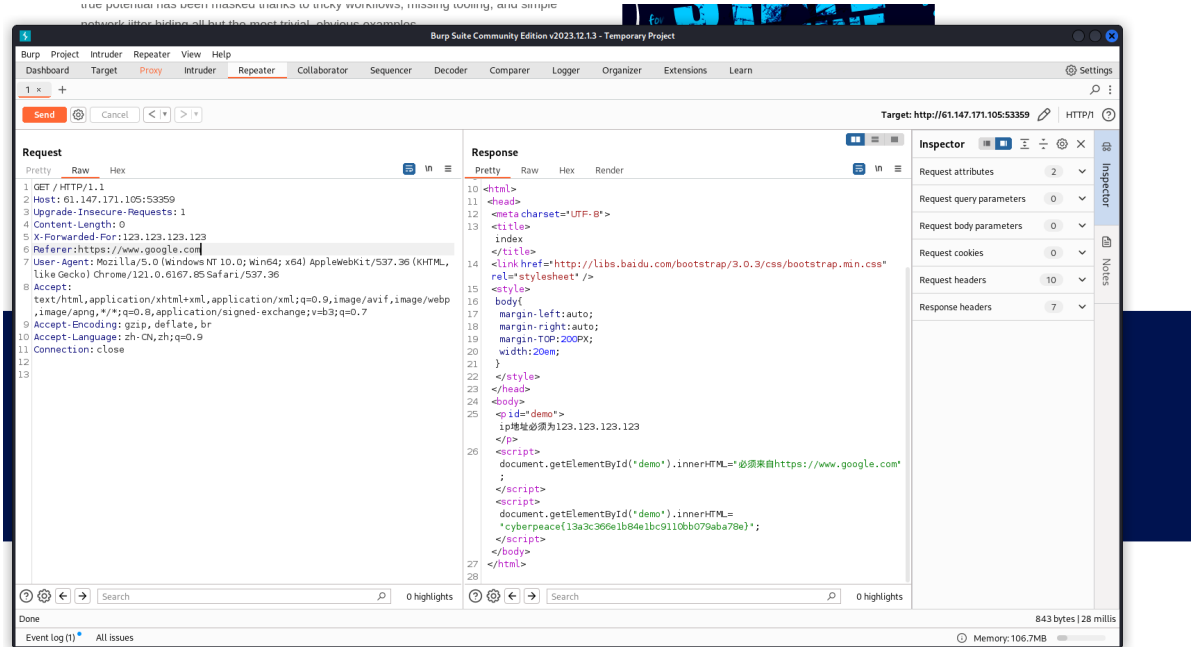
重新做题，先随即做两个

adworld使用随机题随便做的

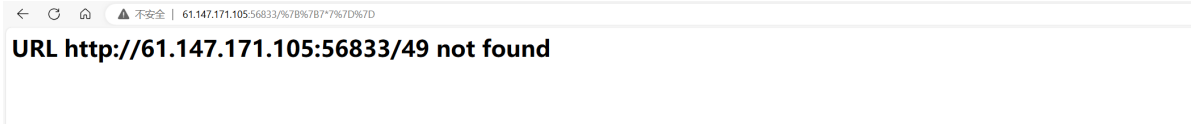
1. **X-Forwarded-For (XFF)**:
   - **用途**：XFF 头部字段用于标识通过 HTTP 代理或负载均衡器连接到 Web 服务器的客户端的原始 IP 地址。它帮助服务器识别请求的真实来源 IP 地址。
   - **格式**：通常是一个逗号分隔的 IP 地址列表，第一个 IP 地址是最初连接到代理或负载均衡器的客户端 IP 地址。例如：`X-Forwarded-For: 203.0.xxx.195, 70.xxx.3.18, 150.xxx.238`。
   - **伪造**：通过修改 HTTP 请求头中的 XFF 字段，可以伪造请求的来源 IP 地址。这在渗透测试和某些攻击场景中可能被利用
2. **Referer**:
   - **用途**：Referer 头部字段包含当前请求的来源页面 URL 地址，通常用于追踪用户行为和引荐来源信息。
   - **格式**：Referer 字段通常位于 HTTP 请求头的第二个位置，紧随 Host 字段之后。例如：`Referer: http://example.com/previous-page`
   - **伪造**：通过修改 HTTP 请求头中的 Referer 字段，可以伪造请求的来源页面 URL 地址。这在绕过某些安全检查或进行钓鱼攻击时可能被利用。

根据提示，构造出符合要求的ip和html



再随机一题

可以看到有ssti注入



经典的注入方程

__class__ 返回类型所属的对象
__mro__ 返回一个包含对象所继承的基类元组，方法在解析时按照元组的顺序解析。
__base__ 返回该对象所继承的基类 // __base__和__mro__都是用来寻找基类的

__subclasses__ 每个新类都保留了子类的引用，这个方法返回一个类中仍然可用的的引用的列表
__init__ 类的初始化方法
__globals__ 对包含函数全局变量的字典的引用

测试了一下没有过滤，直接tplmap