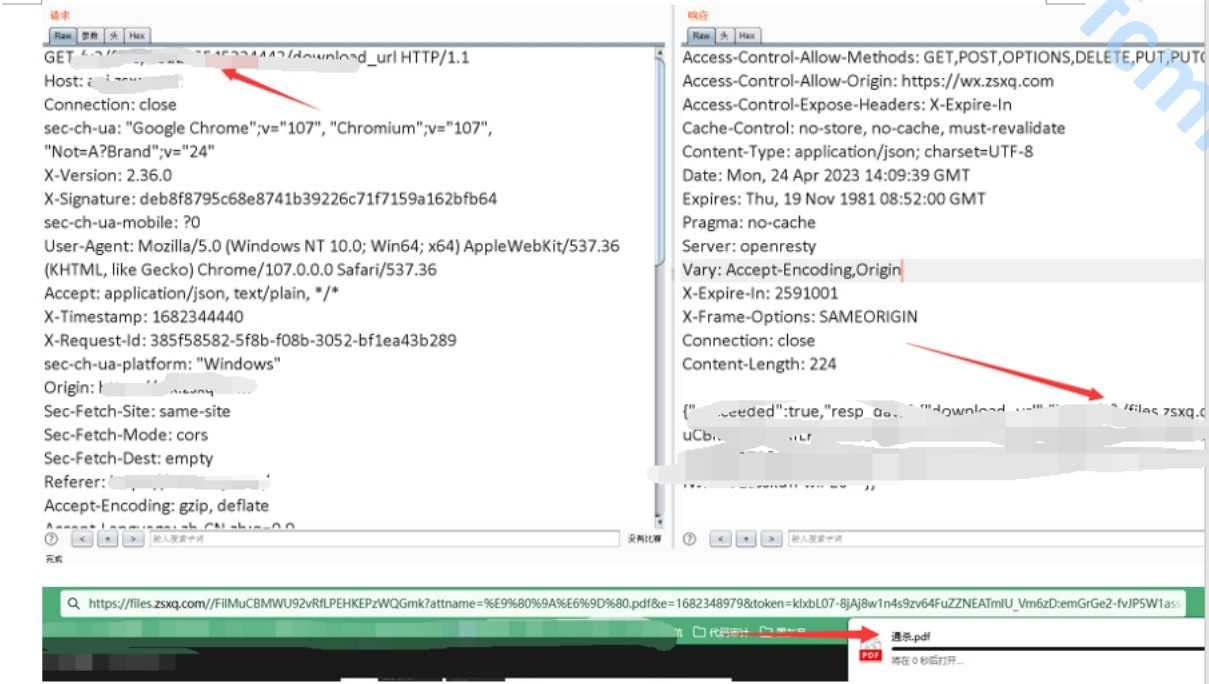
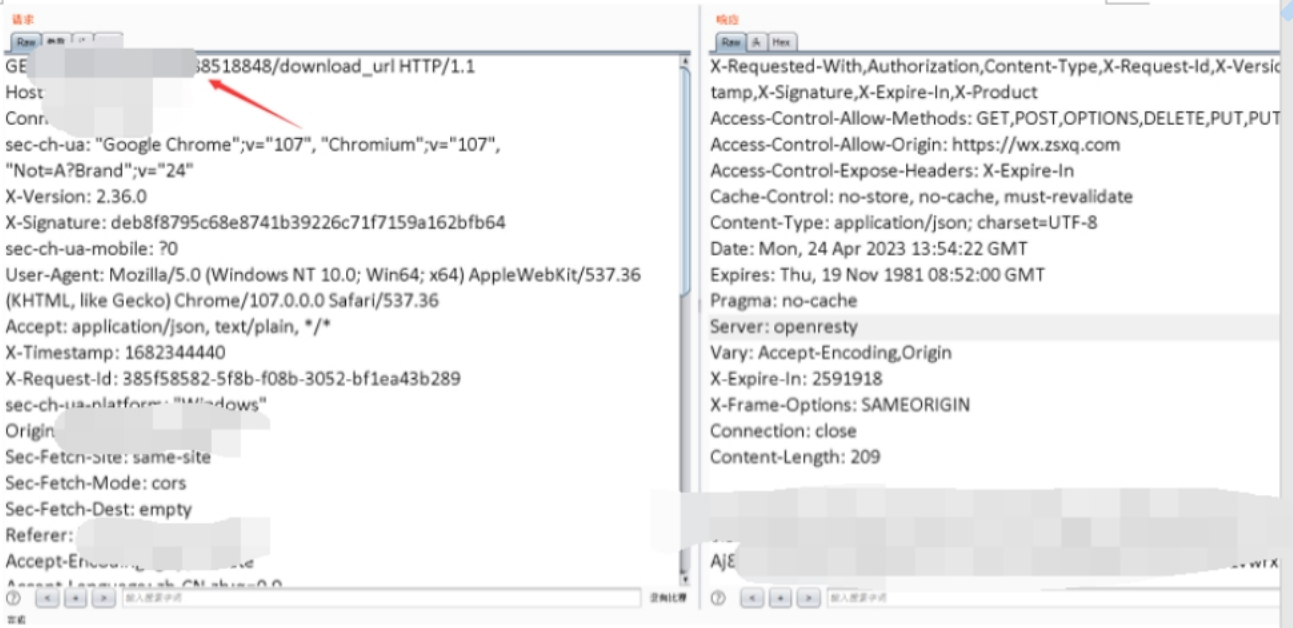


可以看到下载文件没有做鉴权 此时我们有了一个大胆的想法 如果我们可以拿到下面那

些暂时还不能看的文件 file_id 是否可以实现越权下载

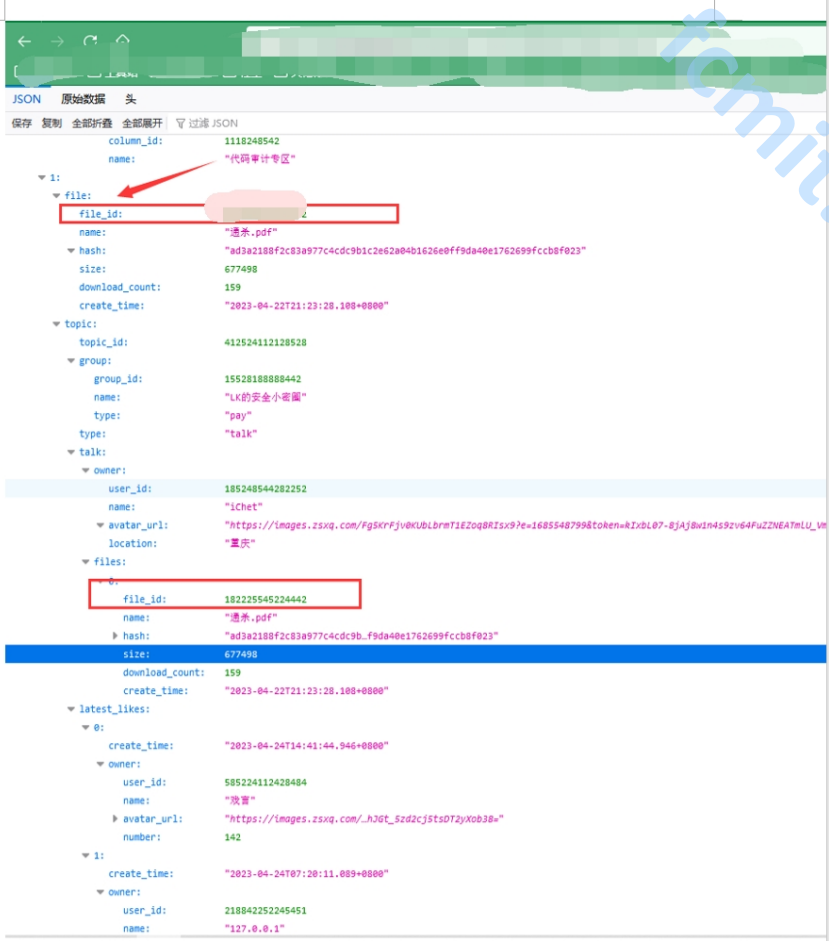
拿到 file_id 的方法很容易



找一下接口信息 找到一处接口泄露

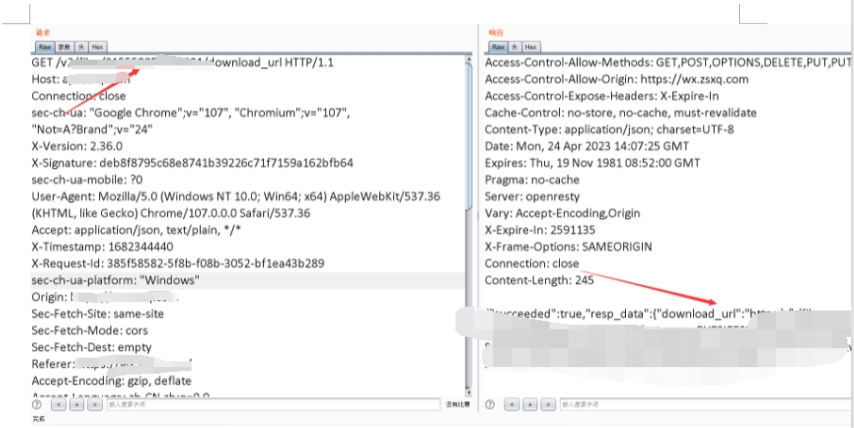
https://[redacted]3188888442/files?count=9

https://[redacted]8888442/files?count=9



发现这个参数是 file_id 首先尝试越权下载文件↵

发现这个参数是 file_id 首先尝试越权下载文件↵



url↵

此时我们换一个 file_id↵

一、详细说明：

知识星球 星主为了防止某些人白嫖会设置三天新人权限，直到三天之后才可以查看星球全部主题。这个漏洞可以绕过三天新人权限越权下载所有文件完成白嫖

三天权限证明

二、漏洞证明：

我们在下载文件的时候开启抓包 通过查看数据包发现下载哪个文件主要由这串数字控制