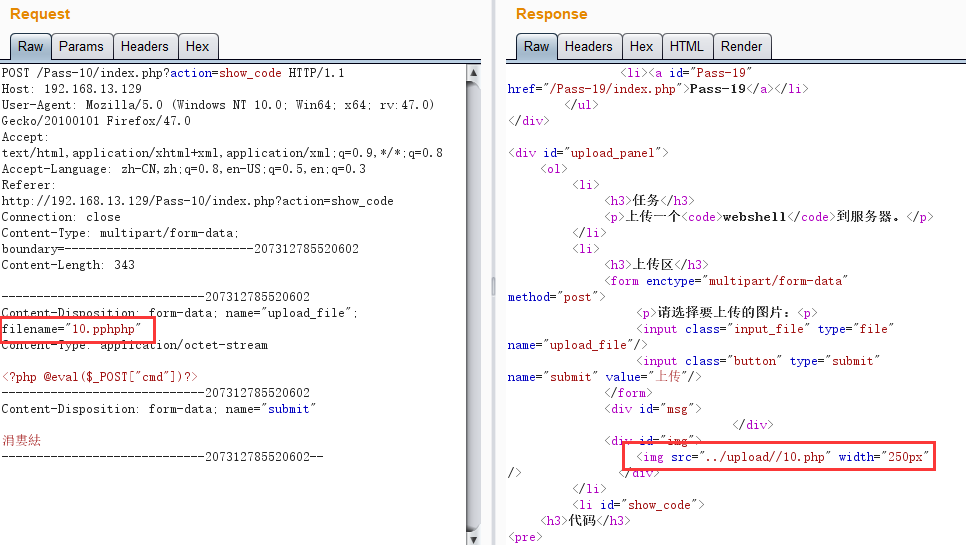
#### Pass-10 双写文件名绕过

双写文件名绕过，文件名改成10.pphphp等格式



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

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

$deny\_ext = array("php","php5","php4","php3","php2","html","htm","phtml","jsp","jspa","jspx","jsw","jsv","jspf","jtml","asp","aspx","asa","asax","ascx","ashx","asmx","cer","swf","htaccess");

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

$file\_name = str\_ireplace($deny\_ext,"", $file\_name); //关键点，把上面出现过的都替换成空格

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

$img\_path = $UPLOAD\_ADDR . '/' .$file\_name;

$is\_upload = true;

}

} else {

$msg = $UPLOAD\_ADDR . '文件夹不存在,请手工创建！';

}