关于91淘课网漏洞的发现与破解

作者：zz 时间:2015-9-17

网站网址: <http://www.91taoke.com/>

漏洞发现时间: 2015-8-1

漏洞发现者: [zhujunxxxxx@163.com](mailto:zhujunxxxxx@163.com)

漏洞危险级别: 高

网站界面:



学生中心的微视频:



微课视频中心



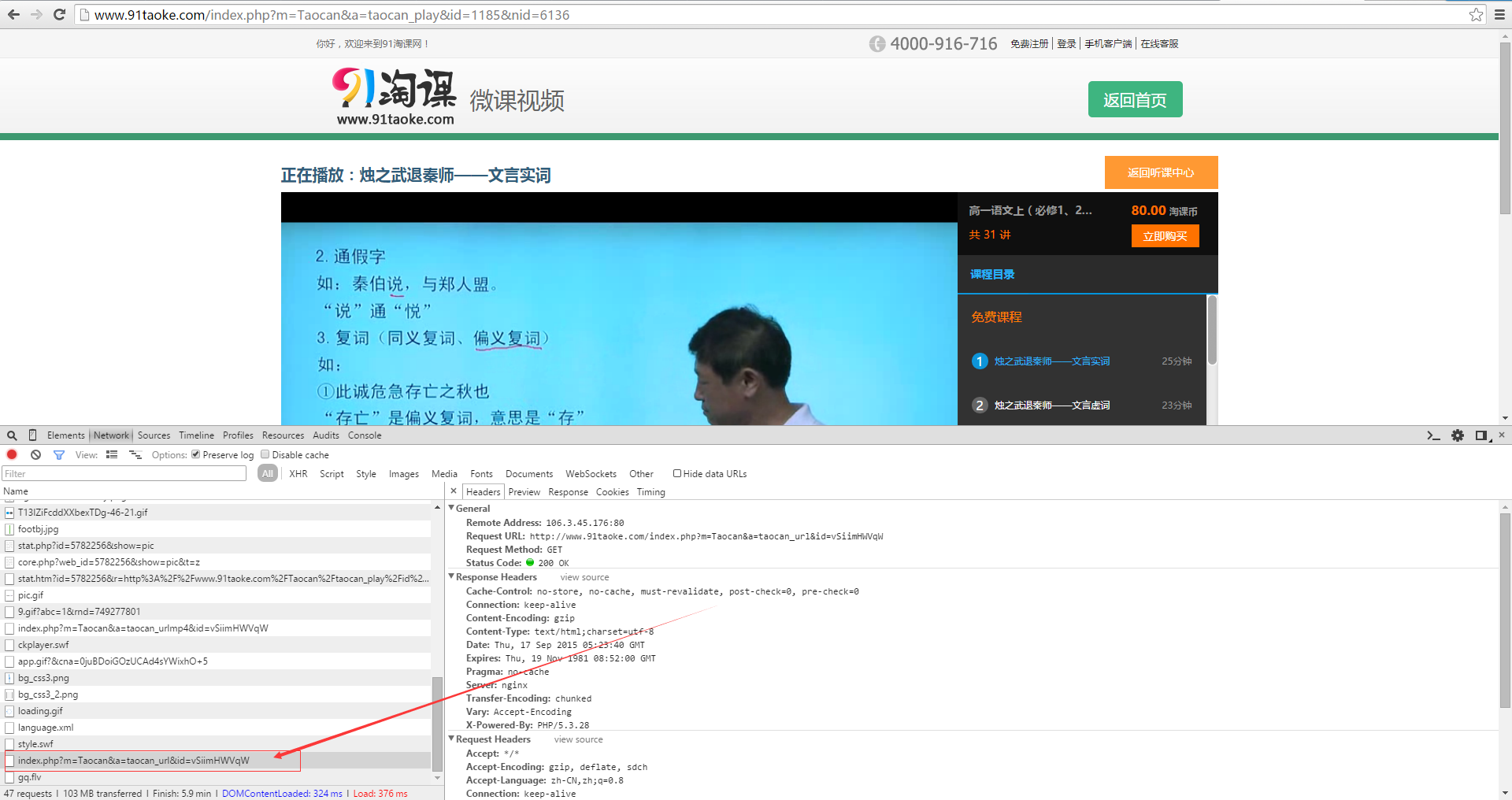
视频播放界面



在这个播放界面我们可以看到除了一些免费播放的以外剩余的都是需要付费的



在页面上我们可以看到这么一个http请求，没错这就是获取播放地址的请求





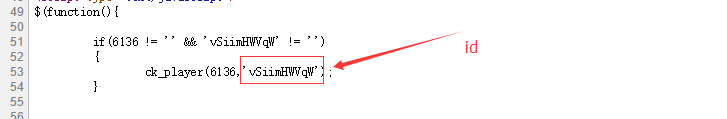
我们可以发现

<http://www.91taoke.com/index.php?m=Taocan&a=taocan_url&id=vSiimHWVqW>

这个地址的参数是刚才

<http://www.91taoke.com/index.php?m=Taocan&a=taocan_play&id=1185&nid=6136>

这个网址打开源码后里面的



至此，我们分析到了要获取一个播放地址的流程，但是

<http://www.91taoke.com/index.php?m=Taocan&a=taocan_play&id=1185&nid=6136>

这个地址中的id我们是知道的，是在



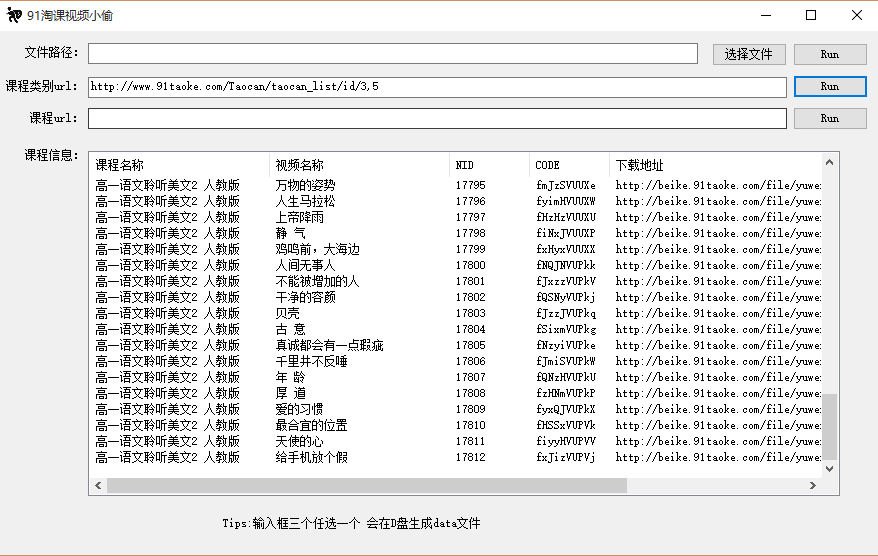
这个课程中心页面里面获取的，最重要的是后面的nid这个参数

我们查看课程中心页面的源码



所以我们就可以获取到nid了

然后就可以写程序疯狂的获取所有收费视频的地址了



通过给出的视频地址下载视频文件

