# 网易公开课精品课业务存在逻辑漏洞

漏洞类型: 逻辑漏洞

漏洞危害: 严重

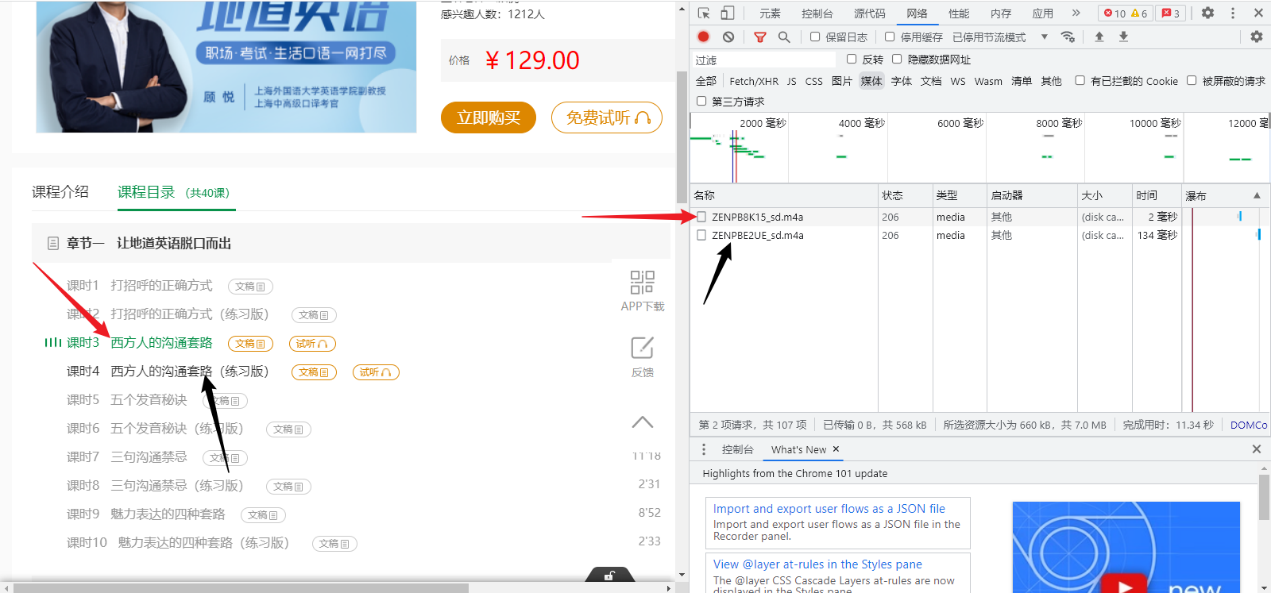
漏洞URL: <https://vip.open.163.com/>

漏洞复现:

首先访问URL:https://vip.open.163.com/

可以看到很多序号付费才能观看下载的课

然后我们点进去一个课,按F12查看,并选中一节试听课播放



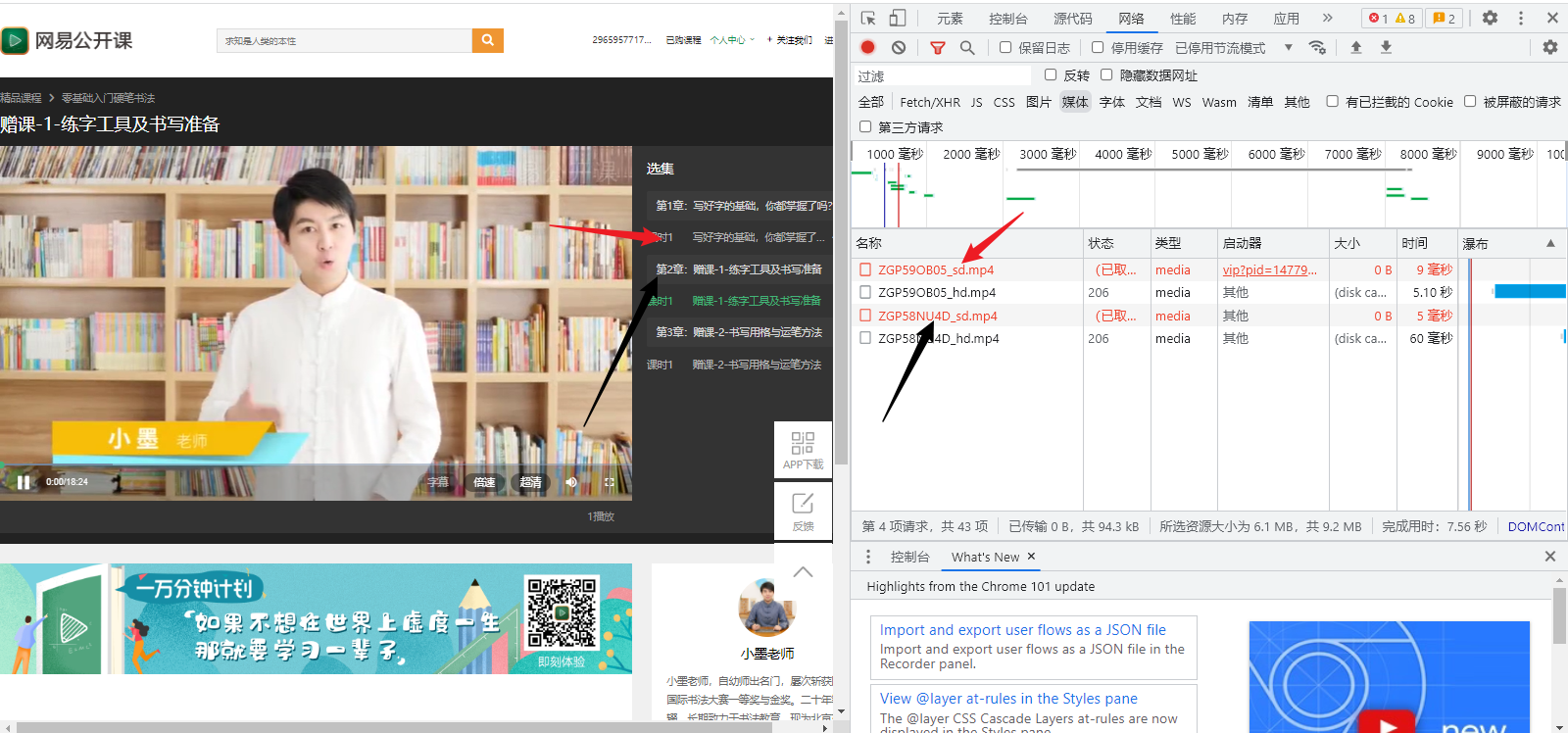
可以看到点击第一个试听的资源的时候,调用了https://open-audio.ws.126.net/nos/m4a/2019/09/10/ZENPB8K15\_sd.m4a

也就是ZENPB8K15这个文件,点击第二个试听资源的时候调用了https://open-audio.ws.126.net/nos/m4a/2019/09/10/ZENPBE2UE\_sd.m4a这个URL地址,也就是ZENPBE2UE这个文件

这两个文件只有后面四位是不一样的,也就是只有后面四位不会变,那么通过爆破后面四位字符就可以获得其他的付费资源从而完成白嫖课程,并且这个课程调用资源地址是非加密的

并且下文的购买提示中也说明不能够下载,但是这个调用资源的URL地址泄露出来,也就可以被下载下来

此时我们购买一节付费的视频课程



这节购买的视频课程也可以看的出来调用了ZGP58NU4D和ZGP59OB05这两个文件,这两个文件也仅仅是后面五位的字符不一样,也可以通过爆破后五位来获取到,并且也可以直接访问资源的URL地址将其保存下来

固恶意用户可以购买付费课查看调用的URL资源地址将视频资源,音频资源非法保存下来

而不付费的用户,可以通过试听课的调用视频URL资源地址的文件,通过爆破,枚举的手段,将后续付费的视频课程,或者音频课程的URL地址爆破或者枚举出来,达到白嫖视频课程的效果