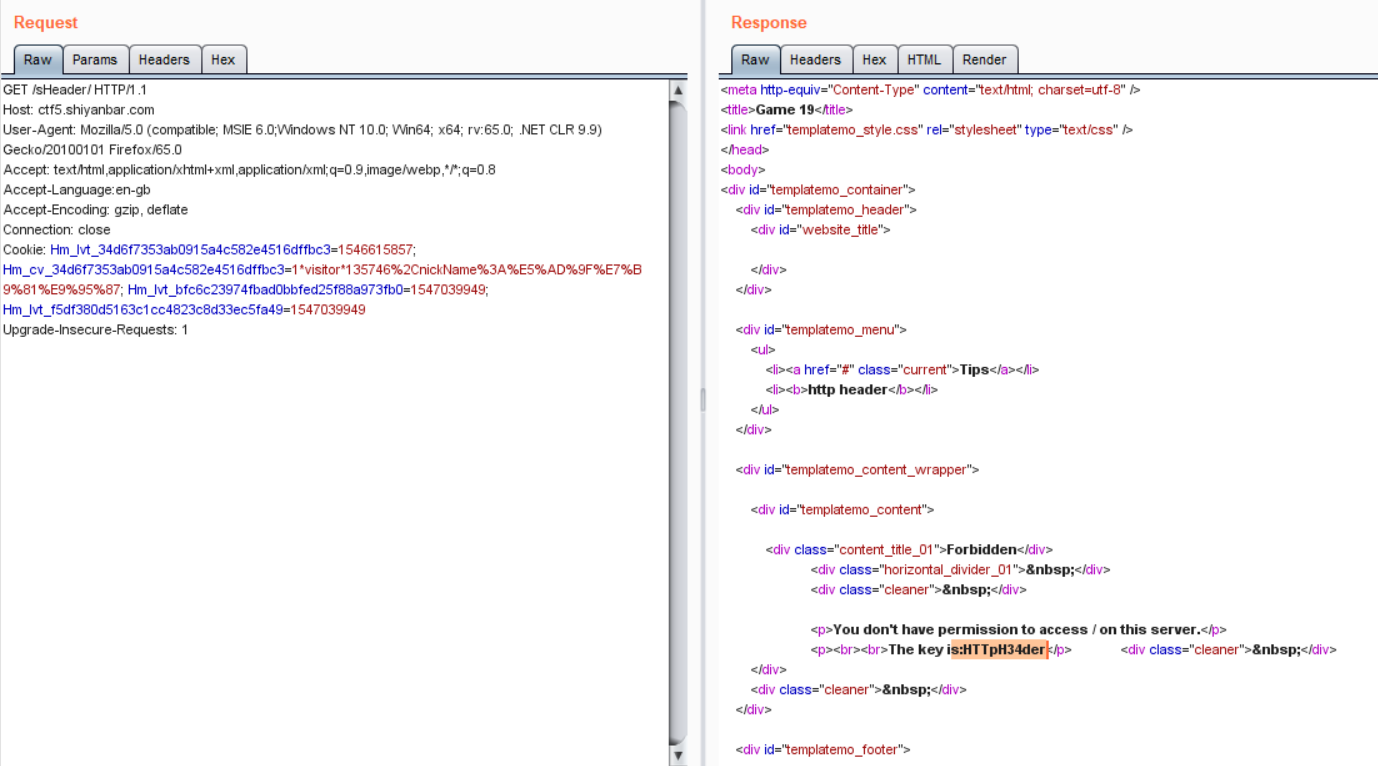
适时的时候加入下面三条指令

compatible; MSIE 6.0

.NET CLR 9.9

en-gb

提交后即可得到flag



Ps 相关信息

首先是在User-Agent中，添加compatible; MSIE 6.0，使得服务器认为我们使用的是IE6.0的浏览器

接下来添加.NET CLR 9.9，使得服务器认为我们安装了.NET 9.9框架

接下来是修改Accept-language，改为en-gb，使得服务器认为我们在英国