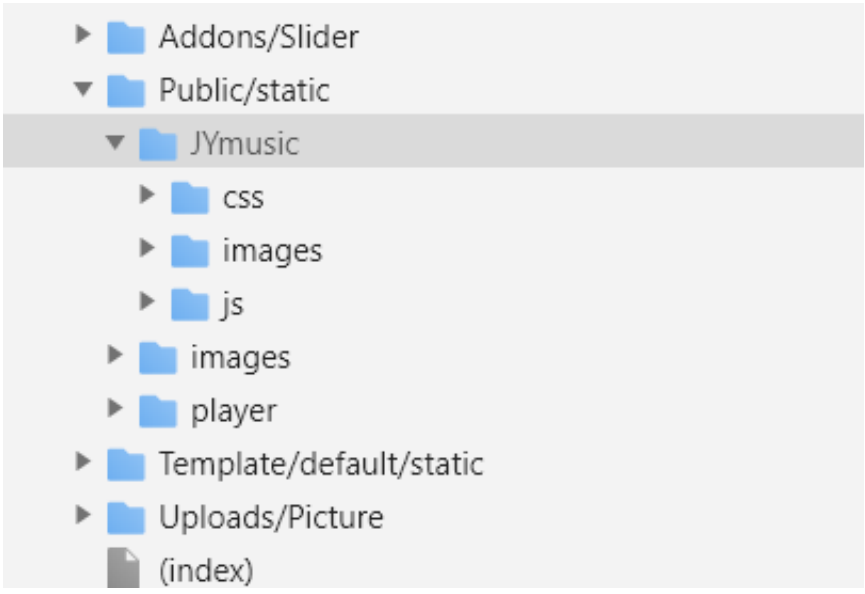
0x00：前言

某天测厂商业务时，发现其中有一个提供音乐播放业务的资产，正好里面有我想听的歌，于是就有了这篇文章

0x01：信息收集

F12简单看下目标信息环境:

ServerSoft:IIS 7.5　**CMS**:JYMusic(ThinkPHP)



▼ Response Headers view source

Cache-Control: private

Content-Encoding: gzip

Content-Length: 15989

Content-Type: text/html; charset=utf-8

Date: Sat, 05 Dec 2020 08:06:41 GMT

Expires: Thu, 19 Nov 1981 08:52:00 GMT

Pragma: no-cache

Server: Microsoft-IIS/7.5

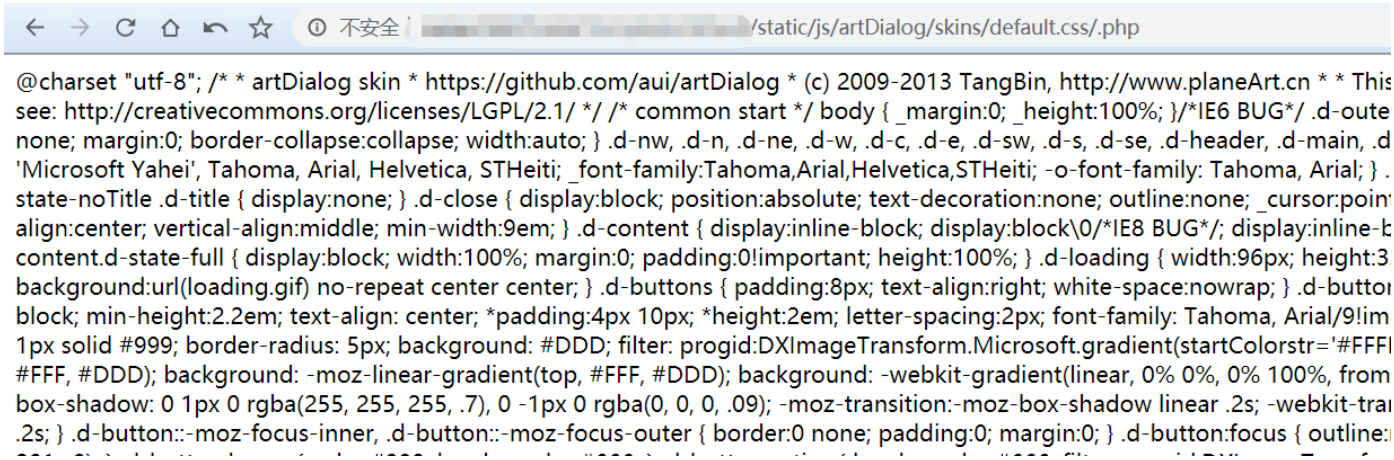
Vary: Accept-Encoding

X-Powered-By: ThinkPHP

X-Powered-By: ASP.NET

0x02：开搞和碰壁

抱着试试看的心态随便找了个资源文件试了发解析漏洞，没想到成功了，那么现在只需要找到上传点就能getshell了。



- 常见的编辑器
  - Ueditor/Umeditor
  - Kindeditor
  - ckeditor/ckfinder
- 程序上传点
  - 头像/文章/附件...
  - 上传组件

目标站开放注册，登录后发现存在头像上传功能，原以为直接可以搞定了，结果却不尽人意，应该是二次渲染了。。。

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml"><head>
<meta content="text/html; charset=utf-8" http-equiv="Content-Type">
<title>系统发生错误</title>
<style type="text/css">
*{ padding: 0; margin: 0; }
html{ overflow-y: scroll; }
body{ background: #fff; font-family: '微软雅黑'; color: #333; font-size:
16px; }
img{ border: 0; }
.error{ padding: 24px 48px; }
.face{ width:320px; margin:20px auto; }
.face img {width:320px; }
h1{ font-size: 32px; line-height: 48px; text-align:center; }
.error .content{ padding-top: 10px}
.error .info{ margin-bottom: 12px; }
.error .info .title{ margin-bottom: 3px; }
.error .info .title h3{ color: #000; font-weight: 700; font-size: 16px;
}
.error .info .text{ line-height: 24px; }
.copyright{ padding: 12px 48px; color: #999; margin:0 auto; width:220px}
.copyright a{ color: #000; text-decoration: none; }
</style>
</head>
<body>
<div class="error">
<p class="face"><img src="/Public/static/JYmusic/images/404.jpg"></p>
<h1>你访问的页面不存在~</h1>
<div class="content" style="margin:0 auto">
</div>
</div>
<div class="copyright" >
<p><a title="官方网站" href="http://www.jyuu.cn">JYmusic</a><sup></sup>[ php
音乐管理程序 ]</p>
```

试了上传一些二次渲染后仍能执行的Webshell后依然发现无法正常getshell，看样得放弃头像这个地方了

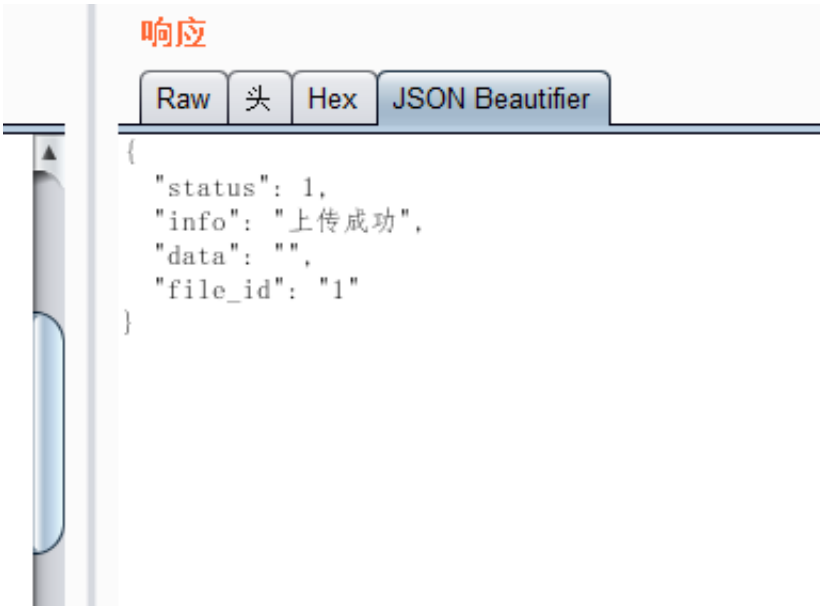
0x03：柳暗花明又一村

既然头像上传走不通那么只能另寻出路，分享音乐功能被改成人工审核，但是猜测接口还是存在的。

这里通过fofa找到一个功能正常的站点，以下称为www.bbb.com

这个站点的分享音乐功能是正常的

直接上传音乐文件

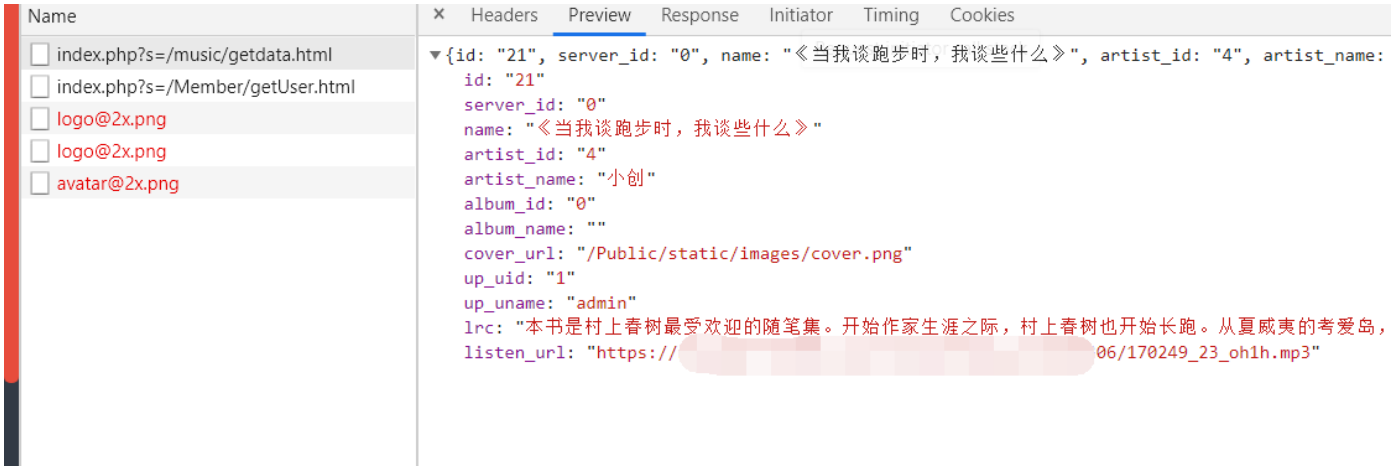


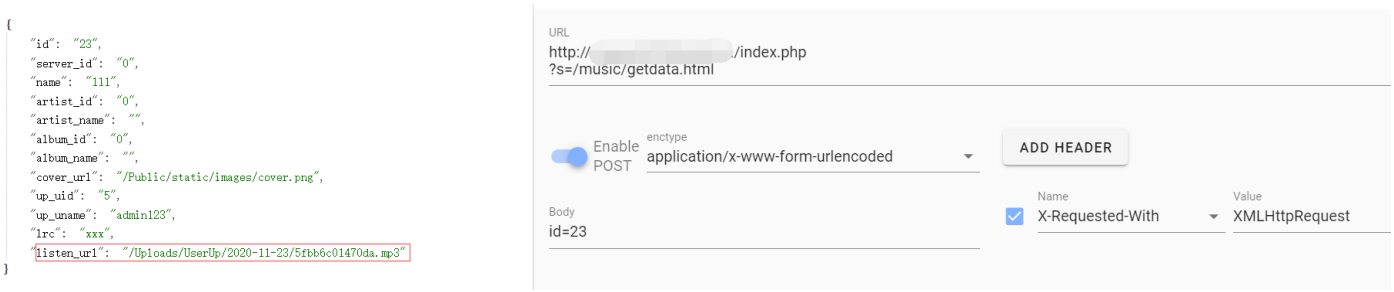
文件正常上传，但是没有返回路径emmm，提交试试。

wtf，没有分类数据咋办，祭出神器F12给select标签加一个有value值的option。

提示分享成功，查看审核列表也有了，编辑发现ID为23，首页随便点进去一个发现id为21。

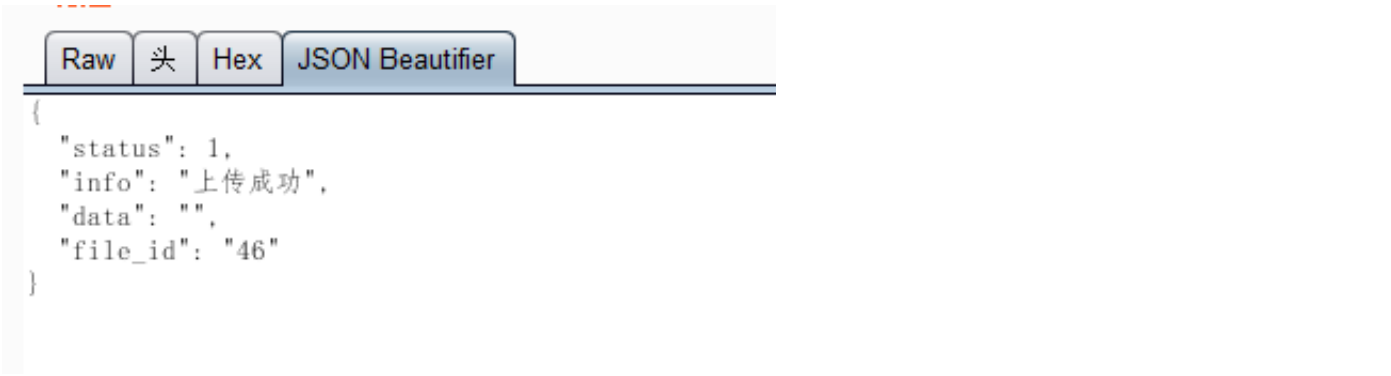
同时发现接口可以获取音乐上传路径，替换为ID=23后取得路径。





那么思路就来了，把www.bbb.com的操作在www.aaa.com重现一遍即可

直接把bbb.com上传音乐文件的请求，移花接木到aaa.com上（burp改包host和cookie，提交时改fileid）。



song=111&genre=123&album=0&fileid=46&lrc=xxx&signature=xxx

通过解析漏洞访问我们后缀名为MP3的webshell

至此成功getshell