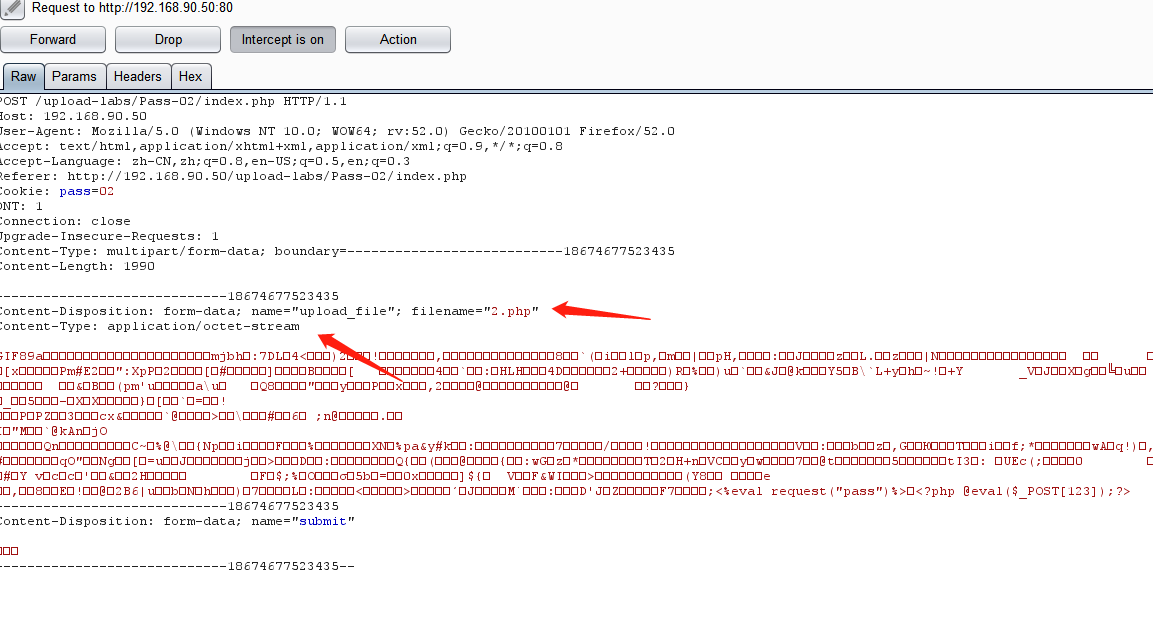
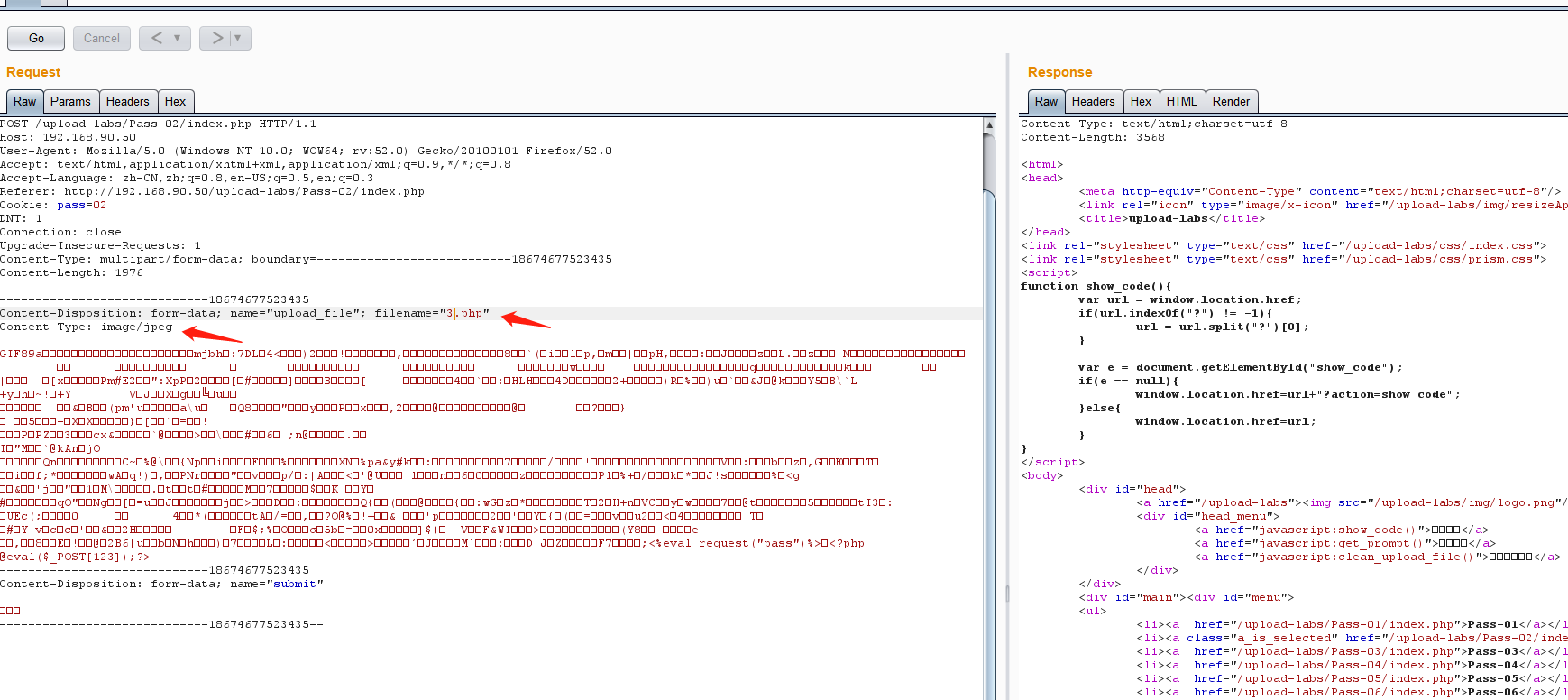
**Pass-02-只检查Content-type**

开始上传一个php，发现提示

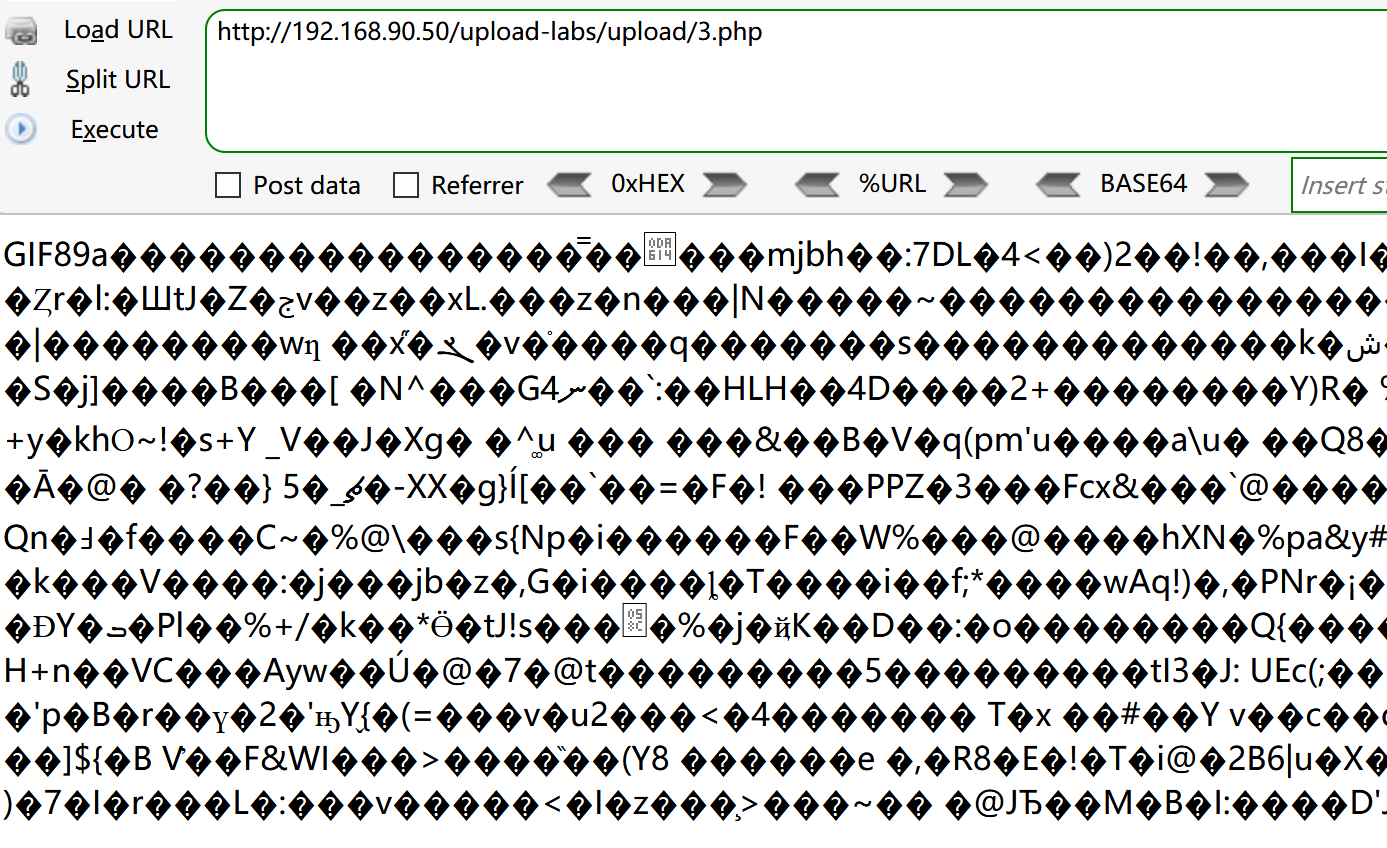
我们猜测这可能是个文件类型，要修改**Content-type。抓包，**



果不其然。我们改成图片的文件格式类型。



我们去校验一下。



分析代码：

$is\_upload = false;

$msg = null;

if (isset($\_POST['submit'])) {

if (file\_exists($UPLOAD\_ADDR)) {

if (($\_FILES['upload\_file']['type'] == 'image/jpeg') || ($\_FILES['upload\_file']['type'] == 'image/png') || ($\_FILES['upload\_file']['type'] == 'image/gif')) {

if (move\_uploaded\_file($\_FILES['upload\_file']['tmp\_name'], $UPLOAD\_ADDR . '/' . $\_FILES['upload\_file']['name'])) {

$img\_path = $UPLOAD\_ADDR . $\_FILES['upload\_file']['name'];

$is\_upload = true;

}

} else {

$msg = '文件类型不正确，请重新上传！';

}

} else {

$msg = $UPLOAD\_ADDR.'文件夹不存在,请手工创建！';

}

}

可以看到，后端php代码只对Content-Type进行了检查。