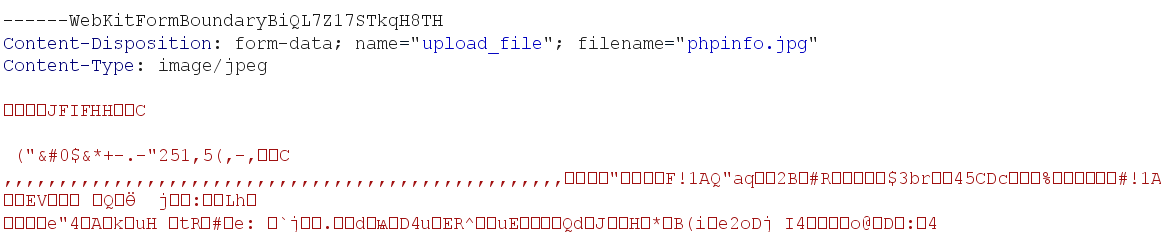
Upload-labs 第1-第8题,14-16(可以查看源代码)

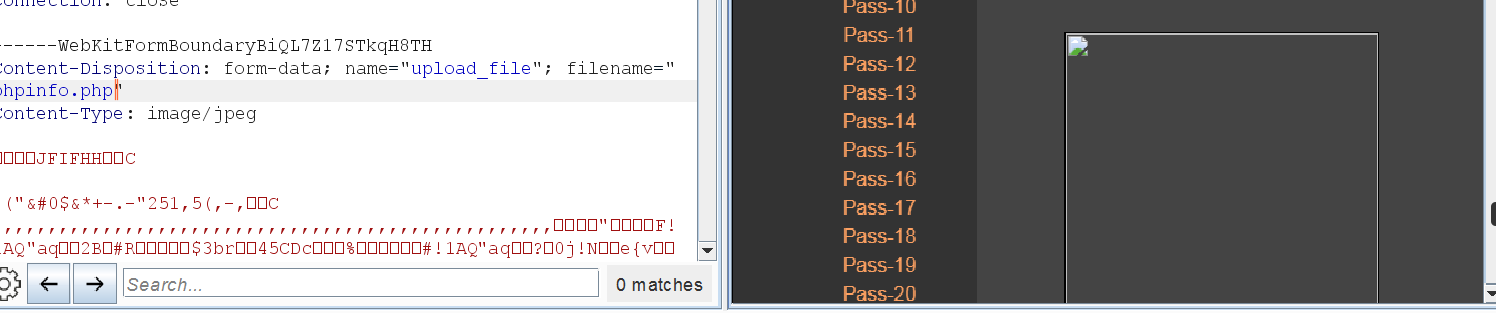
要求有详细的步骤,尽量使用尽可能多的方法,并且使用phpstorm进行调试,并将调试过程截图

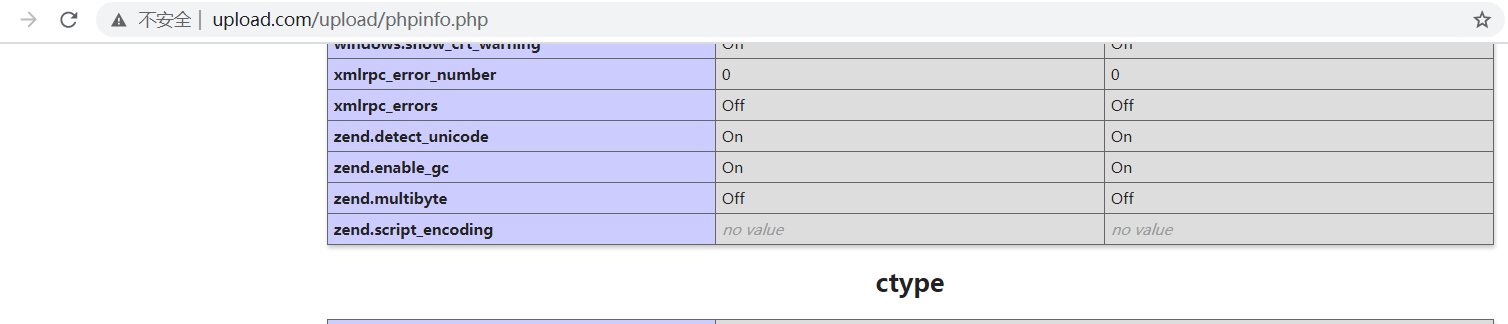
1. 第8题,14-16(可以查看源代码)

第1题

修改文件名后缀getshell





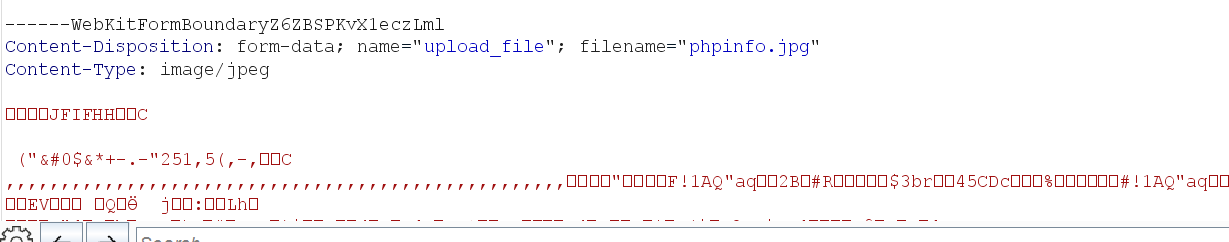


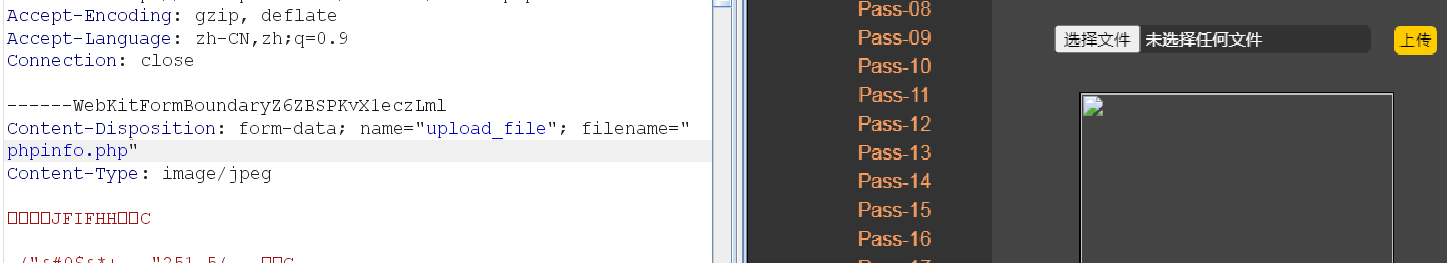
调试代码,后端啥都没有进行校验，直接改后缀即可绕过

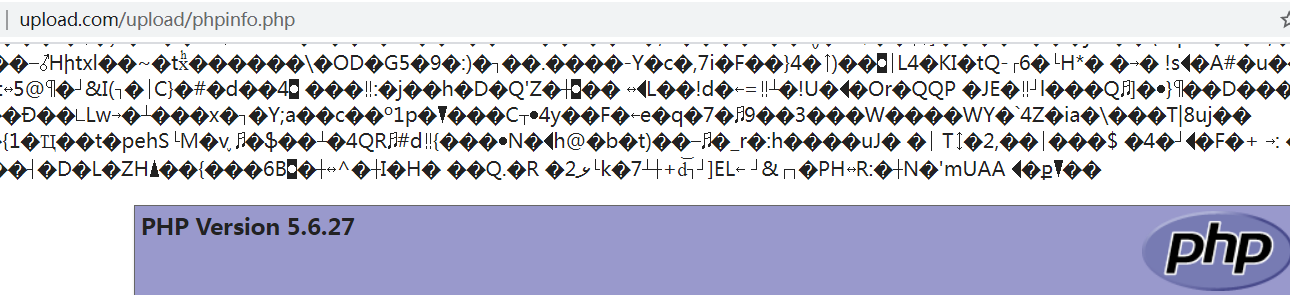


第2题

上传图片吗,修改文件名后缀getshell

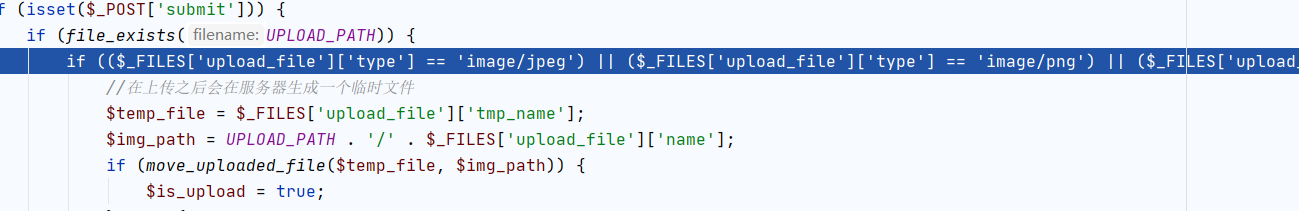






调式代码

代码只对图片的content-type进行校验，这里上传的时候合成图片马，直接绕过

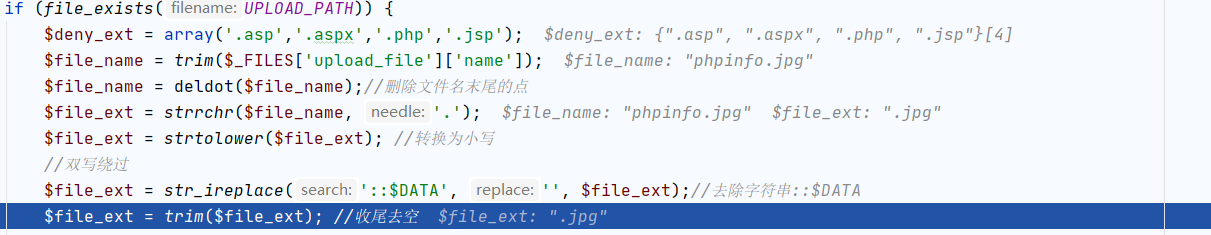


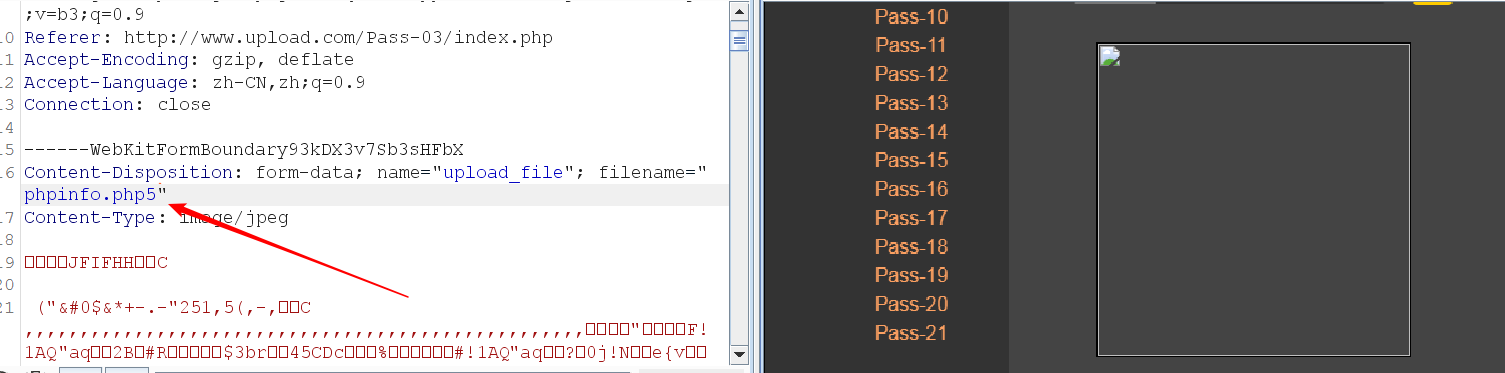
第3题

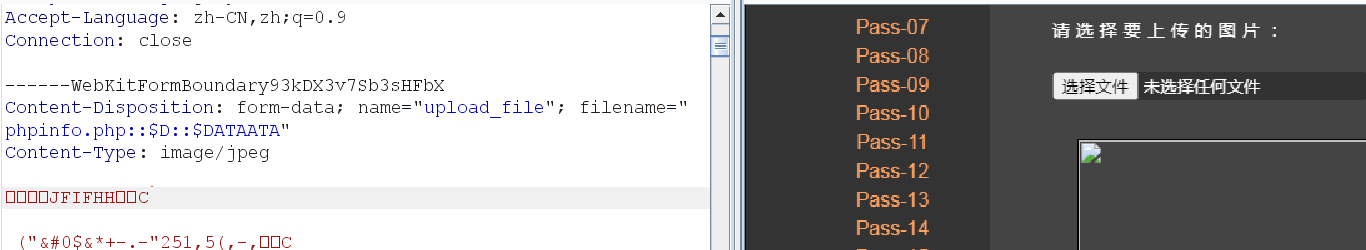
调试代码 发现只是简单过滤了几个文件后缀，可以尝试使用其他支持的后缀进行绕过

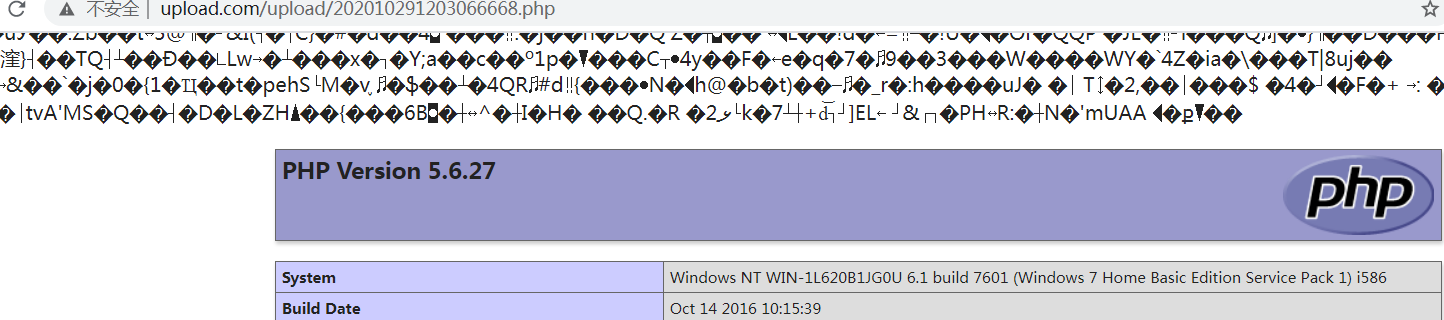
Strrchr:查找指定字符在字符串中的最后一次出现的位置，并且截取这个字符串结尾到末尾的字符串 这里貌似无法绕过

将::%DATA替换为空 只用双写进行绕过









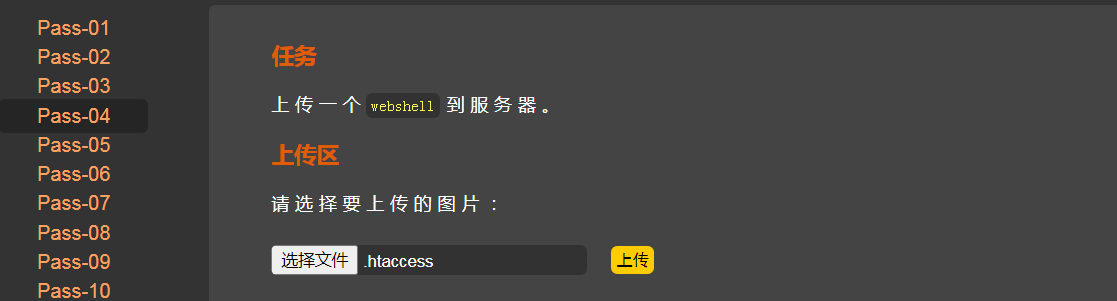
使用php2、php3、php5后缀上传

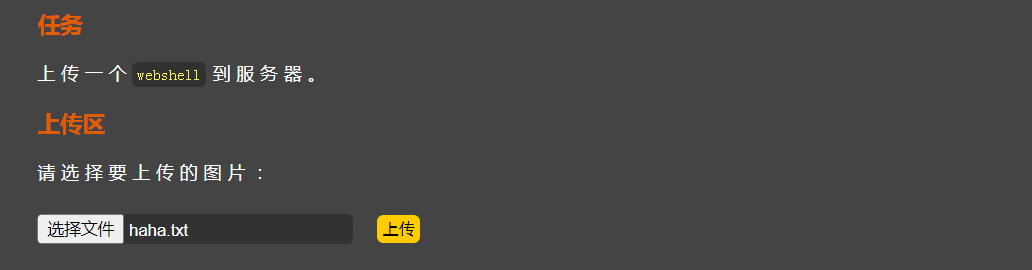
第4题

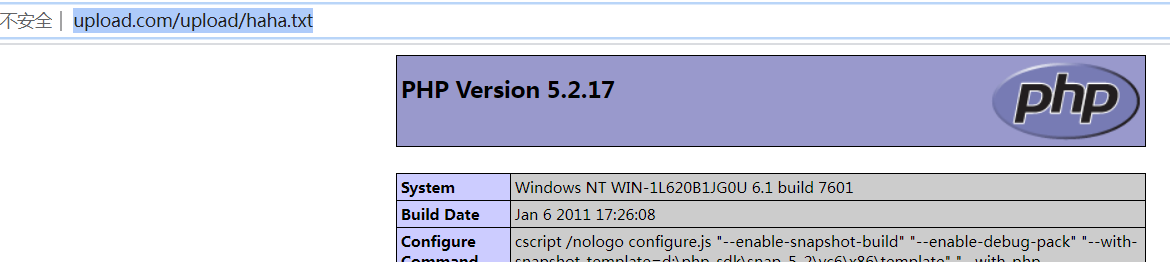
由于没有更改上传的文件名称，所以可以使用.htaccess+普通文件

以及使用. .

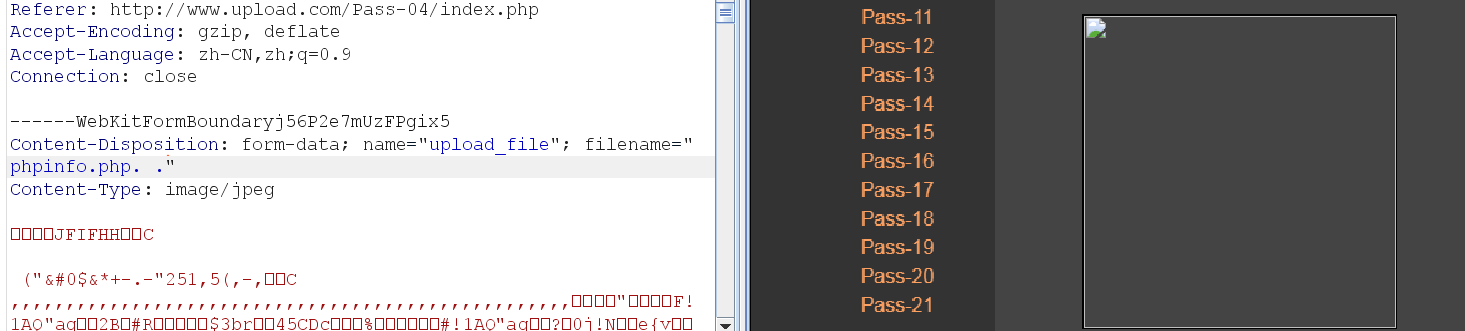


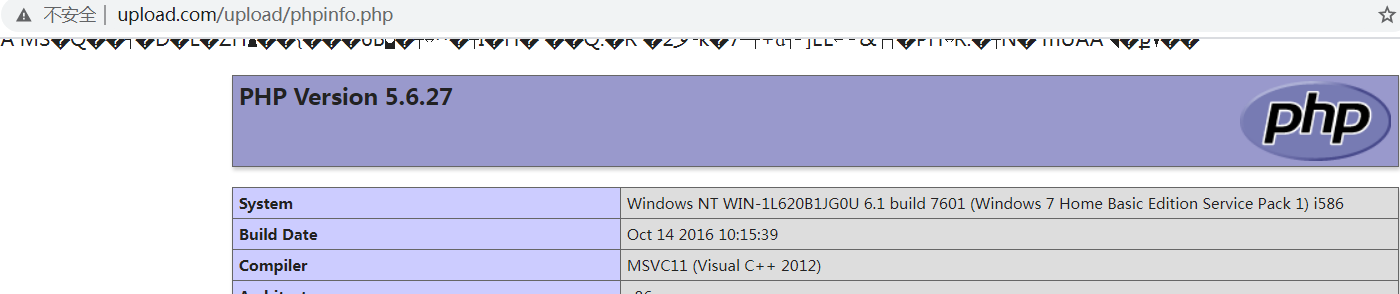






使用. .绕过

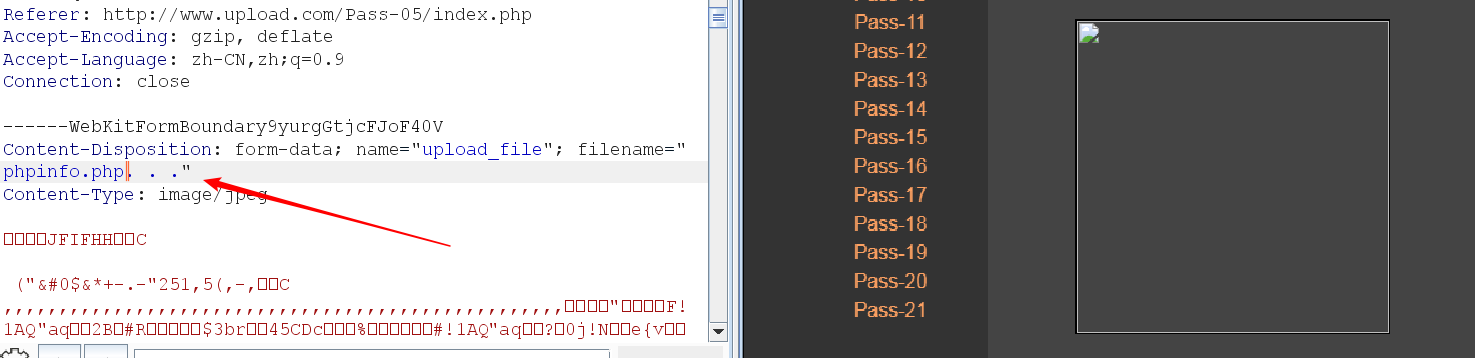


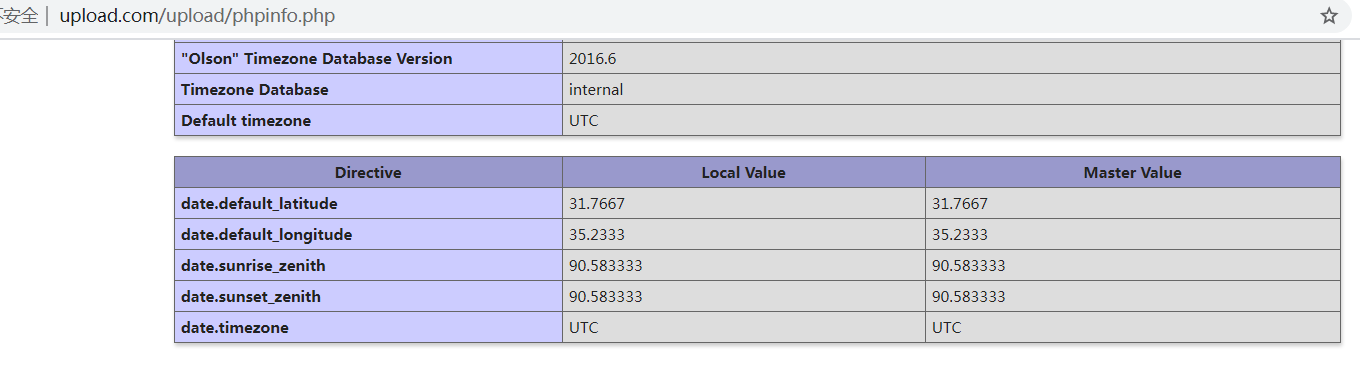


第五题



使用. . . 绕过

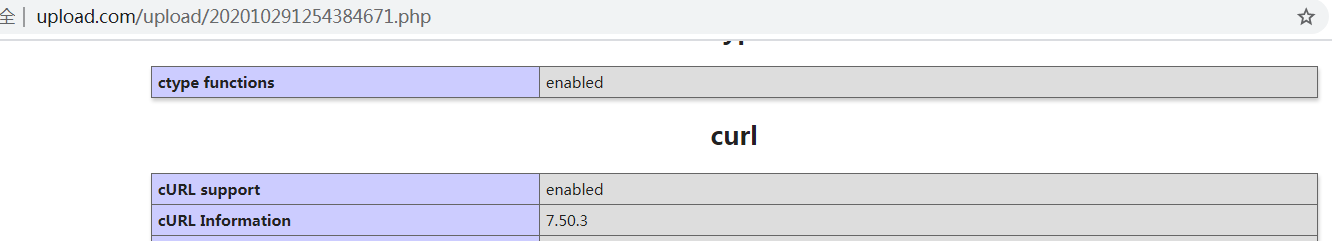




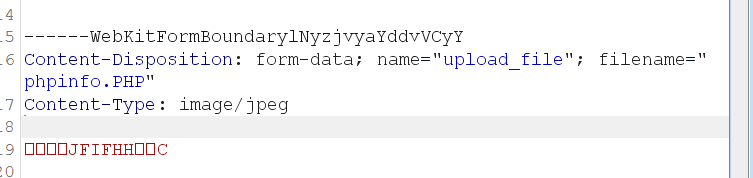
第六题

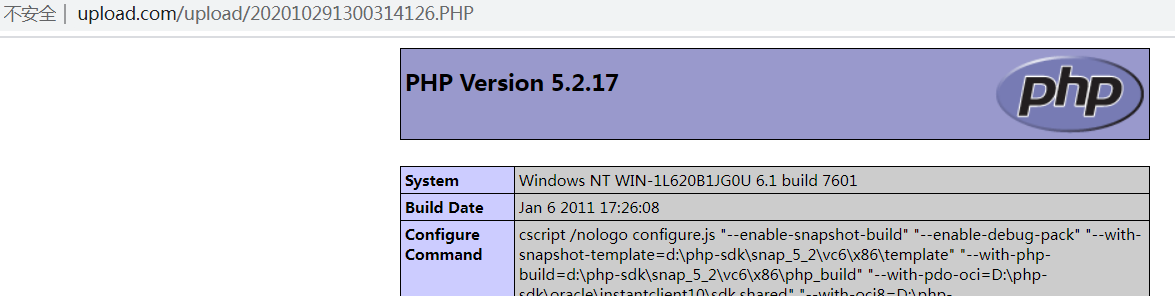


使用双写::$DATA



使用大小写

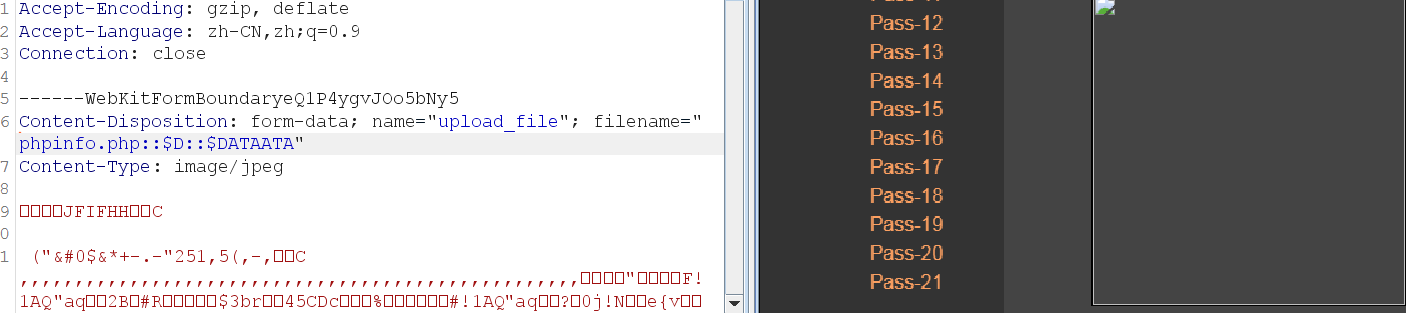


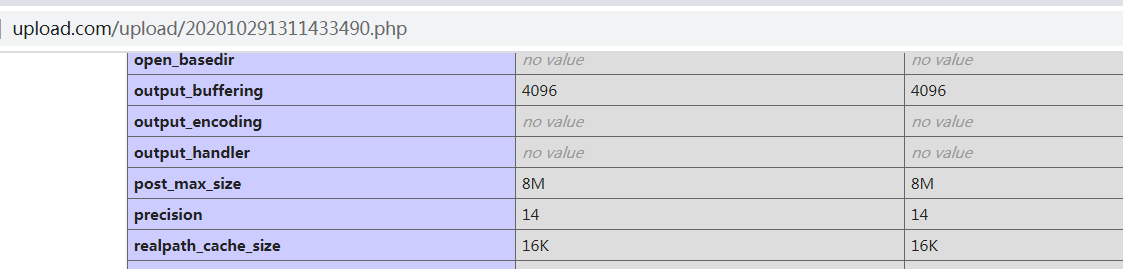


第七题



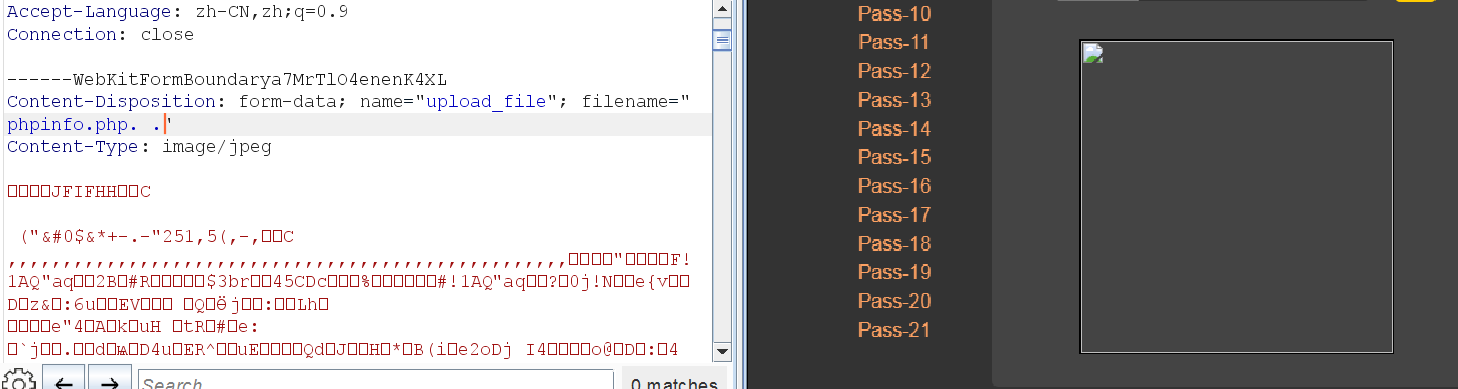
使用双写绕过

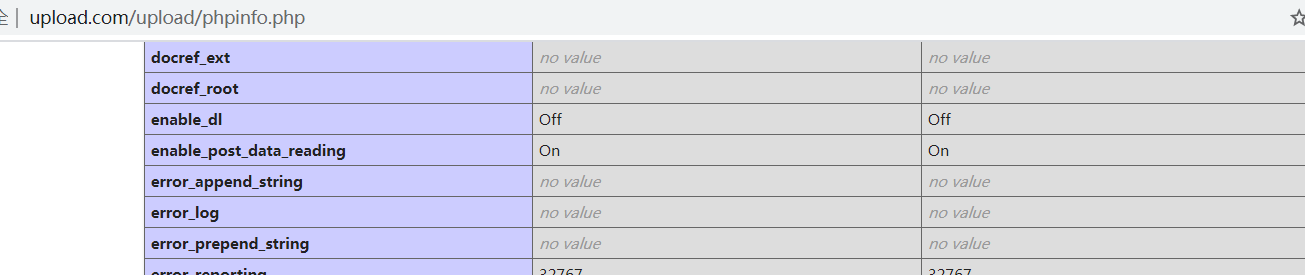




第八题







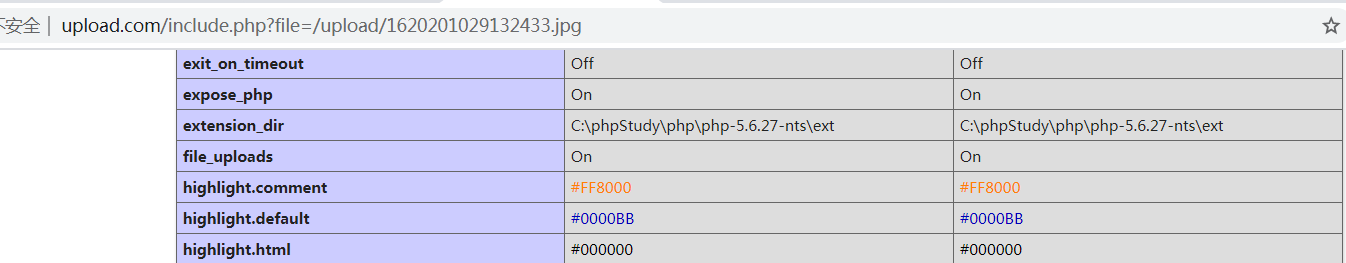
第14题目

通过文件包含漏洞



文件包含

http://www.upload.com/include.php?file=/upload/1620201029132433.jpg

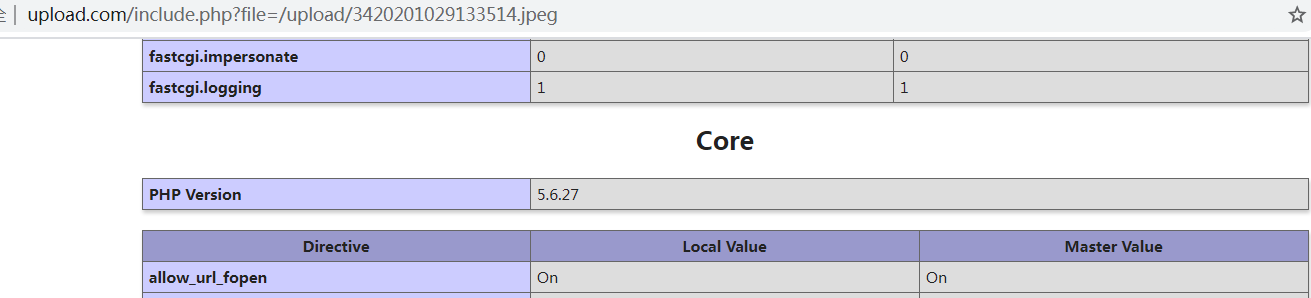


第十五题

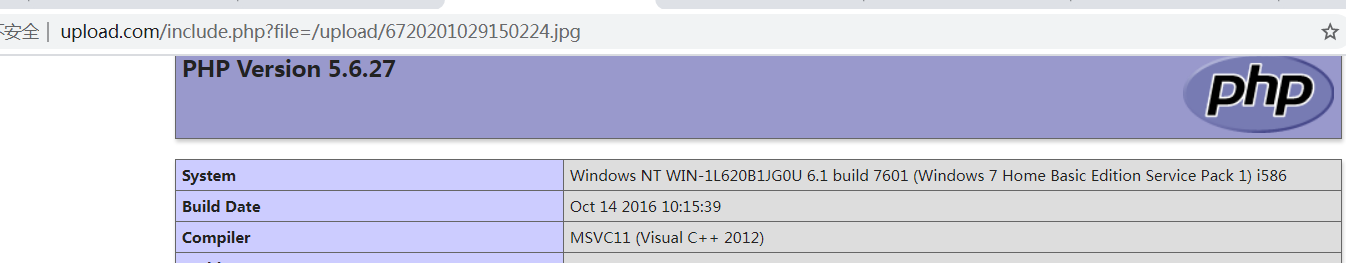


通过文件包含漏洞

|  |
| --- |
| http://www.upload.com/include.php?file=/upload/3420201029133514.jpeg |



第十六题



|  |
| --- |
| http://www.upload.com/include.php?file=/upload/6720201029150224.jpg |