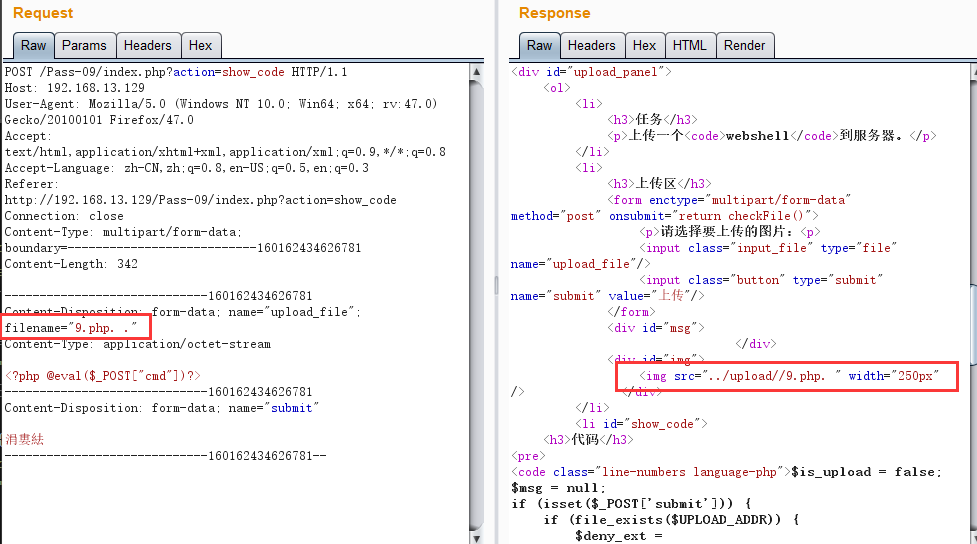
#### **点+空格+点绕过**

**原理同Pass-06**，上传文件名后加上**点+空格+点**，改为09.php. .



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

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

$deny\_ext = array(".php",".php5",".php4",".php3",".php2",".html",".htm",".phtml",".pHp",".pHp5",".pHp4",".pHp3",".pHp2",".Html",".Htm",".pHtml",".jsp",".jspa",".jspx",".jsw",".jsv",".jspf",".jtml",".jSp",".jSpx",".jSpa",".jSw",".jSv",".jSpf",".jHtml",".asp",".aspx",".asa",".asax",".ascx",".ashx",".asmx",".cer",".aSp",".aSpx",".aSa",".aSax",".aScx",".aShx",".aSmx",".cEr",".sWf",".swf",".htaccess");

$file\_name = trim($\_FILES['upload\_file']['name']);

$file\_name = deldot($file\_name);//删除文件名末尾的点

$file\_ext = strrchr($file\_name, '.');

$file\_ext = strtolower($file\_ext); //转换为小写

$file\_ext = str\_ireplace('::$DATA', '', $file\_ext);//去除字符串::$DATA

$file\_ext = trim($file\_ext); //首尾去空

看代码，我们上传的是php. . 删除末尾的.就剩下 .php.空格 strrchr 获取.后面的内容跟就是.php.空格 转换为小写 然后去去空格就是.php. 又回到了之前，钻了个空子